FATF

FATF REPORT

Risk of Terrorist Abuse in Non-Profit Organisations

June 2014

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

CONTENTS

GLOSSARY OF TERMS AND ACRONYMS

Note: For the purposes of consistency, all currencies in this report have been converted to US dollars (USD).

Active recruitment: The recruitment of individuals by a terrorist movement through direct interaction with those individuals. (This type of recruitment is akin to 'talent-spotting.')

APG: Asia/Pacific Group on Money Laundering.

Capability: The operational capacity of a terrorist group to carry out its objectives. A threat is dependent on actors that possess both the *capability* and the *intent* to do harm, in this case towards the NPO sector.

AML: Anti-money laundering

CFT: Countering the financing of terrorism.

CT: Counter-terrorism

Detection: Any action, or series of actions, on the part of government or non-governmental actors that leads to the discovery of activity that could benefit terrorist entities. In the context of this report, this often involves the collection and analysis of different types of information.

Directing official: An individual who holds a leadership position in an NPO and has the ability to direct aspects of the NPO's activities. This includes directors, officers, trustees, and religious leaders.

Disruption: Any action taken by a government or non-governmental actor to interrupt activity that could benefit terrorist entities.

DNFBP: Designated Non-financial Business or Profession.

Dual-use equipment: Equipment that has both peaceful and military applications, depending on intent.

EFT: Electronic funds transfer.

Expressive NPO: Non-profit organisations predominantly involved in expressive activities, which include programmes focused on sports and recreation, arts and culture, interest representation, and advocacy.

FATF: Financial Action Task Force.

FIU: Financial intelligence unit.

Foreign fighters:	Unpaid individuals who are noncitizens of conflict states who join insurgencies during civil conflicts. In the contemporary context, these individuals are often radicalised in their home country and take advantage of underground networks to facilitate their travel into a civil conflict.[1]
Foreign partners:	A foreign entity assisting an NPO in carrying out activities or programmes abroad.
Foreign partner agencies:	National security, law enforcement, or regulatory agencies who exchange information with domestic agencies.
FSRB:	FATF-style regional body.
Humanitarian:	In this report, humanitarian refers to the promotion of human welfare and is not limited to activities undertaken following emergency or disaster situations.
Intent:	The desire of an entity to do harm. (In the context of this report, the desire to abuse the NPO sector to support terrorism or terrorist entities.)
Localised terrorist actor:	Refers to i) citizens or legal residents of a country engage in terrorist activities within or from their home country, sometimes influenced by foreign actors. It should be noted that this influence could range from formal to inspirational. ii) individuals or small groups who have not been actively recruited by a terrorist organisation and who engage in terrorist activity on their own initiative in furtherance of a terrorist cause.
Mandatory NPO reporting:	Reporting that NPOs are required to submit to regulatory or oversight bodies. This includes financial statements, programme information, information on activities, and other information used for regulatory or administrative enforcement purposes.
Money laundering	The processing of criminal proceeds to disguise their illegal origin. This process enables criminals to enjoy their profits without jeopardizing their source.
MSB:	Money services business.
National NPO regulator:	National oversight body responsible for the regulation of national NPOs and the enforcement of standards across the national NPO sector.
National security information:	Intelligence or other sensitive information regarding threats to the security of a state or its citizens. National security intelligence can be derived from open, semi-open, or clandestine sources.
NPO:	Non-profit organisation.

[1] This definition draws on: Hegghammer, Thomas (2013), p. 1; Malet, David (2013), p. 9

NPO representative:	In this report, NPO representative refers to an employee, volunteer, or another individual acting in an official capacity representing an NPO.
NRC:	Norwegian Refugee Council.
OCHA:	United Nations Office of the Coordinator of Humanitarian Affairs.
Passive recruitment:	The recruitment of individuals by terrorist organisations through indirect means, often through different types of media, with the intention of instigating activities on the behalf of the terrorist organisation by those individuals.
Proscribed Terrorist Entities (also commonly termed 'listed' entities):	Individuals or organisations on national or international lists of actors known to be engaged in terrorist activities.
Recruitment:	The processes, both active and passive, through which terrorist entities seek to enlist operational personnel.
Risk Indicator:	In this report, risk indicator is an aspect of an NPO's activities that suggests abuse or risk of abuse that may be terrorism-related, but also has possible alternative explanations.
Resources:	Includes financial and non-financial NPO assets, including donations, property, gifts-in-kind, personnel, and documentation.
Risk:	A function of three factors: threat, vulnerability and consequence.
Service NPO:	Non-profit organisations predominantly involved in service activities, which include the programmes focused on housing, social services, education, and health care.[2]
Strategic shock:	In the context of this report, a strategic shock is an event that causes a spike in demand for NPO funds or services. Major natural disasters, such as the 2004 Indian Ocean tsunami, are an example of a strategic shock.
Front organisation:	A legal entity created and controlled by a second organisation with the intent of masking illegal operations.
Supporter:	An individual not actively engaged in terrorist acts, but actively engaged in supporting terrorist entities.
STR:	Suspicious Transaction Report(ing). This includes suspicious activity reports and other forms of reporting from financial organisations relating to suspicious activities of clients.
Syphoning transactions:	The diversion of funds by external actors where a portion of the funds raised by an NPO, for a charitable purpose, is intercepted and diverted to a terrorist organisation for different purposes.

[2] Adapted from Salamon, Lester M.,. *et al* (2013) p.5.

Terrorist entity:	In the context of this report, a terrorist entity refers to a terrorist and/or terrorist organisation identified as a supporter of terrorism by national or international sanctions lists, or assessed by a jurisdiction as active in terrorist activity.
Terrorism financing:	The financing of terrorist acts, and of terrorists and terrorist organisations.
Threat:	A person or group of people, object or activity, with the potential to cause harm. Threat is contingent on actors that possess both the *capability* and the *intent* to do harm.
Trans-national organised crime:	International grouping of individuals who carry out criminal actions for financial profit.
Violent extremism:	Rigid adherence to an ideological set of religious or political beliefs that propagate violence.
Vulnerability:	Things that can be exploited by the threat or that may support or facilitate its activities. Vulnerability in the NPO sector can exist at either the organisational or sectoral level.
Terrorist abuse indicator:	In this report, a warning indicator is an aspect of an NPO's activities that suggests abuse or a risk of abuse that is directly related to terrorist activity. The presence of these indicators would lead to the rejection of alternative explanations for the risk that are not terrorism-related.

TERRORIST GROUPS MENTIONED IN REPORT

Organisation Name	Acronym Used in Report	Principal Area of Operations
Al Qaeda	AQ	Transnational
Liberation Tigers of Tamil Eelam	LTTE	Sri Lanka with transnational networks
Islamic State of Iraq and al Sham / Islamic State of Iraq and Syria	ISIS / ISIL	Iraq and Syria
Jabhat al Nusra	JN	Syria
Al Shabaab	AS	Somalia and East Africa
Al Qaeda in the Islamic Maghreb	AQIM	North Africa
Hizballah		Lebanon with transnational networks

Organisation Name	Acronym Used in Report	Principal Area of Operations
Hamas		The Palestinian territories with transnational networks
The Caucasus Emirate	IK	Russia
Fuerzas Armadas Revolucionarias de Colombia	FARC	Colombia

EXECUTIVE SUMMARY

1. In October 2001, the Financial Action Task Force drafted eight special recommendations pertaining to terrorist financing in response to a changing threat environment that had culminated in the attacks made on September 11th of that year. Originally labelled as Special Recommendation VIII (SR VIII), the current Recommendation 8, states the following:

> *Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:*
>
> *(a) by terrorist organisations posing as legitimate entities;*
>
> *(b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and*
>
> *(c) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.*

2. While non-profit organisations (NPOs), like their for-profit counterparts, face numerous risks relating to both money laundering and terrorist financing, SR VIII was designed to address specific terrorist financing vulnerabilities and threats faced by NPOs. When the 40 Recommendations were revised in 2012, the FATF integrated the majority of the Special Recommendations on terrorist financing into the general recommendations that address both anti-money laundering (AML) activities and activities meant to counter the financing of terrorism (CFT). The FATF did, however, recognize that three Recommendations remained unique to terrorist financing and grouped them together in Section C of the Recommendations; former SRVIII, now Recommendation 8 (Measures to Prevent the Misuse of Non-profit Organisations), was one of these three. This typologies report represents a significant step forward in understanding the terrorist threat to the NPO sector. Several important findings emerged from the analysis of 102 case studies submitted by FATF member states or compiled from open sources as well as current research on the threat environment. These findings can be summarised as follows:

> ***Key Finding 1:*** *The NPO sector has interconnected vulnerabilities, and terrorist entities seek to exploit more than one type of vulnerability. In the cases analysed for this project, the diversion of NPO funds by terrorist entities was a dominant method of abuse. However, other types of non-financial abuse such as the abuse of programmes, or the support for recruitment, also appeared regularly.*

> ***Key Finding 2:*** *The NPOs most at risk appear to be those engaged in 'service' activities, and that operate in a close proximity to an active terrorist threat. This may refer to an NPO operating in an area of conflict where there is an active terrorist threat. However, this may also refer to an NPO that operates domestically, but within a population that is actively targeted by a terrorist movement for support and cover. In both cases the key variable of risk is not geographic, but the proximity to an active threat.*

Key Finding 3: *Because of the nature of the threat and the resulting nature of state responses, cases of substantial risk are an important source of information for typologies analysis.*

Key Finding 4: *The amalgamation of many types of information held by different actors was an important factor in the detection of cases of abuse or in the identification of substantial risk.*

Key Finding 5: *Disruption of abuse, or the mitigation of substantial risk, was dealt with through multiple means including, but not limited to, criminal prosecution. Administrative enforcement, financial penalties, and targeted financial sanctions play important roles in disruption of abuse.*

UNDERSTANDING THE RISK

3. The third round of FATF evaluations assessing jurisdictions' compliance with the 40 Recommendations found that 57 percent of evaluated states were not compliant or only partially compliant with the current Recommendation 8, while only five percent of states were fully compliant or largely compliant with the Recommendation. A recent study conducted by the Center for Global Counterterrorism Cooperation and the United Nations Counter-Terrorism Committee Executive Directorate identified in its key findings that the level of understanding of the risk to the NPO sector was uneven globally.[3] This finding further highlights the need for a more thorough examination of the threat posed to the NPO sector by terrorist entities in order to increase understanding and awareness of both the threat and risk mitigation best practices.

4. The importance of the NPO sector to the global community cannot be overstated. It is a vibrant sector, providing innumerable services to millions of people. However, this typologies project found that more than a decade after the abuse of NPOs by terrorists and terrorist organisations (hereafter referred to as terrorist entities) was formally recognised as a concern, the terrorism threat to the sector remains, and the sector continues to be misused and exploited by terrorist organisations through a variety of means. The exploitation of a sector devoted to good works by entities intent on harming innocents is a particularly egregious form of abuse that fundamentally undermines public trust in the NPO sector.

5. The NPO sector has responded considerably to these demands by developing several different standards and initiatives to help individual organisations ensure accountability and transparency in their operations. Yet terrorist actors will often employ deception to mask their activities, particularly those outside areas of conflict. The case studies analysed for this report indicate that well-planned deceptions are difficult to penetrate with the resources available to non-governmental actors, making state-based oversight and its capabilities an equally necessary element to detecting the most sophisticated threats to the sector's activities.

6. In the 12 years since the text of Recommendation 8 was first drafted, the threat environment and the NPO sector itself have continued to evolve. Also, states and NPOs now have several years of experience implementing the Recommendation. This experience has prompted new questions about

[3] Center on Global Counterterrorism Cooperation, *et al* (2013), *p.*v.

how best to prevent terrorist abuse of the NPO sector. In response to these questions, this report identifies some important strategic issues facing the NPO sector and national and international policymakers in an effort to highlight issues for future discussions.

SCOPE OF THE PROJECT

7. This typologies project was *analytic* in nature, and not an evaluation of current policy. As such, the report does not recommend policy action, but examines and explains the threat to the NPO sector from terrorist entities, the drivers for this threat, the vulnerabilities in the sector, and complexities facing stakeholder responses. This typologies report examines the abuse of the NPO sector through a wide lens because the activities, and therefore vulnerabilities, of the sector extend beyond its financial flows to include material support. Ultimately, to understand financial vulnerabilities in the sector, it is necessary to understand other interrelated vulnerabilities. The abuse of the NPO sector by terrorists or terrorist organisations raises a number of complex strategic issues, including tension between humanitarian[4] assistance and counterterrorism measures as well as national responses to the international standard. It is not the intent of this report to discuss these issues in great length or recommend solutions, but to identify these strategic issues and provide an analytic foundation for further deliberations.

8. It is important to note that 102 case studies is a substantial number for a typologies report; however, the case study sample is not exhaustive and is determined by the voluntary response of FATF member states and FATF-style regional bodies (FSRBs). The focus of the typologies report was to draw out internationally applicable findings, which, naturally, means that they may not reflect characteristics specific to national jurisdictions. Also, the case studies are likely shaped by the mandates of their originating agencies be they law enforcement, FIU, regulator, etc., and specific risks addressed in national jurisdictions.

NATURE OF THE THREAT

9. Given that Recommendation 8 is one of the recommendations considered unique to CFT efforts, and given the recognition amongst specialists that terrorism financing is an activity distinct from money laundering, it was also necessary to clarify differences between terrorism financing and money laundering. Particularly, the research and analysis needed to clarify how these differences impact the NPO sector, the analysis of abuse in the sector, and ultimately efforts to protect the sector. Terrorism, by its very nature, is a risk for which prevention is paramount and, particularly true in the case of the NPO sector, terrorism financing is a part of a wider picture of threat. Operational case studies have demonstrated that terrorist financiers engaged in the logistical support of terrorist organisations use funds to meet broad logistical requirements, which include but are not limited to, recruitment, travel and the acquiring of weapons. The Interpretive Note for Recommendation 8 recognises this, stating that terrorist and terrorist organisations "exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support

[4] Humanitarian refers to the promotion of human welfare and is not limited to activities undertaken following emergency or disaster situations.

terrorist organisations and operations."[5] The Interpretive Note goes on to state that one of the general principles of the Recommendation is that:

> *Measures adopted by countries to identify and take effective action against NPOs that either are exploited by, or actively support, terrorists or terrorist organisations should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support.*[6]

10. The goal in terrorism financing investigations[7] is to understand threats and vulnerabilities *before* a risk becomes a reality and take preventive action. Threats must be understood and halted before they can exploit vulnerabilities because of the violent and indiscriminate harm inflicted on the public if a terrorist act is committed. Therefore, unlike money laundering investigations that are predominantly enforcement-led and are focused by a predicate offense, terrorism financing investigations are intelligence-led. Given that TF investigations are not focused on a predicate offense, investigators or analysts must rely on a larger set of indicators to make sense of terrorist financing activity. This is especially true when investigators or analysts are trying to understand a subject's intent or level of complicity.

MITIGATING THE RISK

11. Because there is a focus on preventing a terrorist act in terrorist financing cases, instances of abuse or substantial risk are often dealt with through a variety of non-prosecutorial measures, including

- preventive education,
- self-regulation by the sector,
- the designation of individuals and organisations who are or who support terrorist entities, or
- law enforcement action.

Many of these measures will occur prior to the case progressing to a level warranting criminal prosecution. In cases where foreign organisations are abusing or may abuse domestic NPOs, prosecution may not be a viable option, making the application of targeted financial sanctions on domestic or foreign entities an alternative method of protecting domestic NPOs.[8] In the case studies

5 Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), *p.*54.

6 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), *p.*55.

7 Used in the context of this report, the term 'investigation' does not differentiate between a criminal investigation and an administrative or intelligence investigation. This is because the combination of organisations and mandates involved in terrorism cases vary across jurisdictions, and can involve some or all of these aspects depending on the case.

8 Sanctioning as per FATF Recommendation 6 'Targeted Financial Sanctions Related to Terrorism and Terrorist Financing.'

analysed for this report, 88% of known disruption involved an element of administrative action or the designation of entities as terrorists or supporters of terrorism, while 25% of known disruption took the form of criminal charges or prosecution.[9] Therefore, as it is necessary to manage the risk of terrorist financing in the NPO sector early, and to fully understand the vulnerabilities in the sector it is essential to analyse cases of risk as well as cases of abuse.

12. The Interpretive Note to Recommendation 8 states that while the protection of the NPO sector is vital, measures taken to protect the sector "should not disrupt or discourage legitimate charitable activities." The case studies analysed for this report show a range of methods for detecting and disrupting abuse, mixing risk mitigation and disruption of existing abuse. In many instances, successful disruption and mitigation was achieved through the use of targeted regulatory measures based on numerous sources of information and specialised analysis examining NPO programmes and activities. While the overall impact of these disruptions on the sector is difficult to quantify, the analysis supports the idea that targeted intervention based on nuanced analysis lessens the overall impact on the sector's legitimate ongoing operations.

CATEGORIES OF RISK

13. The examination of the available case studies and literature identified five categories of abuse or risk. These are not mutually exclusive categories; many could be seen simultaneously throughout the case studies analysed for this report.

- The *diversion of funds* was a significant method that focused on the substantial financial resources within the sector. Actors inside an NPO, or external actors such as foreign partners, were responsible for the diversion.
- In other cases of abuse, NPOs or directing officials maintained an *affiliation with a terrorist entity,* either knowingly or unknowingly. In these instances, an NPO could be abused for multiple purposes, including general logistical support to the terrorist entity.
- In several cases, NPOs were abused to provide *support to recruitment* efforts by terrorist entities.
- NPOs were also targeted for *abuse of programming*. In these instances, the flow of resources was legitimate, but NPO programmes were abused at the point of delivery.
- Finally, some terrorist entities abused the NPO sector through *false representation*. In these instances, terrorist entities started 'sham' NPOs or falsely represented themselves as the agents of 'good works' in order to deceive donors into providing support.

14. One of the significant questions facing the stakeholders of Recommendation 8 is how to assess which NPOs are most at risk of abuse. The case studies analysed for this report indicated that there is

[9] As addressed in Chapter 5 of this report, because some case studies incorporated more than one type of disruption activity, the percentages do not add to 100%.

a correlation between the types of activities an NPO is engaged in, and the risk of abuse. The majority of the 102 case studies dealt with NPOs engaged in 'service activities' (housing, social services, education, or health care).[10] None of the case studies submitted dealt with NPOs engaged in 'expressive activities' (sports and recreation, arts and culture, interest representation, or advocacy.)[11] Additionally, the case studies and available research indicate there is a stronger risk of abuse for NPOs carrying out activities in populations that are also targeted by terrorist movements for support. Importantly, this does not always correspond to geographic areas of conflict or low-governance. In areas of conflict or low-governance where terrorist movements do not or cannot operate, NPOs may face risks associated with corruption or criminality, but not necessarily terrorism. Conversely, terrorist movements may actively target populations within relatively stable environments for support. For example, the Liberation Tigers of Tamil Eelam (LTTE) targeted Sri Lankan communities within several stable states for both financial and other forms of support. NPOs operating in these stable environments are therefore still at a higher risk. Ultimately, the principal considerations for determining which NPOs are at a higher risk of abuse are the value of their resources or activities to terrorist entities, and the proximity to an active terrorist threat that has the capability and intent to abuse NPOs.

DETECTION AND DISRUPTION

15. The project also examined what types of information led authorities to identify instances of abuse or substantial risk, and what information was used throughout subsequent investigations. The case studies that included the most detailed information, and hence the most nuance, were often built on information provided to regulatory agencies who have, as part of their mandate, the oversight of the NPO sector. However, in cases where complicit organisations relied on deception to mislead donors and other NPOs, the use of national security information to breach this deception was important in protecting the sector as a whole.

16. Case studies showed that, following the detection of abuse or substantial risk in the NPO sector, and depending on the severity of the case, a variety of means resulted in disruption or mitigation. In instances where a criminal threshold had already been crossed, criminal prosecutions were relied on to halt abuse. The use of administrative means and targeted financial sanctions to protect the NPO sector included a wide range of alternative measures that could result in the loss of legitimacy and donor incentives for targeted organisations without affecting the larger operations of the sector. Administrative measures, including targeted sanctions, often include procedures to challenge the administrative decisions as well as other due process elements. This analysis indicates that a wide range of options is available to protect the sector from abuse, and that criminal prosecution is often reserved for the minority of cases that cannot be dealt with through other means.

10 Salamon, Lester M., *et al* (2013), p.5.

11 *Ibid.*

INDICATORS

17. The analysis of the literature and case studies also yielded two types of indicators that could help the NPO sector, government actors, financial institutions, and designated non-financial businesses or professions (DNFBPs) identify and determine the nature of abuse in NPOs. The first type of indicator, termed 'risk indicators,' suggests compliance problems that may or may not be terrorism-related and, while still important in identifying at-risk organisations, may be explained by other forms of abuse. A second set of indicators has a much stronger correlation to abuse by terrorist entities. These indicators have been termed 'terrorist abuse indicators,' as they indicate the presence of terrorism more strongly and provide a warning function to government organisations or NPO directing officials.

NEXT STEPS

18. This report represents a substantial increase in our understanding of the threat posed by terrorist entities to the NPO sector; however, there remains a need to build on this understanding through future research and analysis. For instance, there is a need for national-level studies of abuse in order to increase our understanding of individual jurisdictions, particularly those at a higher risk of terrorist activity. This type of study is already supported under FATF Recommendation 1, which requires a national risk assessment be completed by all member states. Through these studies, unique indicators can be determined and further correlations can be examined. A more nuanced understanding of national risks will likely aid in overcoming some concerns in the sector that NPOs are overly regulated based on inaccurate assessments of risk. Additionally, there is a need to better understand the different threats (in terms of both risks and vulnerabilities) between jurisdictions that are net beneficiaries of NPO services and jurisdictions that are net donors. While this report represents a deeper understanding of the expenditure of NPO resources to guard against diversion, threats related to the source of NPO resources is still not well understood. Further research and analysis should be considered relating to risks and abuses associated with the source of NPO resources related to terrorist financing.

19. Addressing the threat posed to NPOs by terrorist entities requires understanding of the environment that NPOs operate in, the vulnerabilities present in the sector, how terrorist entities seek to exploit these vulnerabilities, and how threats to the sector have been detected and managed. Any future discussions about how best to prevent terrorist abuse of the NPO sector, particularly the strategic issues highlighted in this report, require a nuanced analytic foundation. The complexities inherent in Recommendation 8 have been, and will remain, difficult to navigate. However, if these complexities are not properly navigated, the integrity of the NPO sector will remain at risk. This typologies report aims to provide the necessary analytic foundation to national and international policymakers and the NPO sector, helping them to navigating these complexities, and thus ensuring that the NPO sector's good works can continue to benefit those who truly need them.

CHAPTER 1
INTRODUCTION

BACKGROUND

20. Non-profit organisations (NPOs) are a vibrant and integral part of the contemporary global environment and play a significant role in combatting terrorism.[12] The wide range, geographic reach, and operational endurance of their activities arguably make NPOs unique among international actors. While there is currently no data as to the number of NPOs operating globally, one study of the national NPO sectors of 35 countries indicated the scale and importance of NPO activity. A report by the Johns Hopkins Comparative Non-profit Sector Project published in 2003 determined that by the late 1990s, the 35 national sectors represented a USD 1.5 trillion industry, which is equivalent to the world's seventh largest economy, and encompasses over 39 million full-time equivalent workers.[13] A limited update published in 2013 that examined 16 jurisdictions noted that the non-profit sector accounted for an average of 7.4% of the total workforce, and 4.5% of gross domestic product (GDP) in the jurisdictions for which there was full data available.[14] The NPO sector is also an integral partner for the public sector in implementing shared initiatives, such as the UN Millennium Development Goals. The NPO sector has also traditionally enjoyed substantial public trust, which has been one of the basic components to the sector's success. The maintenance of this public trust is integral to the continued effectiveness of the NPO sector.

21. However, the concept of carrying out good works has been a target for those whose goals are not purely benevolent. The most extreme threat of abuse is posed by those engaged in terrorist activity. While the vast majority of NPOs work tirelessly to better the lives of people around the world, a small number of organisations and individuals have taken advantage of the NPO sector for the most contrary of reasons: to support those who engage in terrorism or support to terrorist organisations. The abuse of NPOs to finance or materially support terrorism may seem to be a risk with low probability, yet the impact of these activities is particularly acute for both the victims of terrorism and those who *should* benefit from the good works of NPOs. This immediate impact is multiplied when one considers the loss of public confidence in the integrity of the NPO sector.[15] A typologies report by the Asia/Pacific Group on Money Laundering (APG) examined this issue from a regional perspective, and FATF typologies reports in 2003 and 2007 included dedicated sections on

---

12 *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/23/39 (United Nations General Assembly, 2013) p.9. The Special Rapporteur's report states: "Fundamentally, the Special Rapporteur believes civil society organisations play a significant role in combatting terrorism. By their direct connections with the population and their prodigious work in, inter alia, poverty reduction, peacebuilding, humanitarian assistance, human rights and social justice, including in politically complex environments, civil society play a crucial role against the threat of terrorism".

13 Salamon, Lester M., *et al* (2003), *pp*.13-15.

14 Salamon, Lester M., *et al* (2013), *pp*. 2-3.

15 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), p.54.

the abuse of NPOs for terrorist purposes.[16] A substantial World Bank policy report also addressed the issue of terrorist financing through the NPO sector, with a particular focus on the question of what constituted a proportionate response.[17] However, since 2001, there has been no dedicated typologies report examining abuse, or the risk of abuse, of the NPO sector by terrorist entities. While the APG report and previous FATF typologies reports have provided first steps towards this kind of examination, there remained a need for a dedicated, wider-ranging, and more current international typologies report addressing the NPO sector. This need has been made all the more acute by the shifts in the threat environment since a Recommendation addressing NPOs (currently Recommendation 8, referred to hereafter as R.8) was first included in the FATF remit in 2001. There have also been concerns voiced by international organisations, research organisations, and the NPO sector itself regarding the balance between counter-terrorism measures and the effectiveness of NPO operations, particularly humanitarian action.[18] Ultimately, there has been a need for an international analytic report to examine, in a policy-neutral way, several core questions relating to the abuse of the NPO sector for purposes of supporting terrorism and terrorist entities. *Figure 1.1* illustrates these core questions.

Figure 1.1: **Key Research Questions**

Who…	…are the NPOs that are most at risk of abuse from terrorist entities?
What…	…is the nature of the threat posed by terrorist entities to the NPO sector?
When…	…are NPOs most at risk of abuse by terrorist entities?
Where…	…are NPOs most at risk of abuse by terrorist entities?
Why…	…are NPOs at risk of abuse by terrorist entities?
How…	…are NPOs vulnerable to terrorist activity? …do terrorist entities abuse the NPO sector? …have cases of abuse been detected and disrupted?

22. This report begins to address these core questions. While the bulk of any typologies report will be focused on the 'how' questions, it is necessary to address, to the extent possible, the other core questions in order to provide full analysis of the risk to the NPO sector and the challenges inherent in mitigating that risk.

SCOPE AND OBJECTIVES

16 Asia/Pacific Group on Money Laundering [APG] (2011), FATF (2003, 2008). A typologies report on abuse of the NPO sector for money laundering was also produced by the Eurasian Group (Eurasian Group on Combating Money Laundering and Financing of Terrorism [EAG], 2012).

17 Van der Does de Willebois, Emile (2010).

18 Mackintosh, Kate and Duplat, Patrick (2013).

23. The 40 Recommendations of the Financial Action Task Force (FATF) make special reference to the NPO sector as both vulnerable and valuable in Recommendation 8 (formerly Special Recommendation VIII) which expresses that member states should act to ensure that NPOs are not abused for the purposes of financing terrorist activity.[19] This recommendation was one of eight special recommendations[20] formulated in October 2001, in the wake of the September 11, 2001 terrorist attacks, to expressly combat terrorism because of several cases that demonstrated the use of NPOs to support terrorist organisations.

24. Recommendation 8 and its interpretive note is the cornerstone of the FATF's action to prevent, detect, and disrupt the abuse of the NPO sector for terrorism financing purposes. However, the FATF toolkit also includes several other Recommendations that have a bearing on the scope of this report and should be considered in conjunction with R.8. Recommendation 1 outlines the importance of risk-based approach to CFT in order to match mitigation efforts to identified risks in an efficient manner.[21] For the study of the NPO sector, R.1 indicates that the identification of substantial risk, as well as abuse, is an important effort.

25. Recommendation 5, which recommends the criminalising of terrorism financing, states that members should "criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts."[22] R.5 recognises that stopping support for terrorist entities includes stopping financing intended for non-military purposes such as recruitment.

26. Recommendation 6, addressing the use of targeted financial sanctions in CFT, states that sanctions should ensure that "funds or other assets" should not be made available "directly or indirectly" to an organisation or individual designated as a supporter of terrorism under international or national sanctions lists.[23] R.6, in the context of NPOs, highlights that funds are not the only means of transferring value to terrorist entities. Goods-in-kind provided indirectly to a terrorist entity can have the same impact as the direct transfer of funds. As NPOs have engaged in many activities that involve the transfer of value through more than just funds, this element of R.6 continues to be important to the scope of this study.

27. Recommendations 24 and 25 pertain to transparency and beneficial ownership of legal persons and arrangements.[24] Both recommendations state that "adequate, accurate and timely information" should be maintained on the beneficial ownership of legal persons and legal arrangements, and that this information "can be obtained or accessed in a timely fashion by competent authorities."[25] Recommendations 24 and 25 indicate the importance of general transparency and good-governance in any legal person, including NPOs.

---

19 Recommendation 8, in FATF (2012a), *p*.13.

20 A ninth special recommendation on cash couriers was added later.

21 Recommendation 1, in FATF (2012a), *p*. 11.

22 *Ibid.* p.13.

23 Recommendation 6, in FATF (2012a), *p*.13.

24 Recommendation 24 and 25, in FATF (2012a), *p*.22.

25 *Ibid.*

28. Quite apart from the FATF standards, countries are also bound by international human rights standards, such as the International Covenant on Civil and Political Rights (Article 22) that protect the freedom of association.

29. This multi-faceted approach is the backdrop against which the various case studies presented in this typologies report have been analysed. As a result, R.8 does not limit itself to a narrow definition of terrorism financing, but also focuses on what is described as material support--as outlined in the FATF definition of 'funds and other assets,' which includes "financial assets, economic resources, property of every kind."

30. As the title suggests, the purpose of this typologies report is to examine the risk of terrorist abuse in the non-profit organisation (NPO) sector. It is clear from a review of the third round of evaluations that states remain challenged in their ability to demonstrate compliance with R.8. While this report aims to aid in raising the level of awareness of some of the issues which R.8 is designed to address, this typologies report is not intended to comment on, nor be limited by, the scope of R.8. This report is also not meant to advance any policy recommendations but rather the purpose of the report is to provide an analytical foundation for future policy deliberations at the national and international levels.

31. As in all FATF typologies reports, the objectives of this typologies report follow closely from the Key Research Questions outlined in Figure 1.1 related to the relevant sector, and can be expressed as follows:

> ***Objective 1:*** To examine the contemporary terrorist threat environment and its impact on the NPO sector.
>
> ***Objective 2:*** To provide an analysis of how and where NPOs are vulnerable to abuse by terrorist entities both at the level of individual organisations, and the sectoral level, primarily based on demonstrated cases of abuse and substantial risk as provided by law enforcement and other government actors.
>
> ***Objective 3:*** To derive operational typologies, trends, and indicators of abuse that will further our knowledge of the threat to the NPO sector by terrorist entities, and note key strategic issues for future policy discussions.

32. These objectives are not mutually exclusive, but are in fact interdependent. Analysing how abuse occurs at the operational-level is important in answering the 'how' questions found in *Figure 1.1*. However, operational-level analysis does not adequately answer several larger questions such as why, and under what circumstances, terrorist entities seek to exploit the NPO sector. Answering these larger questions requires strategic-level analysis of the terrorist threat and the NPO sector. This typologies report incorporates both operational- and strategic-level analysis in an effort to begin to answer these questions, and provide the fullest understanding of abuse possible to date.

THE TERRORISM SUPPORT CONTINUUM

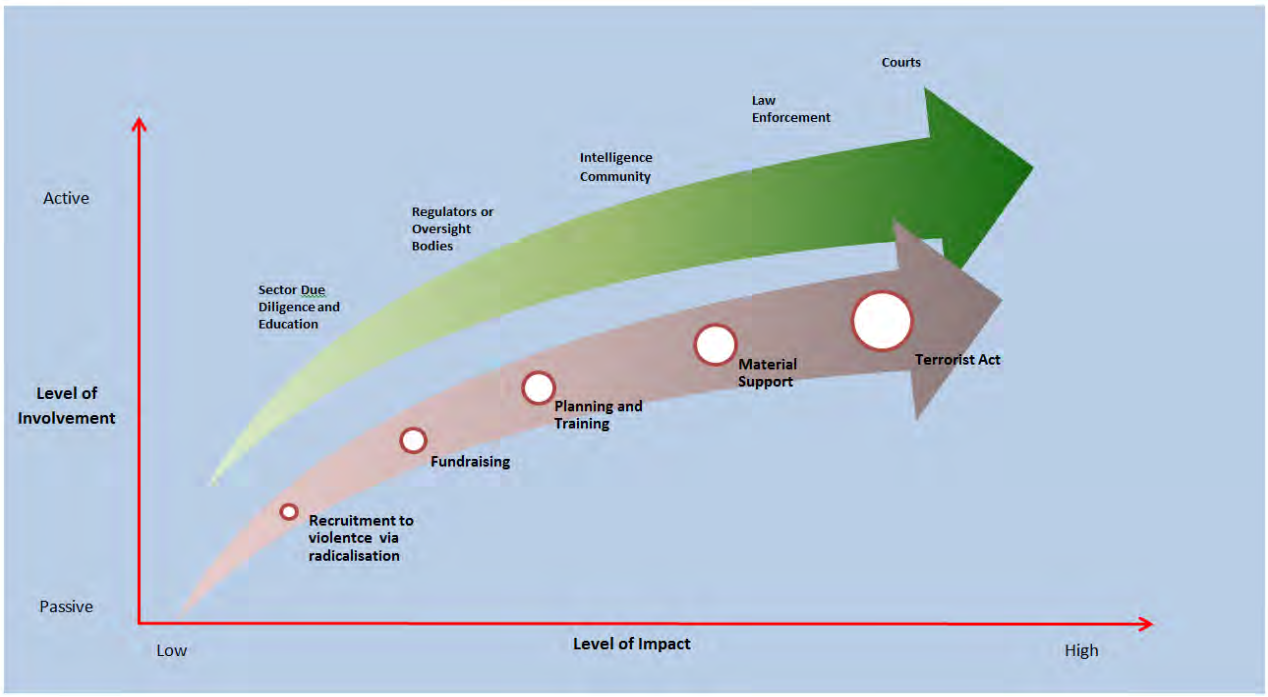
33. Behind any act of terrorism is a logistical trail that can encompass many different elements from recruitment of supporters to the provision of materials. Each element is not necessarily of the same severity, and therefore many jurisdictions approach each element differently. This can be envisioned as a terrorism support continuum, as illustrated in *Figure 1.2*. Dr. Timothy Wittig of the University of Amsterdam has argued that terrorism financing (and wider support to terrorist movements) cannot be separated from its socio-political roots and therefore should be viewed as a continuum.[26]

34. In the continuum presented here, which is operationally focused, a number of support activities, under the general headings recruitment, fundraising, planning and training, and material support, contribute towards a terrorist act. Along the continuum, as terrorist support activities build in impact and intent, different actors become involved in detecting and disrupting the support activities. At the low end of the continuum, the most important actors are the NPOs themselves, along with donors, beneficiaries, and any regulatory or oversight bodies that oversee the sector. With robust due diligence and sector safeguards, this is where much of the risk to the sector will be mitigated. However, some threats will persist along the continuum, employing deception techniques that can be difficult for the NPO sector itself, or even regulatory agencies, to address. In these cases, the sector's own due diligence activities or the investigations of regulatory agencies are augmented by financial intelligence units (FIUs) and other intelligence actors who can penetrate more sophisticated attempts to abuse the sector. At the most severe end of the continuum, the mitigation efforts of the sector and the detection abilities of intelligence organisations are reinforced by the enforcement and prosecution powers of law enforcement agencies and the judicial system, which are necessary to punish ongoing abuse and deter future occurrences.

35. It is important to note that the linear feel of the terrorism support continuum is for illustrative purposes; neither terrorism nor efforts to disrupt it proceed so neatly. The types of support to terrorism indicated in *Figure 1.2* may not always occur in the order illustrated, but are likely to occur in parallel at several points. Correspondingly, the involvement of actors who investigate and mitigate terrorist abuse will not be as linear as illustrated, but will often take place concurrently. Operationally, as indicated in the majority of the case studies analysed for this report, mitigation of abuse is often achieved through the coordinated activities of a number of different actors.

[26] Wittig, Timothy (2011), *pp*.141-58.

Figure 1.2: **The Terrorism Support Continuum**



36. What the terrorism support continuum indicates is that disruption of terrorist support activities, including terrorism financing, is often occurring *prior* to the stage of criminal prosecution through multiple, often simultaneous methods. In light of this, in order to gain a proper and complete understanding of the risk to the sector, the study of NPO abuse must be based on cases drawn from along this continuum, rather than simply at the high end when a case is prosecuted.

TERRORISM FINANCING VERSUS MONEY LAUNDERING: METHODS AND RISKS

37. The terrorism support continuum illustrates a subtle but important conceptual difference between money laundering and terrorism financing that is important in order to understand this typologies work. The FATF *Financial Investigations Guidance* recognises that terrorism financing and money laundering, while often appearing together, are actually operationally different. The *Guidance* states, "money laundering is the process of making dirty money appear clean whereas terrorist financing most often involves clean money being utilised for nefarious purposes."[27] Put another way, money laundering deals with the proceeds of serious crime; it occurs as the result of a criminal act. Conversely, terrorism financing, while in itself a criminal act in most jurisdictions, enables serious criminal acts; efforts to disrupt it are meant to *prevent* future terrorist activities. This is not to say that there is no convergence between TF and other forms of financial crime, including money laundering. In fact, past FATF typologies, and other research examining the resourcing of terrorist movements, have highlighted the terrorism-criminal nexus.[28] The result however is that the investigation of money laundering tends to be law enforcement-led and principally about gathering

27 FATF (2012b), *p.*15.

28 FATF (2008).

evidence in order to prosecute the offenders of already-committed crimes. Terrorism financing investigations, on the other hand, are required by the nature of the threat to be preventive in nature and intelligence-led.

38. Once funds[29] end up in the hands of terrorist entities, it is more difficult to disrupt their eventual use. Terrorism financing is a lower-probability occurrence, but one that can have a higher public impact if it enables a terrorist attack. Strategically, money laundering also has a high impact on a society over time. However, the immediate impact of terrorist activity (specifically the very visible human cost) generates a different public threat calculation. Therefore, many jurisdictions need to mitigate the risk of terrorist financing earlier than would be the case for money laundering because the immediate public impact is substantially higher.

39. Ultimately, the goal in terrorism financing investigations is to understand threats and vulnerabilities *before* a risk becomes reality. Malcolm Sparrow, in his book *The Regulatory Craft*, identifies preventive analysis as a key component of risk mitigation.[30] Threats must be assessed and understood before they can exploit vulnerabilities. It is, therefore, necessary to analyse cases of risk as well as cases of abuse. As such, case studies illustrating both abuse and unacceptable risk are included in the analysis for this report.

DATA COLLECTION AND SOURCES

40. Research for this typologies report was conducted through multiple methods. The core of the research effort was the collection and analysis of case studies drawn mainly from FATF member states, but also through open-source research. Information on larger investigatory trends was also collected from FATF member states, including information on detection methods and interagency cooperation.

41. One of the principal aims of this typologies project was to involve the NPO sector throughout the research process. To this end, NPO sector organisations were consulted formally through questionnaires and workshops that included multiple stakeholders. The questionnaires and the workshops were designed to gain a better understanding of the sector's operations and vulnerabilities to abuse by terrorist entities, as well as how NPOs themselves viewed the risk from terrorist activities.

42. As in any analytic product, there are methodological parameters that must be kept in mind when considering the findings. The focus of the typologies report was to draw out internationally applicable findings. To this end, FATF member states and FATF-style regional bodies submitted 102 case studies, a substantial number for a typologies report but nevertheless not exhaustive. Furthermore, the voluntary response of FATF member states and FSRBs determined the range of cases available for the typologies report. Case studies were also likely influenced by the mandates of the agencies that provided them and the specific risks addressed in the relevant national jurisdictions.

---

29 Referring to funds drawn from legitimate or illegitimate enterprises.

30 Sparrow, Malcolm K (2000), *pp.*265-69.

COLLECTION OF CASE STUDIES

43. A request for case studies was distributed to FATF member states and FATF-style regional bodies (FSRBs) through the FATF secretariat. The request outlined the Terrorism Support Continuum and contained sample cases to assist respondents in selecting, formatting, and sanitising case studies. In response to this request, 14 states submitted a total of 102 case studies to the project team. Geographically, the case study sample spans Europe, North America, Africa, the Middle East, South East Asia, and Oceania. Additionally, case studies originated from different agencies, such as law enforcement, intelligence, and regulatory agencies.

44. Both sanitised and unsanitised case studies have been included in this report, in an effort to capture the benefits of both approaches. The majority of the case studies obtained from member states and FSRBs were sanitised before being submitted to the project team for the following reasons:

1. **Protecting the integrity of NPOs:** In many cases, legitimate NPOs involved in cases of abuse are still operating and providing valuable services. The identification of these NPOs, much like the identification of victims of crimes, could have unintended detrimental consequences.
2. **Lack of consensus regarding the specifics of which entities are deemed to be terrorists:** While there is relative consensus on the high-level understanding of what constitutes terrorist actions, consensus breaks down in debates over whether some movements or entities warrant the label of 'terrorist.' Often, these debates are driven by different perspectives and interpretations of national threat environments. These debates, while important, should not detract from the overall goal of understanding how and why terrorist entities abuse the NPO sector to further violent aims.
3. **Ongoing cases:** Terrorism financing investigations and prosecutions are often long processes. In order to provide a more current analysis, the project team needed to ensure that states were comfortable providing case studies of ongoing cases. In instances where cases are in the investigation phase, it is necessary to protect the integrity of those investigations to ensure operational sources and methods are not compromised. In instances where cases are in the prosecutory phase, it is legally necessary to protect the identities of those individuals or organisations involved.
4. **Disruptions using administrative measures:** Given the need to mitigate risk, many cases of TF abuse in the NPO sector are handled through administrative measures, rather than through criminal prosecutions. As discussed earlier, it is necessary to capture these cases in order to provide the most robust analysis. However, cases handled through administrative measures are not often identified as terrorism-related. The subsequent identification of these cases as terrorism-related could undermine administrative processes as an effective tool for risk mitigation.
5. **The use of national security intelligence:** Because of the nature of terrorism investigations, many cases involve sensitive intelligence information that states have an interest in protecting. In some instances, the compromising of sources or methods could

put individuals or organisations at further risk. In order to ensure that states were comfortable sharing the widest range of case study information, it was necessary to ensure the protection of detailed information concerning investigative capabilities, techniques, or sources.

45. In addition to the sanitised case studies, unsanitised cases have the advantage of increasing understanding by providing more easily recognisable examples of abuse. Unsanitised case studies also allow for the inclusion of additional details available in open sources such as court documents, research reports, official government publications, and media reporting. As such, unsanitised case studies have been included throughout this report where the case in question is a completed criminal prosecution, or the necessary information is already available in the public domain.

COLLECTION OF GENERAL JURISDICTIONAL DATA

46. In the request for case studies distributed to FATF member states and FSRBs, respondents were also asked a number of general questions about the risks that terrorist financing activity posed to their national NPO sector. These questions aimed to elicit information regarding:

- Statistical data collected through any NPO sector reviews, specifically data relating to what types of NPOs are most at risk.
- Findings from any national risk assessments that incorporated the NPO sector.
- Information pertaining to NPOs that are the subjects of financial transaction reporting.

47. This information is incorporated into the chapters of the typologies report addressing the NPO environment, methods of abuse, and methods of detection.

NPO SECTOR QUESTIONNAIRES AND WORKSHOPS

48. As stated previously, an important point for the project team was that the NPO sector should be consistently involved in the research process. A questionnaire was distributed to NPO sector organisations, which asked for the sector's input on several key points, including:

- How respondents view the risk to their organisation(s) from terrorist activity;
- Whether respondents consider their organisation(s) vulnerable to abuse by terrorist entities, and if so, through what vulnerabilities;
- Whether respondents have been involved in, or are aware of, instances where the NPO sector has been abused by terrorist entities;
- Identifying risk-mitigation measures designed by individual organisations, or collectively within the NPO sector.

49. NPO sector representatives also conducted a parallel review, which included their own survey of NPOs.

50. Two workshops with NPO sector organisations, organized by The Charity and Security Network and the European Foundation Centre, took place in New York and Brussels. The goal of these workshops was to foster a wider-ranging and ongoing discussion between national and international government actors, and the NPO sector, regarding a range of issues relevant to the typologies report, including:

- The NPO sector's concerns regarding operational independence and effectiveness;
- The NPO sector's concerns over some national responses to Recommendation 8; and
- The impact of counter-terrorism measures as part of wider compliance and due diligence demands.

51. Because many of these issues are part of wider policy discussions, it is not in the purview of the typologies report to draw conclusions one way or another. However, the workshops were very useful in determining the larger strategic issues that needed to be highlighted by the typologies report. The information obtained through the FATF-led questionnaire, the review conducted by sector representatives, and the workshops was incorporated principally into the aspects of Chapter 2 that address sector vulnerabilities and risk mitigation measures.

OPEN-SOURCE RESEARCH

52. Substantial open-source research informed every aspect of the research process. In addition to the open-source research used to compile un-sanitised case studies, publications by academic researchers, research institutes, and governments were used to assess trends in the NPO sector and the terrorist threat. In all cases, open-source material was assessed for its reliability and rigour by the project team before being incorporated into the source material for the final report.

53. Overall, in spite of the analytic limitations addressed earlier, the body of information, analysis, and findings of this typologies report represents a significant increase in our understanding of the risk posed by terrorist financing activity to the NPO sector, and should help to guide future discussions regarding how best to protect the NPO sector from abuse by terrorist entities.

CHAPTER 2
THE NPO SECTOR AND THE RISK OF TERRORIST ABUSE

THE GLOBAL ENVIRONMENT

54. Globalisation has increased environmental uncertainty for both legitimate and illegitimate international actors, presenting, at the same time, substantial opportunities and substantial risks.[31] For NPOs, technological advancements have expanded fundraising and promotional capacity and have made it easier to coordinate programmes. Interconnected financial and transportation networks have made it easier to transfer funds or goods around the world to branch offices, partner organisations, or directly to beneficiaries. Concurrently, globalisation has increased demands on NPOs, particularly those engaged in humanitarian operations, drawing them into unstable areas where the integrity of their operations are at risk, or changing the risk at a local level.

55. NPOs, being legitimate international actors, can easily capture many operational advantages from globalisation, including:

- Increased mobility;
- Interconnectedness of networks;
- Expanded and deepened access to areas of conflict or low-governance;
- Diversified financial services and logistical networks;
- Decentralised communications and management;
- Increased ability to engage the public.

56. Unfortunately, terrorists seek to capture these same advantages, albeit clandestinely. For instance, the resilience of the Al Qaeda network is largely due to its ability to decentralise its communications and management and diversify its logistical, financial, and recruitment networks. Similarly, the Liberation Tigers of Tamil Eelam (LTTE) ran its global logistics network through numerous subsidiary NPOs and charities. This globalised network of ostensibly humanitarian organisations was so resilient that it ultimately outlasted the LTTE's military wing. The legitimacy and breadth of NPO activities, combined with this overlap in operational needs, can present a tempting target for terrorists looking to realise the advantages inherent in a globalised environment. Ultimately, as different as their goals may be, terrorist networks and NPOs exist in the same global environment, often attempting to reach the same populations. Humanitarian NPOs often seek access to populations that are tied to local or foreign conflict in order to carry out good works; terrorist movements seek access to these same populations in order to exacerbate the forces of conflict or attempt to find sympathetic cover. These parallel attempts to access populations can ultimately

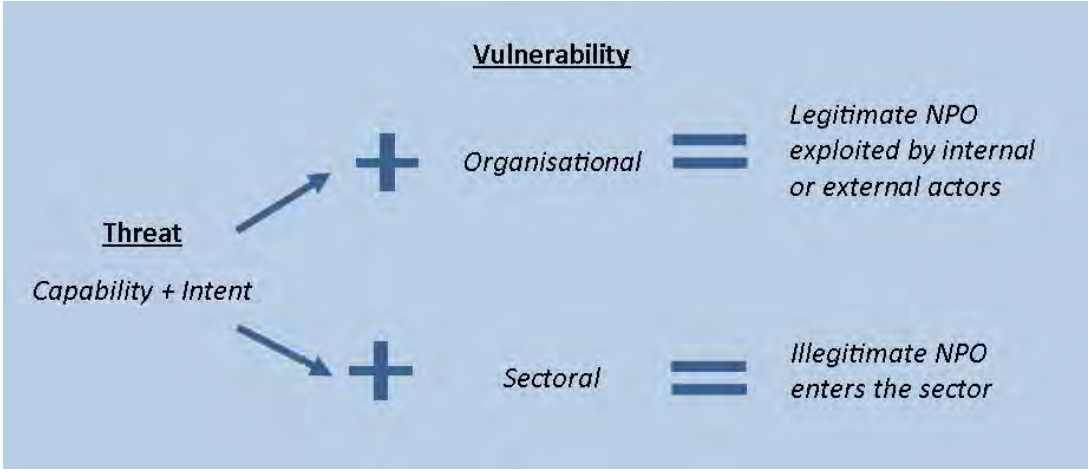
[31] On major global trends, see National Intelligence Council (2012); Development, Concepts, and Doctrine Centre (2013).

bring NPOs into greater proximity to a terrorist threat and has on occasion led to NPO personnel being kidnapped and held for ransom[32].

57. An abuse of the NPO sector in order to finance or otherwise support terrorist activity is, ultimately, the result of a threat actor successfully exploiting vulnerabilities. A **threat** is defined by FATF as "a person or group of people, object or activity, with the potential to cause harm."[33] Additionally, threat is dependent on actors that possess both the *capability* and *intent* to do harm, in this case towards the NPO sector.[34] A terrorist organisation may have the capability to abuse NPOs, for instance by controlling a geographic area where the NPO operates, but may have decided for strategic reasons not to target humanitarian actors. Conversely, a terrorist organisation may have the intent to abuse the NPO sector, for instance through creating an illegitimate NPO to raise funds, but does not have sufficient personnel to maintain the NPO, leaving it without a necessary capability. Both of the situations above pose a **risk**[35] to the NPO sector and would require continued monitoring, but it is only after intent and capability are realised in tandem that an active threat exists.

58. **Vulnerabilities** can exist at the organisational level or at the sectoral level, and have been defined by FATF as "things that can be exploited by the threat or that may support or facilitate its activities."[36] Organisational vulnerabilities are seen in cases where legitimate NPOs are abused by external actors or deceived by internal actors. Sectoral vulnerabilities are seen in cases where illegitimate organisations (commonly referred to as 'sham' NPOs) are allowed to enter the sector and take advantage of its benefits. *Figure 2.1* illustrates the relationship between threat, vulnerability, and abuse of the NPO sector.

Figure 2.1: **Threat and Vulnerability**



32 For instance, see SwissInfo (2014)

33 FATF (2013a), *p.*7.

34 On the components of threat, see Smith, Clifton and Brooks, David J (2013), *p.* 64.

35 Risk is defined by the FATF as "a function of three factors: threat, vulnerability and consequence." See *FATF* (2013a), *p.*7.

36 FATF (2013), *p.*7.

59. The case studies analysed in this report illustrate operational abuse, or significant risk of abuse, in the NPO sector. To adequately understand how abuse occurs, however, it is necessary to assess both the vulnerabilities of the NPO sector and trends in the terrorist threat at the strategic level. The convergence of the terrorist threat, the NPO sector, and national or international governance also raises several issues that pose substantial questions for policymakers. In surveying these issues, this report does not make policy recommendations. Instead, this report seeks to provide an analytical foundation for future policy deliberations at the national or international level.

THE NON-PROFIT SECTOR

60. One of the inherent challenges in assessing the risk of terrorist abuse in the NPO sector is defining what a non-profit organisation is, and more importantly, which of these organisations are most at risk. The FATF has defined a non-profit organisation in its Interpretive Note to Recommendation 8 as "a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or the carrying out of other types of 'good works.'"[37] The FATF has also stated in its Best Practices guidance for R.8 that measures to combat TF activity in the NPO sector should "apply to NPOs which account for 1) a significant portion of the financial resources under control of the sector; and 2) a substantial share of the sector's international activities."[38] However, there is still uncertainty within the NPO sector regarding the most appropriate target of risk mitigation efforts.[39]

61. The case studies analysed for this report, both those submitted by states and those available through open-source research, indicate that those NPOs most at risk of abuse for TF are engaged in particular types of activities. One substantial study done by Johns Hopkins University's Centre for Civil Society Studies provides a useful classification of NPO activities that helps narrow down those organisations most at risk. The report lists eight types of activities carried out by NPOs which are then split between two general categories.[40] *Figure 2.2* illustrates the eight activity types, and two general categories.

Figure 2.2: **NPO Activity Types**

Service Activities	Expressive Activities
Housing	Sports and Recreation
Social Services	Arts and Culture
Education	Interest Representation
Health Care	Advocacy

Source: Salamon, Lester M., *et al* (2013), p.5.

37 'Interpretive Note to Recommendation 8 in FATF (2012a), *p*.58.

38 FATF (2013b), *p*.4.

39 Response by NPO sector umbrella organisation to FATF NPO Sector Questionnaire, February 2014.

40 Salamon, Lester M., *et al* (2013) p.5. It is also recommended that readers look at the *International Classification of Non-Profit Organisations* (ICNPO) for a more detailed breakdown of these activity types.

62. *Figure 2.3* indicates the number of times service and expressive activities were identified as the principal activity of NPOs in the case studies submitted for this report. However, many submissions did not specify the activities of NPOs in enough detail to differentiate activity types.

Figure 2.3: **NPO Activity Categories Observed in Case Studies**[1]

Number of times service activities were identified as principal NPO activity	Number of times expressive activities were identified as principal NPO activity	Number of cases where principal NPO activity type could not be identified
64 [2]	0	38

Notes:

1. Numbers will not add up to the total number of case studies because: 1) many cases did not identify the principle activities of the NPO in enough detail, and 2) many cases identified more than one type of principle activity per NPO, or more than one NPO was involved in the case study.
2. While religious NPOs may be considered expressive, certain programmes and activities conducted by religious organisations are often service-oriented. As such, many of the case studies involved the activities being conducted by religious organisations.

63. The same study noted that NPOs engaged in service activities account for an average of 73% of total gross added value generated by the NPO sector across the 14 states surveyed,[41] indicating that service activities account for the share and scope of the NPO sector that the FATF referred to in the R.8 Best Practices guidance. In the case studies analysed for this report, all the NPOs involved were principally engaged in service activities such as the humanitarian provision of housing, social services, cultural services,[42] education, and healthcare; none had expressive activities, such as interest representation and advocacy, as their primary focus. Therefore, based on available information, the conclusion emerges that 'service NPOs' are most frequently abused by terrorist movements.

64. For NPOs focused on service activities, globalisation has brought two conflicting proliferations. The end of the Cold War, which took with it the bipolar power balance developed over five decades, let loose many simmering tensions, resulting in new conflicts. At the same time, state actors trying to adapt to the new environment had difficulty addressing these conflicts and the resultant humanitarian demands through traditional means.[43] More generally, governments began to devolve the provision of many services to the private sector, including NPOs, in an effort to increase efficiency and decrease demands on the public purse. These developments resulted in a *proliferation of demands* on the NPO sector. At the same time however, the complexity of the global environment has resulted in a *growth of risk* to the sector's activities as terrorist groups, serious

41 This percentage is based on the breakdown of service versus expressive activities within the NPO sectors of the 14 states surveyed. The 14 states surveyed were Australia, Belgium, Brazil, Canada, Czech Republic, France, Israel, Japan, Kyrgyzstan, Mozambique, New Zealand, Norway, Portugal and Thailand.

42 'Cultural services' here refers to activities such as the maintenance of cultural centres.

43 On these trends, see Munro, Alan (1999)

organised criminal networks, and insurgencies have found new opportunities in areas struggling to build or evolve governance structures.

65. Due to similar drivers, safeguarding the integrity of operations has become a key requirement for most sectors with an international presence. Requirements to comply with anti-corruption legislation in several jurisdictions have driven investment in more sophisticated due diligence procedures in the business sector.[44] Similar compliance demands on the financial sector have arisen as a response to the growth of transnational organised crime and associated money laundering or counterfeiting operations. Due diligence compliance is also important for an increasing number of public sector activities, driven by developing international regimes such as human rights law.[45] New compliance requirements have come about for different reasons in different sectors, but, cumulatively, the growing complexity in the global environment has placed new demands on *all* legitimate international actors to safeguard the integrity and accountability of their operations.

66. The NPO sector has responded considerably to these demands by developing several different standards and initiatives to help individual organisations ensure accountability and transparency in their operations. *Figure 2.4* provides a list of some of the standards and initiatives, along with the organisations responsible for developing or maintaining them.

Figure 2.4: **Transparency Standards and Initiatives Developed by NPO Sector**

Standard or Initiative	Developing Organisation(s)
Principles of Conduct in Disaster Response Programmes	International Red Cross and Red Crescent Movement
The Do No Harm Handbook: The Framework for Analysing the Impact of Assistance on Conflict	Collaborative for Development Action, Inc.; CDA Collaborative Learning Projects
Private Voluntary Organization (PVO) Standards	InterAction
Humanitarian Accountability Partnership Standard	Humanitarian Accountability Partnership
Preventing Corruption in Humanitarian Operations Handbook of Good Practices	Transparency International
Humanitarian Charter and Minimum Standards in Humanitarian Response	The Sphere Project
Evaluation and Learning Activities	Active Learning Network for Accountability and Performance in Humanitarian Action

44 Bishop, Toby J.F. and Hydoski, Frank E. (2009).

45 De Schutter, Olivier, *et al* (2012).

Standard or Initiative	Developing Organisation(s)
Cycle of Collective Learning	Group URD
Emergency Capacity Building Project	Interagency Working Group on Emergency Capacity
People in Aid Code	People in Aid
Muslim Charity Forum	Human Appeal International; Human Relief Foundation; Islamic Relief; Muslim Aid; and Muslim Hands.
INEE Minimum Standards Handbook	International Network for Education in Emergencies
Enhancing Learning and Research in Humanitarian Assistance	Save the Children UK; Institute Bioforce; RedR; FrontlineSMS
Assessments and Monitoring Activities	Central Bureau on Fundraising
Peacebuilding Evaluation System	Alliance for Peacebuilding

Note: Adapted from a response to the FATF *NPO Sector Questionnaire*, February 2014.

67. The development of these types of standards and initiatives by the NPO sector is a vital step in ensuring the integrity of the sector's activities. Yet terrorist actors will often employ deception to mask their activities, particularly those outside areas of conflict. The case studies analysed for this report indicate that well-planned deceptions are difficult to penetrate with the resources available to non-governmental actors, making state-based oversight and its capabilities an equally necessary element to detecting the most sophisticated threats to the sector's activities. This is further explored in Chapter 4, which surveys how the case studies of abuse were detected.

NPO SECTOR OPERATIONS AND VULNERABILITIES

68. Before establishing how abuse can manifest itself in the NPO sector, it is necessary to have a model of NPO operations that is generally applicable, particularly to the service activity organisations as discussed earlier. The case studies analysed for this report, as well as available literature on NPOs, indicates that NPO operations can be reduced to five general elements (see *Figure 2.5*):

1. The *collection of resources* refers to any activity undertaken by an NPO to acquire resources either directly or through third parties such as volunteers.

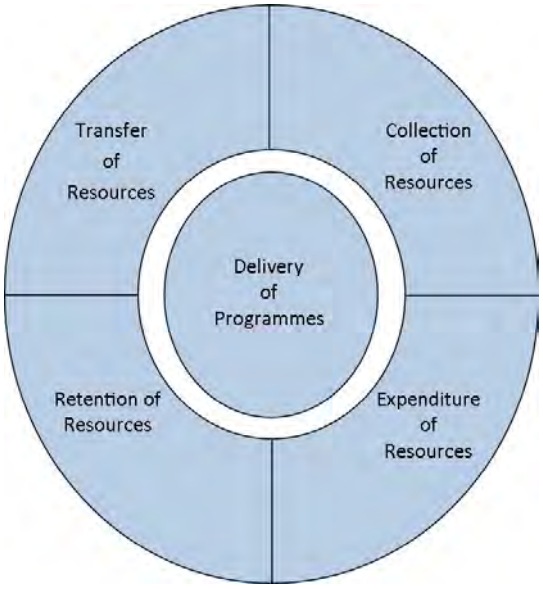
2. The *retention of resources* refers to the storage or maintenance of resources by an NPO. Retention includes activities ranging from the maintenance of funds within bank accounts to the management of property or facilities.

3. The *transfer of resources* can occur at multiple instances during NPO operations and refers to any point at which the resources of the NPO are transferred between different actors.

4. The *expenditure of resources* refers to any point at which an NPO's resources are exchanged in return for goods or services.

5. The *delivery of programmes* refers to the point at which an NPO is carrying out programme activities. This could include activities such as the distribution of aid, the provision of medical treatment, the holding of fundraising events, or the hosting of a guest speaker.

Figure 2.5: **General Model of NPO Operations**



69. The term 'resources' is used purposefully in order to include gifts-in-kind, or non-financial resources that hold value (such as property.) Also, these elements are not presented linearly because not all elements are included in an NPO programme all the time. For instance, if an NPO programme is managed entirely by the organisation's own staff, then it is not transferring resources. The different elements are not mutually exclusive, particularly when more than one NPO is involved.

70. Running through these elements are characteristics of the NPO sector that create vulnerabilities to abuse by terrorists. Conversely, however, these are also the characteristics that make the sector uniquely effective international actors. The vulnerabilities can be grouped within four overarching categories:

1. Extended logistical networks

Logistical networks are the linkages through which NPOs collect, retain, transfer, and deliver resources related to their operational activities. **Extended logistical networks** give the NPO sector greater reach, allowing NPOs to deliver programmes in multiple areas through multiple partners. Conversely, because of their scope, extended logistical networks also increase vulnerability. With more individuals, wider ranges of activities, and possibly substantial geographic distances involved, it can be challenging to maintain adequate control of resources. For NPOs engaged in humanitarian work, logistical networks often flow through geographic areas of conflict or low governance. Also, there is an increased risk that resources will have to flow through other sectors where governance may be less stringent (for

example, unregulated money businesses). Both of these aspects increase the risk that resources can be diverted or that the delivery of programmes can be corrupted.

2. *Large transitory workforces*

The NPO sector also relies heavily on a **large transitory workforce**. Volunteers make up a significant and important portion of this workforce. A major comparative study of 22 countries estimated that NPO activity accounted for 19 million full-time equivalent employees. The addition of volunteer workers brings this estimate to 29 million.[46] However, the nature of the NPO sector workforce can make it difficult to scrutinise staff, particularly volunteers or foreign partners.[47] Additionally, for small- and medium-sized NPOs, this type of workforce can make it difficult to attract and retain personnel that have technical expertise in risk assessment, compliance, and legal matters. These personnel pressures can lead to NPO activities going forward without adequate due diligence and safeguards in place, increasing the risk of abuse.

3. *Operational capacity*

The NPO sector also possesses **high operational capacity**.[48] The FATF has already noted that NPOs may be vulnerable because they "have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity."[49] The case studies and available literature on NPO abuse appear to support this finding. The NPO sector is resource intensive and transnational in nature. These resources and associated logistical networks are valuable to terrorist movements if they can be exploited. Also, NPOs have a unique ability to reach people, particularly those in conflict areas or Diasporas. Exploiting this unique access presents terrorist movements with an opportunity to recruit for their movements through the abuse of NPO resources and programmes.

A further important aspect of the operational capacity of NPOs is the public trust afforded to the sector. Because the sector has generally enjoyed high public trust, scrutiny of NPO activities has often been less consistent and robust than in other sectors. For terrorist entities looking to minimise risk to their own operations and logistical networks, piggybacking on, or mimicking, legitimate NPOs has presented an attractive solution.

---

46 Salamon, Lester M. *et al* (1999), *pp*.9-10.

47 The scrutiny of staff refers to performing due diligence on staff in order to support wider transparency and accountability measures, including counter-terrorism.

48 This is true for the sector cumulatively, and particularly for larger organisations. Smaller NPOs, while possessing less capacity overall, still may have capacity that is disproportionate to their size through the use of networks and innovative approaches to activities.

49 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), p.54.

4. *Organisational culture*

The final area of vulnerability has to do with **organisational culture**. This aspect was explained in a response to the NPO sector questionnaires, where the respondent indicated that the emphasis placed on values in some NPOs could contribute to poor decision-making and risk management.[50] Studies have examined the importance of values in non-profit organisations, and identified that for some organisations, value calculations represent the real 'bottom line.'[51] While this is not a consistent vulnerability, the tendency to trust external and internal actors may leave some NPOs vulnerable to abuse.

THE CURRENT NATURE OF THE TERRORIST THREAT

71. Like most threats, terrorism is not static. To adequately assess the threat to the NPO sector it is necessary to examine the current trends in terrorism and to understand how and when terrorist entities may interact with the NPO sector. Terrorist entities adapt their networks and strategies to suit changing environments. For instance, the loss of Afghanistan as a safe haven forced Al Qaeda (AQ) to decentralise, relying more on regional affiliates and dispersed leadership networks.[52] The decentralisation or fragmentation of significant groups such as Al Qaeda or the Liberation Tigers of Tamil Eelam (LTTE) has complicated terrorist networks within the threat environment. However, the most challenging evolution in the terrorist threat has been the strategic emphasis placed on local cells or individuals who have engaged in terrorist activity on their own initiative.[53]

72. Easily recognisable hierarchical organisations have become less central now that calls for donations of funds or related material supporting terrorism can be made to a general audience through the internet. The internet has been widely used by terrorist movements to facilitate many aspects of their operations, including fundraising and recruitment to support terrorism or terrorist organisations.[54]

73. The increased ability of terrorist movements to motivate individuals indirectly, without concrete chains of command, has led to a slow but noticeable growth in **localised terrorist actors**.[55] This term refers to citizens or legal residents of a country who engage in terrorist activities within or from their home country, sometimes influenced by foreign actors. It also refers to individuals or small groups who have not been actively recruited by a terrorist organisation but who engage in

50 Submission in response to *NPO Sector Questionnaire*, December 2013.

51 On the role of values and organisational culture, see Tonkiss, F. and Pacey, A (1999), pp.257-74; Anheier, Helmut K. (2000).

52 Regional affiliates of the AQ movement include Al Qaeda in the Arabian Peninsula (AQAP) operating principally out of Yemen, Al Shabaab in East Africa, and Al Qaeda in the Islamic Maghreb (AQIM) in North and West Africa.

53 AQ and its affiliates, such as al Shabaab, have repeatedly tried to capitalise on homegrown and self-starter actors. For instance, see SITE Monitoring Service (2014).

54 United Nations Office on Drugs and Crime (2012), *pp*.3-12; Von Behr, Ines; Reding, Anais; Edwards, Charlie and Gribbon, Luke (2013).

55 See Jenkins, Brian Michael (2011); Precht, Tomas (2007).

terrorist activity on their own initiative in furtherance of a terrorist cause.[56] The important aspect of this trend is that recruitment, logistical support (including financing), and attacks can occur locally with minimal and indirect interaction with formal organisations.

Localised terrorist actors: Refers to

i) citizens or legal residents of a country engage in terrorist activities within or from their home country, sometimes influenced (ranging from formally to inspirationally) by foreign actors.

ii) individuals or small groups who have not been actively recruited by a terrorist organisation and who engage in terrorist activity on their own initiative in furtherance of a terrorist cause.

Examples of terrorist acts involving localised terrorist actors include:

- Various plots and actions by the Hofstad Network in the Netherlands from 2003-2005.
- The July 7, 2005 suicide bombings in London.
- The attack on Glasgow airport in 2007.

74. Taken as a function of the overall strategic positioning of terrorist movements, the development of localised terrorist actors represents a significant and influential aspect of the threat environment. For instance, the concept of 'leaderless resistance,' has featured frequently in the al Qaeda movement's principal media publication, *Inspire*, which is widely available online.[57] Also, because of the inherent difficulty in detecting domestic, self-selected and generally autonomous actors, these plots have resulted in a number of successful attacks in states that have otherwise been difficult for external actors to operate in.[58]

75. While the decentralisation of networks and a reliance on localised actors have taken on a new importance, the international threat posed by more formal organisations has still proven very relevant and is often the inspiration for localised terrorist actors. Recent activity indicates that terrorist organisations will still seek to finance and resource traditional paramilitary capabilities.[59] Given the parallel emphases placed on localised terrorist actors or networks and traditional terrorist organisations, the nature of the terrorist threat has not shifted from one to another, but has become

56 Sagemen, Marc (2008); Michael, George (2012).

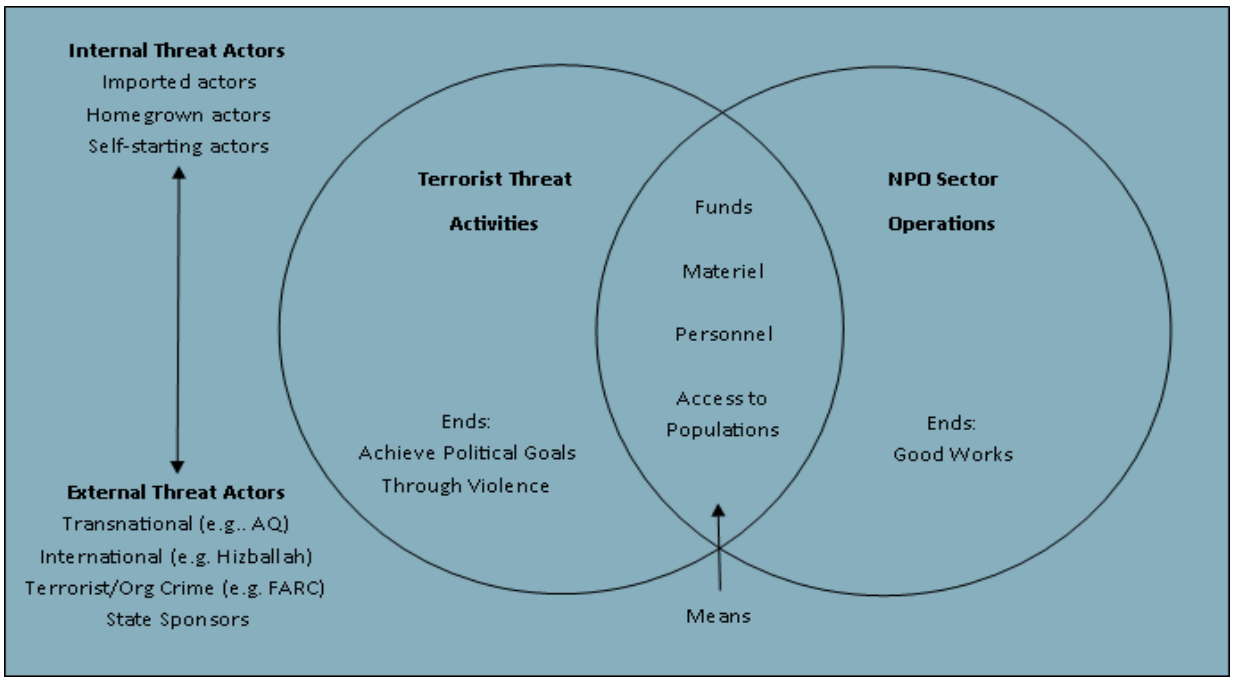
57 For instance, see the importance of Abu Musa'ab al Suri. Lia, Brynjar (2008); Samuels, David (2012); Stalinsky, Steven (2011).

58 Several home-grown plots have come to fruition, including: the bombings of the Boston Marathon in 2013; the killing of a UK serviceman in Woolwhich, London in 2013; the attacks on Oslo and Utoya by Anders Breivik in Norway in 2011; the Fort Hood shootings in 2009; the July 7 bombings bombings in London, UK, in 2005; and the killing of Theo Van Gogh in the Netherlands in 2004.

59 For instance, Al Shabaab's attack on Nairobi's Westgate shopping centre, the suicide bombings in Volgograd by militants connected to the Islamic Caucasus Emirate, AQIM's attack on the Tigantourine gas plant in Algeria in 2013, and Hizballah's continuing involvement in the Syrian conflict are illustrations of the more centralised terrorist organisation at work.

more varied. The 'foreign fighters'[60] phenomenon embodies this variation. Traditional terrorist organisations are engaged in active operations abroad and still represent a substantial threat.[61] Concurrently, homegrown violent extremists are making their way to these organisations as volunteers and engaging in terrorist attacks abroad.[62] This indicates a more symbiotic relationship between domestic and international threat actors. *Figure 2.6* attempts to illustrate some of these relationships. Terrorist networks and NPOs seek very different ends, but often rely on similar logistical capabilities, shown as 'means' in *Figure 2.6*, that are consistent through domestic or foreign operations. Funds, materiel, personnel, and public influence[63] are key resources for NPOs, but are also sought by domestic and foreign terrorist entities. As a result of their need for similar types of resources, legitimate and illegitimate actors can end up colliding, and this is not limited to international activities.

Figure 2.6: **The Terrorist Threat to NPOs**



TERRORIST ABUSE AND THE RISK TO NPOS

76. The trends in the terrorist threat environment raise the question of how terrorist abuse, and some specific forms of abuse such as terrorist financing (TF), are developing, and how this impacts the NPO sector. For instance, substantial attention to terrorism post-9/11 has driven some activities,

60 Individuals who travel abroad to take part in conflicts, usually because of an ideological affiliation (i.e. they are otherwise 'foreign' to the conflict).

61 Mohammed, Arsham and Zakaria, Tabassum (2013).

62 Hegghammer, Thomas (2013); Zelin, Aaron Y. (2013).

63 'Public influence' in this case refers to the ability to reach a particular public audience either physically through operational activities, or via messaging.

including terrorism financing, further underground, which raises the possibility that the cover afforded by legitimate organisations such as NPOs is more attractive to terrorist entities. Statistically reliable data is very difficult to obtain due to the opacity of terrorist support activities and the preventative nature of counter-terrorism efforts.[64] However, some broad trends can be discussed, particularly concerning terrorism financing.

77. The 2008 FATF report examining terrorist financing typologies identified that terrorist activity can often be locally self-financed through a variety of means.[65] Other examinations of contemporary TF trends note the decentralisation of terrorist movements and indicate that for local supporters of terrorism, self-financing based on locally available opportunities is increasingly a preferred strategy.[66] Localised TF corresponds to the operational strategies examined earlier for several important reasons:

1) Current terrorist strategies de-emphasise spectacular attacks, such as 9/11, in favour of a higher rate of less complex attacks. This makes localised TF a more viable strategy.[67]
2) Counter-terrorism measures have increased the risk of exposure in international TF activity. The international logistical networks of terrorist organisations are high-value assets that groups try to protect. Localised TF allows terrorist groups to insulate their core logistical networks from their operational networks.[68]
3) Localised TF allows terrorist supporters to exploit local opportunities. The supporters' existing networks become viable sources of funds from fraud, theft, narcotics sales, or even legitimate businesses.[69]

78. Available information regarding recent terrorist plots supports the idea that localised TF has become increasingly important, particularly in light of decentralization of terrorist movements.[70] For instance, the Madrid bombings of 2004 were financed by the sale of narcotics, using existing networks that one of the plotters already had access to.[71] The bombers who attacked the London transit system in 2005 financed their plot personally, using bank loans, credit cards, and savings.[72] Najibullah Zazi, who plotted suicide bombings on the New York transit system in 2009, used stolen credit cards to finance aspects of his group's plot.[73] In a case directly relevant to NPOs, a localised plot by UK-based terrorists to bomb targets in Birmingham in 2010 directly involved the abuse of

64 Similar difficulties have been cited in relation to other sources of TF, for instance counterfeiting. See Noble, Ronald K. (2003).

65 FATF (2008), *p.*14.

66 Napoleoni, Loretta (2013), *pp.*13-26; Pollinger, Zachary A. (2008).

67 Napoleoni, Loretta (2013), *pp.*13-26

68 Basile, Mark (2004), *pp.*169-85.

69 FATF (2008), *p.*4.

70 For a general overview, see Gomez, Juan Miguel del Cid (2010), *pp.*3-27.

71 Rollins, John; Wyler, Liana Sun; Rosen, Seth (2010), *pp.*19-20.

72 *Report of the Official Account of the Bombings in London on 7th July 2005*, HC 1087 (London: The Stationary Office, 2006) p.23.

73 Apuzzo, Matt and Goldman, Adam (2013), *p.*103.

two local charities in order to finance their domestic bomb plot. Because of its relevance to the abuse of the NPO sector for terrorist purposes, the Birmingham plot warrants more detailed explanation. The following case study was developed entirely from the open-source documents cited and was not developed from any state's response to the request for case studies. As with any open-source research, the veracity of the findings is directly related to the credibility of the sources.

Case Study 33

In 2011, West Midlands Police, in collaboration with the British Security Service and the London Metropolitan Police Service, began an investigation into several individuals based in Birmingham. [1] Two of the principal subjects of the investigation, Irfan Naseer and Irfan Khalid, had made trips to Pakistan in 2009 and 2010, where they had recorded suicide videos and attended training in preparation for terrorist activity.[2] Physical and technical surveillance of Naseer, Khalid, and co-plotter Ashik Ali uncovered a significant plot to detonate up to eight explosive devices in crowded places around Birmingham.

Physical surveillance revealed that Naseer, Khalid, and Ali were engaged in street fundraising for the large UK charity Muslim Aid.[3] Investigators found that the plotters had volunteered with Muslim Aid as fundraisers, obtaining donation buckets and high-visibility vests with the charity's name on them. The three men gathered donations over the course of a single day and had returned USD 2 500 in donations to Muslim Aid.

However, before returning the donation buckets and vests, and unbeknownst to Muslim Aid, the three men continued to fundraise for several more days posing as Muslim Aid volunteers. The donations collected over these subsequent days were deposited into the plotters' personal bank accounts. In total, they diverted USD 23 000[4] in donations to finance the bomb plot.[5] A similar scheme was also used to defraud a second charity, Madrasah-e-Ashraful Uloom.[6]

In September 2011, police disrupted the bomb plot, arresting Naseer, Khalid, Ali, and several other suspects. The three were convicted on terrorism charges in February 2013, and sentenced to prison terms ranging from 15 years to life.7

After the 2011 arrests, police made Muslim Aid aware that the organisation had been abused by the bomb plotters. Muslim Aid filed a serious incident report with the Charity Commission of England and Wales, which is the national regulator of charities in the UK.[8] The Commission worked with the charities involved to review and strengthen their safeguards to mitigate the risk of future abuses.

Notes:

1. Dodd, Vikram and Taylor, Richard Norton (2011); Birmingham Mail (2013).
2. LaVille, Sandra (2013).
3. Willets, John (2012).
4. For the purposes of consistency, all currencies in this report have been converted to US dollars (USD).
5. West Midlands Policy Counter-Terrorism Unit (2012).
6. Young, Nicki May (2013).
7. BBC (2013).
8. Young, Nicki May (2013).

79. The majority of case studies analysed for this report are transnational in nature, indicating that much of the risk to the NPO sector from terrorist abuse comes from international terrorist entities moving resources into or out of a state. However, the Birmingham plot discussed in Case 1 illustrates that localised abuse poses a risk to NPOs as well. Of the 102 case studies analysed, 21 cases included abuse or substantial risk of abuse that was domestically oriented, or where the antagonist was a domestic actor. Also, of these 21 cases, 14 occurred in countries that do not have substantial domestic terrorist or insurgent presence. Therefore, according to the cases available, it cannot be assumed that an NPO is risk-free because it is engaged in domestic activities in a relatively stable environment. This is not to say that all domestic NPOs face a substantial level of risk; what is important is that viewing the risk of abuse through the lens of geography could still allow for substantial risk to the sector.

80. The case studies analysed for this report indicated that there is a correlation between the types of activities an NPO is engaged in and the risk of abuse. As explained earlier in this chapter, all of the case studies where the principal activities of NPOs were identifiable dealt with NPOs engaged in 'service activities', none dealt with NPOs engaged in 'expressive activities'. Moreover, the case studies and available research indicate that there is a stronger risk of abuse for NPOs carrying out activities in populations that are also targeted by terrorist movements for support. Importantly, this does not always correspond to geographic areas of conflict or low-governance. In areas of conflict or low-governance where terrorist movements do not or cannot operate, NPOs may face risks associated with corruption or criminality, but not terrorism. Conversely, populations within relatively stable environments may still be actively targeted by terrorist movements for support. For example, Sri Lankan communities within several stable states have been targeted by the LTTE for both financial and other forms of support. NPOs operating in these stable environments are therefore still at a higher risk. Ultimately, the principal considerations for determining which NPOs are at a higher risk of abuse are the value of their resources or activities to terrorist entities, and the proximity to an active terrorist threat that has the capability and intent to abuse NPOs.

81. A second important consideration is the connection between terrorism financing and recruitment activity, and what this means for the risk of abuse in the NPO sector. The FATF has stated that "terrorists and terrorist organisations exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations."[74] In its guiding principles, the FATF also stated that "all should agree that [charity] does not include activities that directly or indirectly support either domestic or international terrorism."[75] The case studies analysed for this report indicate that NPO-funded programmes or facilities can be abused to promote recruitment by terrorist movements. Out of the 102 case studies analysed for this report, 27 included the abuse of the NPO sector to support recruitment by terrorist movements.

82. While it may seem at first glance that activities supporting recruitment are not linked to terrorism financing activities, there are important linkages. An NPO may have a legitimate educational programme, devote resources to it, and hire teachers, all of which are entirely legitimate

74 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), *p*.54.

75 FATF (2013b), *p*.6.

activities. However, if the teachers then engage in recruitment to terrorist causes, the educational programme and the resources devoted towards it become abused. In determining the threat posed to the NPO sector by external or internal actors, gauging intent is an important consideration as discussed earlier in the definition of a threat. The existence of activities or material that supports recruitment by terrorist movements is a signal that NPO funds are being, or are in danger of being, intentionally misappropriated. In short, recruitment-related activities are, in themselves, a form of support to terrorist organisations and often an indicator of a wider intent to support terrorism. Additionally, the existence of such activities or material can represent the exploitation of NPO programmes at the point of delivery.

STRATEGIC ISSUES

83. The abuse of the NPO sector by terrorist entities raises a number of complex strategic issues. It is not the intent of this report to discuss these issues in great length or recommend solutions, but to identify these strategic issues and provide an analytic foundation for further deliberations.

ISSUE 1—A TENSION CREATED BY EQUALLY NECESSARY IMPERATIVES

84. The importance of NPOs in the global community has been recognised by the FATF in the opening paragraphs of the interpretive note to Recommendation 8, which states "Non-profit organisations (NPOs) play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world."[76] Resulting from this, the FATF has clearly stated that measures taken to protect the NPO sector from abuse by terrorist entities "should not disrupt or discourage legitimate charitable activities."[77] However, some have raised concerns that counter-terrorism measures enacted nationally are having just such an impact on the operations of legitimate NPOs. A report jointly commissioned by the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and the Norwegian Refugee Council (NRC) argued that there have been structural, operational, and internal impacts to the NPO sector and individual organisations as a result of counter-terrorism (CT) measures.[78] Particularly, the OCHA/NRC report indicates that there is concern that CT measures result in a "distortion of the core humanitarian principle of impartiality," that CT measures create barriers to efficient delivery of aid, and that there has been significant additional administrative burdens placed on individual organisations.[79] There are also arguments at the national and international levels that some existing humanitarian exceptions in CT measures are inconsistent with other efforts to halt support to terrorist movements.[80] One of the more recent examinations of this issue was done by the Australian Independent National Security Legislation Monitor (INSLM), who pointed out that in several instances humanitarian exceptions were inconsistent with both the Australian Criminal Code and

76 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), p.54.

77 *Ibid.*

78 Mackintosh, Kate and Duplat, Patrick (2013), *pp*.102-114.

79 *Ibid.*

80 Independent National Security Legislation Monitor (2013), *pp*.77-85.

United Nations counter-terrorism resolutions. The INSLM argued that exceptions should only exist for high-capacity organisations with proven reliability such as the International Committee of the Red Cross or UN aid agencies.[81] This view is, in itself, a compromise position as the view of the FATF has been that humanitarian exceptions should be handled on a case-specific basis through national mechanisms such as licenses or approved exemptions.

85. Halting the flow of resources to terrorist organisations and ensuring humanitarian aid can reach those in need, are equally necessary endeavours. In the NPO sector, however, there is an inevitable tension between these two endeavours. On one hand, NPOs have a responsibility to help those in need in a neutral and timely manner. This imperative is embodied within the humanitarian principles as cited in the OCHA/NRC report. At the same time, NPOs also have an obligation to donors to ensure that money which was provided by citizens trusting it would be used towards benevolent causes, is not used for other purposes, *particularly* if that involves support to terrorist movements. Navigating this complex issue is an important consideration for the NPO sector, national governments, and international organisations. Based on the inherent linkages between these two equally necessary demands, there are challenges in separating the impact that one has on the other.

ISSUE 2—NATIONAL RESPONSES TO INTERNATIONAL STANDARDS

86. The standards set by international bodies such as the FATF are ultimately subject to implementation by national governments. This is necessary as different jurisdictions have to respond to particularities within their own NPO sectors, governance systems, and cultures. This idea is explicitly stated in the Interpretive Note and Best Practices paper for Recommendation 8.[82] However, there has been concern that some national responses to international standards have misused FATF recommendations to justify the abuse of civil society for political purposes, particularly to suppress dissent.[83] While in some instances these concerns pertain to states where there are pre-existing, known problems with the abuse of civil society, the possibility that R.8 could be abused to justify such activities cannot be ignored, and may undermine the legitimate purpose of the Recommendation.

87. In states where there is a risk that Recommendation 8 will be used to exacerbate systematic abuse of civil society, the protection of human rights is part of a broad-based discussion. Indeed, the United Nations General Assembly has identified violations of human rights, political exclusion, and related issues as "conditions conducive to the spread of terrorism."[84] One aspect of the discussion is

81 *Ibid.*

82 'Interpretive Note to Recommendation 8 (Non-Profit Organisations)' in FATF (2012a), *p*.55; FATF (2013b), p.6.

83 Carothers, Thomas and Brechenmacher, Saskia (2013); United Nations Human Rights (2012).

84 The UN Counter-Terrorism Strategy also encourages states to implement the FATF Recommendations. See *United Nations Global Counter-Terrorism Strategy*, A/RES/60/299, 2006. However, the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association has stated: "Unduly restrictive measures, which can lead donors to withdrawal support from associations operating in difficult environments, can in fact undermine invaluable [Civil Society Organisation] initiatives in the struggle against terrorism and extremism, and ultimately have adverse consequences on peace and security." *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/23/39 (United Nations General Assembly, 2013) p.9.

the state's international obligations *both* in terms of security standards and also the maintenance and protection of human rights. The other aspect of the discussion is the norm of national sovereignty which limits the extent to which international actors can dictate affairs at a national level. Simultaneously promoting the benefits of a vibrant civil society and the security provided by robust counter-terrorism measures is often the goal of international actors; but such simultaneous goals may not be shared by some national governments. In these cases, it is important to differentiate between the objectives of the international standard (in this case the FATF Recommendations) and the quality of national-level implementation of that standard.

CONCLUSION

88. In examining the threat posed by terrorism to the NPO sector, the vulnerabilities of the sector, and some of the significant strategic issues facing the international response, it becomes apparent that each is adaptive and evolving. The NPO sector plays a fundamental role on the international, national, and local levels. Both the integrity and efficacy of the sector is vital to its ability to continue to play such a valuable role. Concurrently, the decentralisation of terrorist movements has made it more difficult to monitor and disrupt activities, has created a more diverse range of threat actors, and has in some instances exacerbated the risk to parts of the NPO sector.

89. A strategic analysis of these developments indicates that there are numerous interconnected drivers at play. Often, these drivers are mutually reinforcing, but just as often they have inherent tensions between them. These drivers are summarised in *Figure 2.7*.

Figure 2.7: **Key Environmental Drivers**

Environmental Driver	Explanation
Driver 1: Necessity for effective CT measures because of damage caused by terrorist entities.	Driver 1 refers to the requirement for national and international governmental bodies to respond to the terrorist threat in order to protect civilians.
Driver 2: Operational efficacy of the NPO sector.	Driver 2 refers to the maintenance of the NPO sector's effectiveness and efficiency in the delivery of programmes and activities.
Driver 3: Duty to donors to maintain accountability in humanitarian operations.	Driver 3 refers to the duty of the NPO sector and other stakeholders to ensure that funds or materiel entrusted to the sector by donors are used for the purposes they were intended.
Driver 4: Duty to beneficiaries to provide assistance.	Driver 4 refers to the duty of the NPO sector and other stakeholders to ensure that assistance is provided to beneficiaries in a manner consistent with international humanitarian standards.
Driver 5: Collective action of	Driver 5 refers to the rules and standards set by

Environmental Driver	Explanation
international regimes	international bodies (such as the FATF 40 Recommendations) in an effort to ensure collective prosperity and security.
Driver 6: Independent action of national states	Driver 6 refers to the ability of a state to act in accordance with, or at odds with, international norms based on the state's status as a sovereign entity.

90. International efforts to counter terrorism and protect and promote the NPO sector ultimately navigate between all of these drivers. The goal of this typologies report is to provide the analytic map to help guide this navigation.

CHAPTER 3
METHODS AND RISK OF ABUSE

–A description of the methods and risks of terrorist abuse of the NPO sector identified through the analysis of case studies–

91. The main way in which the risk of terrorist abuse of the NPO sector can be understood is through the examination of case studies. While there is no question that the study of actual instances of abuse is important to gauge the extent of the problem, it is equally important to examine cases where the risk of terrorist abuse has been observed. Terrorism financing occurs in preparation for subsequent serious criminal acts, as opposed to money laundering which follows from serious criminal acts. Until the risk environment is fully understood, it will not be possible to implement measures to effectively address the risk of terrorist abuse of the NPO sector. For the purposes of this project, case studies include situations where risk has been identified, and subsequently mitigated, in addition to actual cases of abuse.

92. The case studies demonstrated several ways through which terrorist entities could abuse NPOs. *Figure 3.1* outlines these broad types of abuse and provides a definition of each.

Figure 3.1: **Methods and Risks of Abuse**

Methods and Risks of Abuse	
Diversion of Funds	An NPO, or an individual acting on behalf of an NPO, diverts funds to a known or suspected terrorist entity
Affiliation with a Terrorist Entity	An NPO, or an individual acting on behalf of NPO, maintains an operational affiliation with a terrorist organisation or supporter of terrorism
Abuse of Programming	NPO-funded programmes meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism
Support for Recruitment	NPO-funded programmes or facilities are used to create an environment which supports and/or promotes terrorism recruitment-related activities
False Representation and Sham NPOs	Under the guise of charitable activity, an organisation or individual raises funds and/or carries out other activities in support of terrorism

93. The frequency in which each category of methods and risks of abuse was observed can be summarized as follows:

Figure 3.2: **Methods and Risks of Abuse – Frequency Observed**

Methods and Risks of Abuse	Frequency Observed
Diversion of Funds	54%
Affiliation with a Terrorist Entity	45%
Abuse of Programming	10%
Support for Recruitment	26%
False Representation	14%

Note: Given that case studies often represented multiple methods of abuse and/or risk, the above breakdown of frequency does not add up 100%.

94. The case studies submitted in support of the project demonstrated that abuse and risk of terrorist abuse of the NPO sector was commonly the result of a lack of robust internal governance and/or appropriate external oversight. Additionally, just under half of the case studies involved some form of affiliation with a known terrorist entity or one suspected[85] of supporting terrorist activity, and the majority of NPOs that appeared in the case studies were legitimate organisations as opposed to 'sham' NPOs started purely for the purpose of supporting terrorist entities.

DIVERSION OF FUNDS

95. The most commonly observed method and risk of abuse of NPOs to support terrorism involves the diversion of funds. In this typology, funds raised by NPOs for humanitarian programmes—disaster relief, humanitarian relief, cultural centres, relief of poverty, advancement of education, advancement of religion—are diverted to support terrorism at some point through the NPO's business process. Essentially, the diversion of funds occurs when funds raised for charitable purposes are re-directed to a terrorist entity. Approximately half of the cases involve some element related to the diversion of funds.

96. Diversion of funds was seen at different stages of the NPO business process, such as during the collection and transfer phases. Diverted funds were used to support terrorist organisations, such as the financing of an organisation's infrastructure and its military operations. Cases included the procurement of munitions, equipment and communications devices, as well as the financial support of the families of terrorists. Cases identified that diverted funds were used to support terrorist individuals and organisations both domestically and abroad.

97. The diversion of funds typology can be divided into cases where the diversion was carried out by actors internal to the organisation as well as external to the organisation. Internal actors are

85 The term 'suspected' used throughout this report refers to instances where there is information or intelligence assessed as credible indicating an entity is supporting or engaged in terrorism.

named individuals of the NPO, such as directing officials and staff. External actors, however, are merely associated with the NPO as third-parties, such as fundraisers and foreign partners. In some cases, it was unclear whether or not the diversion of funds was carried out by actors internal or external to the NPO.

DIVERSION OF FUNDS BY ACTORS INTERNAL TO NPOS

98. Of the cases demonstrating the diversion of funds typology, an overwhelming majority involved actors internal to the NPO. Diversion of funds by internal actors occurs when a portion of the funds raised by an NPO, for a charitable purpose, is syphoned off and diverted to a terrorist organisation for different purposes. Cases analysed also demonstrated instances where funds raised by third-parties (ostensibly for charitable purposes) were channelled through the NPO to a terrorist organisation. The use of the NPO to facilitate such transactions has the effect of obscuring an audit trail, severing or distancing any link to a terrorist entity, and decreasing the likelihood of detection by authorities.

99. The case studies demonstrate that internal NPO actors are well positioned during the collection, retention, and transfer phases of NPO operations to divert funds for nefarious purposes using a variety of techniques. This particular vulnerability, paired with the threat of insiders who aspire to support terrorism, present considerable risk to the NPO sector. The severity of this risk is supported by the fact that almost half of all the cases submitted involved an element of diversion of funds by internal actors.

100. During the collection phase, diversion of funds involves the interception of cash prior to the deposits into NPO accounts, while during the retention and transfer phases, the funds are diverted by a variety of means, ultimately ending up in the control of terrorist organisations. Cases involving the diversion of funds by internal NPO actors demonstrate that the following means are used:

- wire transfers;
- cash transactions and cash couriers;
- unrelated persons and personal accounts;
- unrelated businesses and business accounts;
- money services businesses; and/or
- travellers' cheques and cashiers' cheques.

101. The following case involves an NPO directing official taking cash donations intended for the NPO and depositing them into an unrelated company account. From there, the funds were believed to be transferred to a foreign terrorist organisation.

Case Study 11

Diversion of Funds by Actors Internal to NPOs

Collection Phase

A domestic company was established with very broad commercial purposes. Numerous small deposits were made to the company's account by the individual who had signing authority on the account. The funds were immediately transferred to foreign-based companies.

An investigation by the national FIU revealed that the individual with signing authority on the company's account was also a directing official of an NPO. It was suspected that the small deposits made on the company's account originated from fundraising by the NPO.

Law enforcement information indicated that the NPO was known to have ties to a terrorist group. A second directing official of the NPO, who was also a manager of the company, also had ties to the terrorist group.

The investigation concluded that the domestic company was a front company being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

102. In another case, NPO officials willingly worked with foreign organisations in controlled areas that were suspected of supporting terrorism in order to gain access and provide humanitarian assistance.

Case Study 32

Diversion of Funds by Actors Internal to NPOs

Transfer Phase

A domestic NPO was established to provide a place of religious worship for a diaspora community that had come from an area of conflict, and to raise and disburse funds for humanitarian causes.

The national NPO regulator became suspicious when the NPO's mandatory reporting indicated that it had sent funds to organisations that were not legally prescribed beneficiaries. These funds were sent ostensibly in response to a natural disaster that had affected the diaspora community's homeland. One of the beneficiary organisations, however, was believed to be the domestic branch of an international front organisation for a foreign terrorist group operating in the diaspora community's homeland.

The regulator audited the NPO and discovered that it had sent funds to five organisations or individuals that were not legally prescribed beneficiaries. This included USD 50 000 sent to the international front organisation through the domestic branch, and USD 80 000 sent directly to the front organisation's headquarters branch located in the area of conflict.

While the audit was ongoing, the regulator received two leads from the public regarding the NPO. Both leads cited concerns regarding the opacity of the NPO's leadership, and that decisions to send funds overseas had circumvented normal accountability procedures set out in the NPO's governing

documents. One of the leads indicated that a shift in the demographic of the diaspora community had meant a new faction had gained control of the NPO's board of directors. This faction was more sympathetic to the cause of the foreign terrorist organisation. While these issues had already been noted through the regulator's audit, the leads supported the regulator's concerns regarding the NPO's management.

The NPO leadership replied to the regulator's concerns by stating that the urgent need to respond to a natural disaster had led the NPO to bypass some internal procedures and to work with whichever organisations could operate in the affected areas. Taking this into consideration, the NPO retained its registration but was forced to pay penalties. The NPO also entered into a compliance agreement with the regulator that would enforce strict due diligence and accountability standards.

103. Another diversion of funds case involves an NPO directing official that is suspected of diverting funds raised for humanitarian activities and held in the NPO's account, to facilitate terrorism.

Case Study 28

Diversion of Funds by Actors Internal to NPOs

Retention and Transfer Phases

A domestic NPO was raising funds supposedly for humanitarian relief in an area of conflict. The NPO used collection boxes outside religious institutions to solicit donations. The funds raised were held in a domestic bank account.

The founder of the NPO is suspected of diverting the funds raised to facilitate terrorism rather than using them for the stated humanitarian activities.

A law enforcement investigation resulted in the arrest of the founder of the NPO for terrorism facilitation offences. The case is still under investigation. While to date there has been no conviction, USD 60 000 in collected funds were seized.

104. The following case involves NPO directing officials diverting funds in support of terrorism using a variety of methods.

Case Study 3

Diversion of Funds by Actors Internal to NPOs

Retention and Transfer Phases

The national FIU received STRs on the domestic branch of a foreign-based NPO, which was listed locally. The domestic NPO transferred funds to the banned foreign-based NPO through a bank account in a third country. It also transferred funds to NPOs in high-risk areas and made cash withdrawals of large banknotes.

An investigation by the FIU revealed that directing officials of the domestic NPO carried large amounts of cash out of the country. In the financial intelligence reports relating to the cross-border movement of physical currency, the directing officials indicated that the funds were donations destined for charities located in both high-risk and low-risk areas.

The domestic NPO also transferred funds to a second local NPO. STRs submitted on the second NPO indicated that its directing officials transferred funds to individuals in developed countries in a region not related to the NPO's area of operation.

As a result of the investigation, the domestic NPO was listed as a supporter of terrorism and its assets were frozen.

DIVERSION OF FUNDS BY ACTORS EXTERNAL TO NPOS

105. Other instances of the diversion of funds involve actors external to the NPO. In these cases, third-party associates of the NPO, such as external fundraisers or foreign partners, are diverting funds that are destined for, or provided by, an NPO. Cases analysed for this project showed the diversion of funds by external actors occurring during the collection, retention and transfer phases of NPO operations.

106. The following case represents a situation where two separate external actors are involved in the diversion of funds. An MSB facilitating the transfer of funds between an NPO and its intended beneficiaries was deducting a 'tax' to be passed on to a terrorist organisation. In addition, the beneficiaries of the charitable funds were themselves being taxed by terrorist entities.

Case Study 36

Diversion of Funds by Actors External to NPOs

Transfer Phase

In response to a humanitarian disaster, a large international NPO was providing aid by way of cash payments to beneficiaries in areas controlled by a terrorist organisation. The NPO delivered the cash payments through a local MSB.

An examination of the humanitarian relief programme, carried out by one of the NPO's partner organisations on its behalf, raised concerns. The examination revealed that in certain instances, the MSB was deducting a 'tax' to be passed on to a listed terrorist organisation. In other instances, the beneficiaries of the charitable funds were being 'taxed' by representatives of the terrorist organisation themselves following the receipt of the financial aid.

The examination also found that there was a general understanding and acceptance that a portion of charitable funds would be diverted for terrorist purposes and that this was common practice amongst NPOs and related organisations working in the area.

Following a joint investigation by the national NPO regulator, the national FIU and law enforcement, the NPO was advised of its responsibilities with regards to reporting such incidents, and was required to provide training for its staff in order to better safeguard against similar future incidents.

107. In another case of diversion of funds involving external actors, the transferred funds meant for humanitarian relief were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation.

Case Study 22

Diversion of Funds by Actors External to NPOs

Transfer Phase

A domestic NPO was established to support charitable work in foreign areas of conflict.

An investigation by the national FIU, initiated by suspicious transaction reporting, revealed that locally collected funds were being transmitted to foreign-based charitable organisations. The investigation also uncovered that, once the funds were received by the foreign-based charitable organisations, they were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation.

While there were established connections between the foreign-based charitable organisations and the terrorist organisation, direct links between the domestic NPO and the terrorist organisation could not be substantiated.

AFFILIATION WITH A TERRORIST ENTITY

108. The second most commonly observed method and risk of abuse in the submitted case studies relates to the existence of, or suspicion of, an operational affiliation between an NPO and a terrorist entity. This affiliation translates into activity that is meant to financially or otherwise support activities carried out by one or both parties. Affiliations observed range from informal personal connections involving NPO directing officials and terrorist entities, to more formalised relationships between NPOs and terrorist entities. Approximately 45% of cases considered for this study involve an element of affiliation between an NPO and a terrorist entity. Affiliation cases uncovered connections between NPOs and terrorist entities relating to every element of NPO operations: the collection, transfer, retention and expenditure of resources, as well as the delivery of programmes. In many cases, affiliations encompassed all of these elements.

109. The case studies in this group demonstrate two main types of affiliation resulting in abuse and/or risk. The first type of affiliation is where NPOs' internal actors, namely directing officials and staff, have established or suspected links to a terrorist entity. The cases where NPOs are abused by internal actors affiliated to terrorist entities demonstrate that these individuals are able to exercise influence over the operations of the NPO that ultimately support terrorist entities.

110. In the following case, an individual who was on a terrorism watch-list used fake identification to gain employment with an NPO established to advance education.

Case Study 50

Affiliation with a Terrorist Entity

Delivery of Programmes Phase

A boarding school, registered as a religious NPO, hired an individual on a terrorist watch-list. Unbeknownst to the NPO, this individual was responsible for harbouring fugitive perpetrators involved in a terrorist bombing.

Using fraudulent identification, the individual obtained residence and employment as an English language teacher at the boarding school. The director of the school was unaware of the individual's true identity or that he was on the terrorist watch-list.

The individual was subsequently charged and convicted of terrorism-related offences.

111. The second type of affiliation is where a more formalised relationship exists between the NPO and a terrorist entity. As detailed in Chapter 2, characteristics that make NPOs effective international actors can also make them particularly vulnerable to abuse. The cases of this type show that terrorist entities that operate regional NPO branches can broaden their operational support network. The cases demonstrate that these branches are being used to carry out activities relating to fundraising, the diversion of funds, the procurement of weapons, the recruitment of supporters, military training, and other operation tasks.

112. In the following case, the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was operating as a foreign outpost of the Sri Lankan-based LTTE.

Case Study 44

Affiliation with a Terrorist Entity

Collection, Retention, Transfer, Expenditure, and Delivery of Programmes Phases

In January 2005, the Australian Federal Police (AFP) received a letter of complaint from the Sri Lankan High Commission, requesting that the AFP investigate alleged fundraising activity in Australia by the Liberation Tigers of Tamil Eelam (LTTE). The letter contained references to an international network of 'special task forces' fundraising for the LTTE under the guise of the Asian tsunami disaster relief, involving persons in Australia, Denmark, France, Germany, Italy, the Netherlands, Norway, Sweden, Switzerland, and the United Kingdom. As a result of the letter, the AFP Joint Counter Terrorism Team in Melbourne began an investigation into the allegations.

The investigation determined that the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was a cover organisation for the LTTE. The TCC solicited funds from, and coordinated radio and print material for, the Tamil community in Australia. It also lobbied politicians regarding Tamil independence in Sri Lanka and procured electronic and marine equipment on behalf of the LTTE. Hundreds of Australian-based Tamils were persuaded to contribute monthly direct-debit payments to the TCC. The TCC also used charity tins to collect money roadside and in shopping centres.

Reportedly, the Australian arm of the LTTE was run by three men: courier Aruran Vinayagamoorthy, Tamil community newspaper editor Sivarajah Yathavan and accountant Arumugan Rajeevan. The same men were also involved in directing the operation of the TCC. Raids on their homes uncovered video footage of Rajeevan and Yathavan firing a machine gun on board an LTTE gunboat in Sri Lanka and visiting one of the group's terrorist training camps. Also uncovered were photographs of Vinayagamoorthy and Rajeevan posing with LTTE founder Velupillai Prabhakaran. Vinayagamoorthy was recorded telling an associate that "[the] TCC are the Tigers and the Tigers are TCC."

Vinayagamoorthy and Yathavan ultimately pleaded guilty to providing the LTTE with more than USD 1 million. Vinayagamoorthy also admitted to providing the LTTE with electronic devices, at least one of which was used to make and detonate a bomb used in a terrorist attack.

From an NPO regulatory perspective, the TTC case encompassed multiple (red flag) indicators of risk: it facilitated the transfer of funds to a developing country with an established presence of terrorism; it collected funds in relation to disaster situations; and it was an ethnocentric organisation whose members and supporters did not approve of the listing of an organisation.

This case involved the use of financial intelligence from Australian Transaction Reports and Analysis Centre (AUSTRAC) to monitor the flow of funds out of Australia.

Note:
This case is drawn from a state submission in addition to the following open source article: Moor, Keith (2010).

ABUSE OF PROGRAMMING

113. Another observed method in which terrorists may abuse NPOs is through the abuse of their programming. The cases in this typology demonstrate that deviations to benevolent NPO-funded programmes, at the point of delivery, can result in abuse intended to support terrorism. The case studies also demonstrate varying levels of involvement of actors both internal and external to NPOs in abuse. While activities relating to this typology were carried out at a domestic level, affected parties were commonly more widespread.

114. In the following case study, an NPO was exploited by an internal actor who had been empowered to manage the NPO's online presence. While maintaining a website to further an NPO's purposes is appropriate, maintaining a website that promotes terrorism is not.

Case Study 75

Abuse of Programming

Delivery of Programmes Phase

A domestic NPO was the subject of negative open source information suggesting it was condoning suicide bombers on its website.

A review of the NPO's website by the national NPO regulator found that the NPO had published a list of 'martyrs' online, including a number of suicide bombers. Engagement by the NPO regulator resulted in the removal of inappropriate content from the website.

The investigation by the NPO regulator concluded that the NPO had inadequate governance procedures and an ineffective risk management system in place. The NPO was directed to review its governance structure to effectively manage the risks to the NPO.

115. In another abuse of programming case, an NPO was established to advance religion and education, both charitable purposes in the jurisdiction in which it operated. However, this activity was manipulated by advancing philosophies designed to promote recruitment to a terrorist organisation.

Case Study 78

Abuse of Programming

Delivery of Programmes Phase

An NPO was carrying out religious and educational activities domestically, with no foreign activities. Information provided by the national FIU indicated that the NPO had received over USD 13 000 from a foreign organisation known to provide support to a foreign terrorist group.

Subsequent open source research indicated that the NPO's education programs espoused an ideology that was shared by several foreign terrorist groups. Concerns arose that this shared ideology was being exploited for recruitment purposes for a terrorist organisation. It was subsequently revealed that a former student of the NPO's school had been charged in another country with terrorism offences. The student had also met with several other individuals who were later convicted of terrorism offences.

The NPO was audited by the national regulator, and the audit found that the NPO could not account for the origin of much of its income and expenditures. Based on this, the NPO was deregistered.

SUPPORT FOR RECRUITMENT

116. The case studies analysed for this report indicate that NPO-funded programmes or facilities can be abused to promote recruitment by terrorist movements. Out of 102 case studies analysed for this report, 27 are known to have included the abuse of the NPO sector to support recruitment by terrorist movements.

117. As discussed in Chapter 2, the existence of activities or material that supports recruitment by terrorist movements is a signal that NPO funds are being, or are in danger of being, intentionally misappropriated. Recruitment-related activities are, in themselves, a form of support to terrorist organisations and often an indicator of a wider intent to support terrorism. Additionally, the existence of such activities or material can represent the corruption of NPO programmes at the point of delivery. An NPO may have a legitimate educational programme, devote resources to it, and hire teachers, all of which are legitimate activities. However, if the teachers then engage in recruitment for terrorist causes, the educational programme and the resources devoted towards it become corrupted.

118. Support for recruitment cases included instances of abuse and risk where existing terrorist entities were using, or believed to be using, NPOs to promote and recruit for their activities. This method of abuse concerns instances where NPO resources were used to promote causes directly associated with terrorist violence. NPO-funded activities in support of recruitment were observed at the collection, transfer and delivery phases of NPO operations, both domestically and internationally. Cases of support for recruitment demonstrate NPO involvement in the following:

- transferring funds to terrorists;
- providing financial support to families of terrorists;
- carrying out of a fire bomb attack (by an NPO directing official);
- organising and hosting events that support terrorism or terrorist entities; and
- publishing materials, online or otherwise, supporting terrorism or terrorist entities.

119. Cases also demonstrate that NPO facilities were used to:

- recruit and train individuals to engage in acts of terror such as bomb manufacturing and suicide bombing;
- provide a meeting place for terrorist entities; and
- host speakers that advocate terrorism.

120. In the following support for recruitment case, an NPO is carrying out programmes and activities, on behalf of a designated terrorist organisation, that promote, support and fund terrorist recruitment and militant activities.

Case Study 80

Support for Recruitment

Delivery and Transfer Phases

On 4 November 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including al Qaida and affiliated organisations.

Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for a UN designated terrorist organisation, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UN 1267 designated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas. As of early 2009, Al Rehmat Trust

had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, Al Rehmat Trust was raising funds on behalf of Khudam-ul Islam, an alias for JEM.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including financial support to wounded Taliban fighters from Afghanistan.

FALSE REPRESENTATION AND SHAM NPOS

121. False representation occurs when, under the guise of charitable activity, organisations and individuals raise funds, promote causes and carry out other activities in support of terrorism. Specifically, the false representation cases can be divided into two categories. The first category involves 'sham NPOs' where the NPO is created as a front to support terrorist activity and its stated purposes are false. The second category involves situations where individuals or groups of individuals falsely claim to be acting on behalf of existing legitimate NPOs.

122. The cases demonstrate that sham NPOs and individuals falsely claim to be acting on behalf of existing legitimate NPOs, scheme to collect funds to support terrorism, and/or deliver programmes in support of terrorism.

123. In the following sham NPO case, an NPO claiming to be a school was actually established solely to recruit students for attacks against local police, prosecutors and judges, and to manufacture bombs.

Case Study 96

False Representation

Delivery of Programmes Phase

A bomb blast occurred at a religious boarding school being operated as an unregistered NPO. The ensuing investigation found that the school was being used by members of a terrorist group to recruit students for attacks against local police, prosecutors and judges and for the manufacture of homemade bombs.

The director of the school was convicted of terrorism-related offences.

124. In the case study detailed below, two individuals were observed falsely representing themselves as members of a well-known NPO in order to raise funds to support a militant fighting abroad.

Case Study 97

False Representation

Collection Phase

Two individuals were raising funds domestically for a family member who was fighting alongside a listed terrorist organisation abroad. The individuals, claiming to be representatives of a well-known domestic humanitarian aid NPO, were raising the funds by way of public street collections. The collection efforts were in breach of the domestic law.

The individuals in question did not have the consent of the domestic NPO to solicit donations on its behalf nor did they deliver to funds raised to the NPO. Once a sizeable amount of money had been collected, it was sent to the family member abroad using wire transfers.

As a result of a joint investigation between the FIU, NPO regulator, and law enforcement authorities, the two individuals were arrested and convicted of terrorist fundraising and sentenced to jail.

CHAPTER 4
METHODS OF DETECTION

–A description of the methods used to detect instances of abuse and risk uncovered through an analysis of information collected during the course of the project–

125. The analysis of information collected during the course of the project included an examination of how instances of abuse and risk were detected by relevant stakeholders: that is, who provided what information to whom. The analysis identified different types and sources of information, the frequency of their use, and their role in the detection of terrorist abuse and risk in the NPO sector. According to the case studies and other information collected in support of the project, detection-related efforts rely on many types and sources of information, which are broadly grouped into six categories:

Figure 4.1: **Methods of Detection—Sources and Types of Information**

Methods of Detection – Sources and Types of Information	
NPO Regulatory Information	• Lead information from the public • Whistleblowers • Audits of existing NPOs and NPO applicants • Collection and analysis of obligatory NPO reporting – Information on programs and activities – Information on directing officials and other internal actors – Information on partners and other external actors – Information on sources and beneficiaries of resources – Information on financial activity • Information voluntarily provided by NPOs
Open-Source Information	• Media articles and new aggregators • Terrorism watch-lists • Lists of designated entities • Corporate databases • A scan for web presence of NPOs and related entities • Any other information found on the Internet
FIU and Other Financial Information	• FIU financial reports – suspicious transactions – cross border currency transactions – large cash transactions – electronic funds transfers • FIU financial intelligence analysis

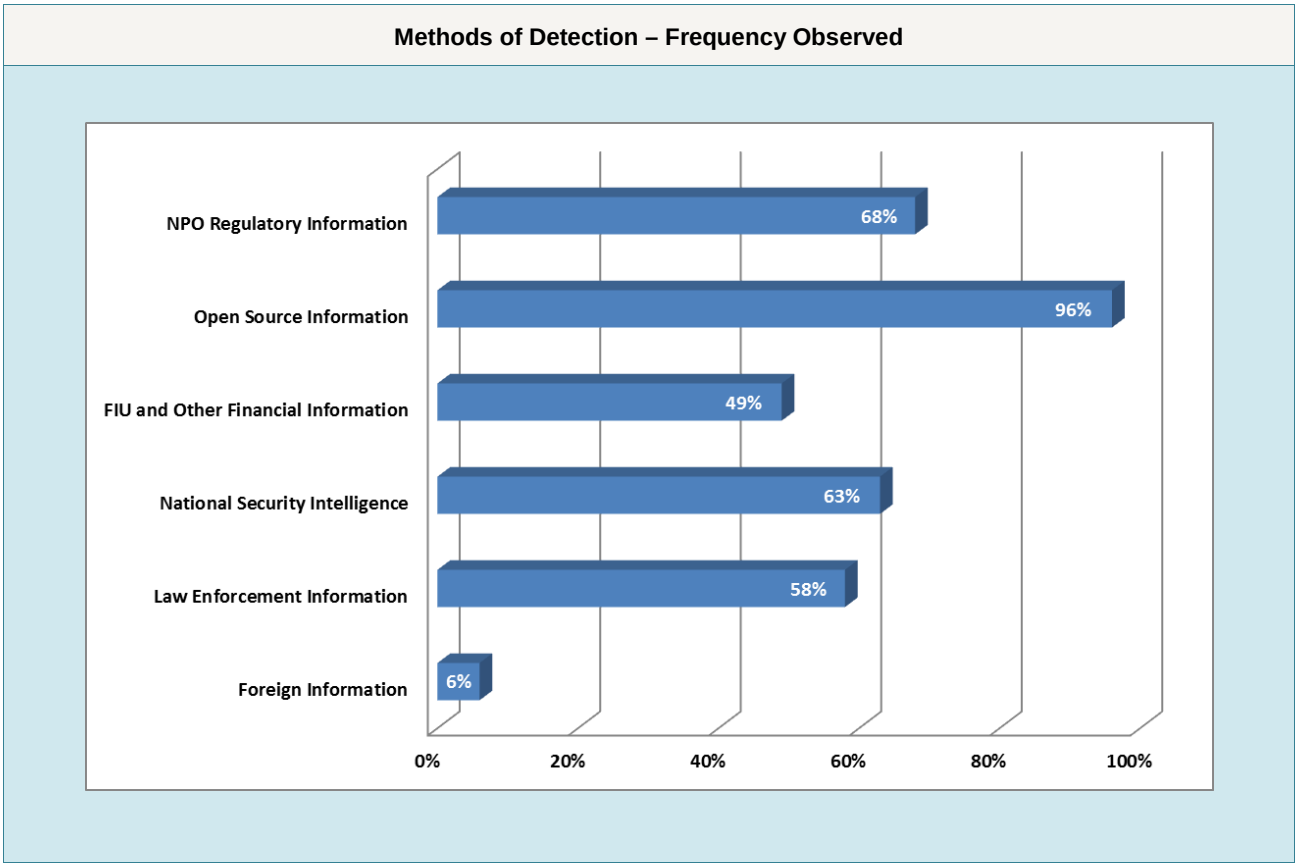
National Security Information	• Threat assessments • Risk assessments • Geopolitical assessments • Intelligence and other sensitive information
Law Enforcement Information	• Relevant criminal records • Linkages of internal and external NPO actors to relevant criminal investigations • NPO nexus to criminals and criminality • Execution of search warrants and production orders • Intelligence and other sensitive information
Foreign Information	• NPOs' foreign partners • Foreign partner agencies (of the state) – Foreign national security intelligence – Law enforcement intelligence – FIU intelligence – Information from regulatory bodies

126. Based on the information collected during the course of the project, detection efforts commonly encompass multiple types of information, from varying sources. Many jurisdictions attributed their ability to combat terrorism financing and the abuse of NPOs to effective interagency collaboration, or a whole-of-government approach. In fact, all jurisdictions that provided detailed information regarding their detection efforts employed an interagency approach to combatting the risk of terrorist abuse of the NPO sector. The case studies suggest that in the majority of instances, the detection of risk and abuse was achieved through the simultaneous consideration of multiple types of information from different sources.

127. Information collected during the course of the project further demonstrated that a collaborative approach to detection of abuse and risk ensure that investigative actions being carried out by one body don't conflict with or jeopardize actions being carried out by another.

128. The importance and frequency with which multiple types and sources of information are relied upon to detect risk and abuse is demonstrated by the case studies. *Figure 4.2* illustrates the frequency with which each of the six categories of methods of detection was observed in the cases. On average, information from three methods of detection categories was used in each case.

Figure 4.2: **Methods of Detection—Frequency Observed in Case Studies**



Note: Cases considered for frequency calculations included only those for which details regarding types and sources of information used in detection-related efforts was provided.

NPO REGULATORY INFORMATION

129. NPO regulatory information includes obligatory NPO reporting, information from NPO compliance and enforcement-related activities, and information voluntarily provided by NPOs and the public. In 68% of the cases analysed for this report, NPO regulatory information was used in detection-related efforts. Those case studies demonstrated that NPO regulators rely on a wide-range of tools and powers, mostly administrative in nature, to help identify, address and mitigate the risk of NPO abuse while continuing to promote legitimate charitable activities. The FATF's Interpretive Note to Recommendation 8 asserts that an effective approach to identifying, preventing and combating terrorist abuse of NPOs must involve an element of supervision and monitoring of the NPO sector. In certain jurisdictions, as shown in the case studies, NPO regulators led supervision and monitoring efforts that resulted in successful detection of abuse of the NPO sector. In addition, the case studies show that NPO regulators often make information pertaining to NPOs available to the public. In general, this practice increases NPO accountability and transparency.

130. In the following case study, a lead from the public which reported an affiliation between an NPO and a terrorist entity was corroborated by additional sources of information accessed by the national regulator. In reaching its decision to deregister the NPO, the national regulator considered audit information, national security intelligence and open-source information.

Case Study 14

Detection methods observed:

NPO Regulatory Information, Open Source Information, National Security Intelligence

A domestic NPO engaged in humanitarian activities abroad was sending money to a foreign partner in an area of conflict. A lead from the public to the national NPO regulator identified that the NPO had received a small donation from a known front organisation of a foreign terrorist group. Information contained in the NPO's obligatory reporting to the national regulator confirmed that the NPO had received this donation.

A short time later, a document obtained during an unrelated audit identified the NPO as a preferred funding conduit for the front organisation. The document's date corresponded with a dramatic increase in donations to the NPO. Open-source research and national security intelligence identified three of the NPO's representatives as being supporters of the foreign terrorist group, and identified the NPO's foreign partner as another front for that terrorist group.

A subsequent audit of the NPO by the national regulator found that the NPO had donated USD 700 000 to its foreign partner but was unable to account for the final use of these resources. The NPO was ultimately deregistered by the national regulator.

OPEN SOURCE INFORMATION

131. NPOs, not unlike most for-profit organisations, increasingly rely on an online presence to achieve organisational visibility and transparency, and to raise funds. Consequently, information about NPOs, and related internal and external actors, can often be accessed with relative ease. In 96% of the case studies, open source information was identified as contributing to the detection of abuse and risk. Equally, open source information can be valuable in discounting the presence of risk. It should be noted that there is a significant difference between information that might 'trigger' an investigation and information that simply contributes to an investigation. Given that the analysis did not try to determine 'triggers', the fact that the use of open source information was more predominant than other sources of information should not be interpreted as indicating it is more useful in identifying cases than other sources of information. Nor does it suggest that open source information is more reliable.

132. The case studies demonstrated that accessing, monitoring and analysing open source information allowed competent authorities to scan the environment in which NPOs were operating without disrupting legitimate NPO operations. In other words, authorities were able to assess risk prior to employing other, more intrusive, methods of detection, such as audits. The cases further

suggested that lists of designated entities, corporate databases, and the media were all widely used sources of information to help detect abuse and risk.

133. In the following case, media reports first identified an affiliation between an NPO and a terrorist organisation to the national FIU. During the course of their investigation, the FIU also accessed information from domestic law enforcement, banks, domestic government partner agencies, foreign NPO regulatory bodies, as well as the NPO itself and its foreign partners.

Case Study 30

Detection methods observed:

Open Source Information, FIU and Other Financial Information, National Security Intelligence, Law Enforcement Information, Foreign Information

A domestic NPO was one of many branches of a foreign-based, international NPO established to help rehabilitate people affected by internal conflict in the foreign country.

When the foreign country was affected by a natural disaster, the domestic branch collected and transferred funds back to the international NPO's home office in the affected area.

International press reports identifying an affiliation between the international NPO and a terrorist group led to an investigation by the national FIU. The investigation revealed that a significant sum of funds had been transferred from the domestic NPO, through several intermediary accounts, to accounts belonging to members of the terrorist group.

The investigation, however, was unable to determine whether the directing officials of the domestic NPO had knowledge of the ultimate destination of the funds transfers.

FIU AND OTHER FINANCIAL INFORMATION

134. FIU and other financial information was present in 49% of the case studies analysed for this report. Information collected by FIUs, namely financial reports, as well as related analysis, was seen to enable competent authorities in gaining a better understanding of circumstances surrounding instances of abuse and scenarios of risk. The cases demonstrated that in many instances, FIUs and banks (reporting entities) were uniquely positioned to detect suspicious financial activity involving NPOs' possible support for terrorism. Accordingly, a number of case studies were initially detected by banks and reported to FIUs in STRs.

135. FIU and other financial information also helped authorities corroborate domestically required NPO reporting to oversight bodies and identify relationships and associations among NPO-related individuals and organisations. Given that in the majority of the case studies analysed for this report, mitigation of abuse was achieved through the coordinated efforts of a number of different actors, the links identified by financial transactions, when considered in conjunction with other source information, often proved to be as important as the transaction details themselves.

136. In the following case, FIU and other financial information detected suspicious financial activity suspected of being in support of terrorism. A consequent FIU-led investigation accessed NPO

regulatory information, open source information, national security intelligence and law enforcement information. The investigation identified that a leading member of the domestic NPO was also a prominent figure in a foreign militant organisation with links to a foreign terrorist group.

Case Study 60

Detection methods observed:

FIU and Other Financial Information, NPO Regulatory Information, Open Source Information, National Security Intelligence, Law Enforcement Information

A domestic NPO received a large sum of funds, from a foreign NPO operating in an area of conflict. A directing official of the domestic NPO tried to withdraw most of the funds in cash. After the bank advised against this, a portion of the funds was withdrawn through banking machine withdrawals. In addition, another individual, unassociated with the NPO, made large cash withdrawals.

The domestic NPO's bank filed an STR with the national FIU. An investigation by the national FIU revealed that the foreign NPO was linked to a listed terrorist entity. It was also determined that a leading member of the domestic NPO was also a prominent figure in a foreign militant organisation with links to a foreign terrorist group.

NATIONAL SECURITY INTELLIGENCE

137. For the purposes of this report, national security intelligence includes information relating to terrorist threats to the security of a state or its citizens. National security intelligence contributed to the detection of abuse and risk in 63% of cases. It derives from varying sources and reports on a wide-range of subject matters. The analysis demonstrated that national security intelligence provides context to the risk environment in which NPOs operate. This included information on individuals and organisations with relevant links to activities that conflicted with national security interests.

138. In the following case, a national NPO regulator accessed national security intelligence when assessing risk relating to the activities of an NPO registered with the state. While NPO obligatory reporting initially detected suspicious financial activity of an NPO, national security intelligence led to the discovery that the beneficiary of transfers ordered by the NPO was, in fact, a terrorist entity.

Case Study 21

Detection methods observed:

National Security Intelligence, NPO Regulatory Information, Open Source Information

An NPO was formed with the stated purpose of funding foreign humanitarian activities in an area of conflict. While analysing the NPO's obligatory reporting, the national regulator noted that the NPO had contravened its registration requirements by providing funds to organisations considered to be outside of the legally prescribed set of beneficiaries.

The national regulator audited the NPO while concurrently accessing national security intelligence. Intelligence material indicated that the NPO was suspected of belonging to a network of humanitarian organisations that were sympathetic to, and influenced by, a foreign terrorist organisation operating in the same area of conflict. The audit revealed that the NPO had sent over USD 600 000 to a known front organisation for a foreign terrorist group. The front organisation itself was a listed terrorist entity in several countries. Additionally, the audit found that the NPO was unable to account for the ultimate use of much of its donated resources.

Based on its investigation, the national regulator deregistered the NPO and shared relevant material with national security partners.

LAW ENFORCEMENT INFORMATION

139. Information deriving from law enforcement activity was identified in 58% of cases analysed. Information from criminal investigations helped provide competent authorities with a better understanding of the risk environment in which NPOs were operating, and context surrounding instances of abuse and circumstances of risk. It provided insight on individuals and organisations linked to NPOs, and their relevant links to criminality.

140. In the following case, a law enforcement investigation uncovered that an NPO registered and funded by the state was, in fact, a front organisation for a terrorist organisation.

Case Study 93

Detection methods observed:

Law Enforcement Information, FIU and Other Financial Information, and Open Source Information

A domestic NPO established as a cultural youth association was the recipient of several government grants.

A law enforcement investigation into the operations of the NPO found that it was a front organisation for a terrorist group. The real activities of the NPO included raising and managing funds for the terrorist group, and disseminating the group's extremist message through the Internet.

While the NPO had a formally constituted governing body, it was created and directed by members of the terrorist group. The principal individuals involved were arrested and the NPO and its website were shut down.

FOREIGN COOPERATION AND INFORMATION

141. Foreign information includes information obtained from NPOs' foreign partners as well as information from foreign partner (government) agencies. According to the FATF's Interpretive Note to Recommendation 8, in order to effectively identify, prevent and combating terrorist abuse of NPOs, states must employ effective mechanisms for international cooperation. As demonstrated in the case studies, many NPOs operate transnationally. Naturally then, it stands to reason that

international cooperation and information sharing should contribute to the detection of terrorism-related abuse and risk of the sector. However, only 6% of the case studies identified accessing foreign information when detecting abuse and risk. The reason for this could be a reflection of what the third round of evaluations identified as generally poor compliance with Recommendation 8, specifically in relation to international cooperation.

142. In the following case, information from two foreign (government) partner agencies contributed to the national regulator's ability to detect, understand and address a situation of risk involving an NPO purportedly carrying out international humanitarian work.

Case Study 62

Detection methods observed:

Foreign Information, NPO Regulatory Information, Open Source Information, National Security Intelligence

An NPO carrying out international humanitarian work in a foreign area of conflict applied to the national NPO regulator for registration. On reviewing the NPO's application, the regulator became concerned that some of the NPO's purposes and activities were considered to be outside of those legally prescribed. Also, the foreign organisations that the NPO was partnering with in the foreign area of conflict were not legally prescribed beneficiaries

While reviewing the NPO's application, the regulator accessed national security intelligence indicating that the NPO was believed to be acting as a domestic front organisation for a listed terrorist group operating in the foreign area of conflict. It was identified that the NPO would transfer resources, through legitimate means, to several organisations operating in the area of conflict. Some of these foreign organisations were themselves identified as being part of the infrastructure of the same listed terrorist group.

Two foreign partner agencies also provided information that the national regulator was able to draw on during its review of the application. One foreign partner indicated that the NPO had been the subject of investigation in its jurisdiction in relation to terrorist activities.

The regulator informed the NPO of its concerns. The NPO attempted to address some aspects of the regulator's concerns, including opening a branch office within the foreign area of conflict in an attempt to demonstrate better control of resources and oversight of programmes. However, further investigation by the regulator indicated that the core risks were not being addressed and notified the NPO of this.

As a result of the NPO regulator's investigative efforts and administrative actions, the NPO abandoned its application for registration. Information regarding the regulator's review was passed on to national security partners to facilitate their own investigations.

CONCLUSION

143. The case studies demonstrate that the detection of terrorist abuse and risk within the NPO sector is essentially accomplished by accessing and assessing different types of information from different sources. The different types of information varied in terms of their frequency of their use, their level of impact on NPO operations and their role in detecting abuse and risk. Some information served to initiate investigative actions, while others served to provide the necessary context to support investigative and enforcement actions. Overall, the examination of how instances of abuse and risk were detected by relevant stakeholders supports the notion that mitigation of risk is achieved through the collaborative efforts of a number of different actors. While different actors offer, at times very different types of information, when put together, a complete picture of the risk environment is achieved. Given that appropriate risk mitigation is only achieved by a reliable understanding of the risk environment, the findings of this analysis are particularly relevant.

CHAPTER 5
METHODS OF DISRUPTION

– A description of the methods used to disrupt instances of abuse and risk uncovered through an analysis of information collected during the course of the project–

144. The analysis of information collected during the course of the project included an examination of how instances of abuse and risk were disrupted by relevant stakeholders. The case studies identified a wide range of activities undertaken by NPOs that were either in direct support of terrorism and terrorist entities, or that played an indirect role in a broader terrorism-related objective. The examination of the methods of disruption used to mitigate instances of abuse or significant risk, in relation to the points in time in which such methods were employed, contributed to a better overall understanding of the risk of terrorist abuse in the NPO sector. The methods of disruption, and the frequency with which they were observed, can be broadly categorised as follows:

Figure 5.1 Methods of Disruption – Frequency Observed

Methods of Disruption	Frequency Observed
Sector Outreach, Education and Self-regulation	20%
Criminal Prosecution	27%
Administrative Enforcement, Penalties, and Targeted Sanctions	71%

Note: Given that some case studies represented multiple methods of disruption, the above breakdown of frequency does not add up 100%.

145. As demonstrated by the Terrorism Support Continuum model introduced in Chapter 1, support of terrorism can encompass different activities. This same model is used here to illustrate the methods of disruption identified in the case studies (see *Figure 5.2*). On the lower end of the continuum, the activities in support of terrorism have a lower impact and the level of involvement by actors involved is more passive. Equally, in terms of complicity, the lower end of the continuum represents actors that are *non-complicit*[86]. At the other end of the continuum, however, the activities represent high-impact intentional instances of abuse.

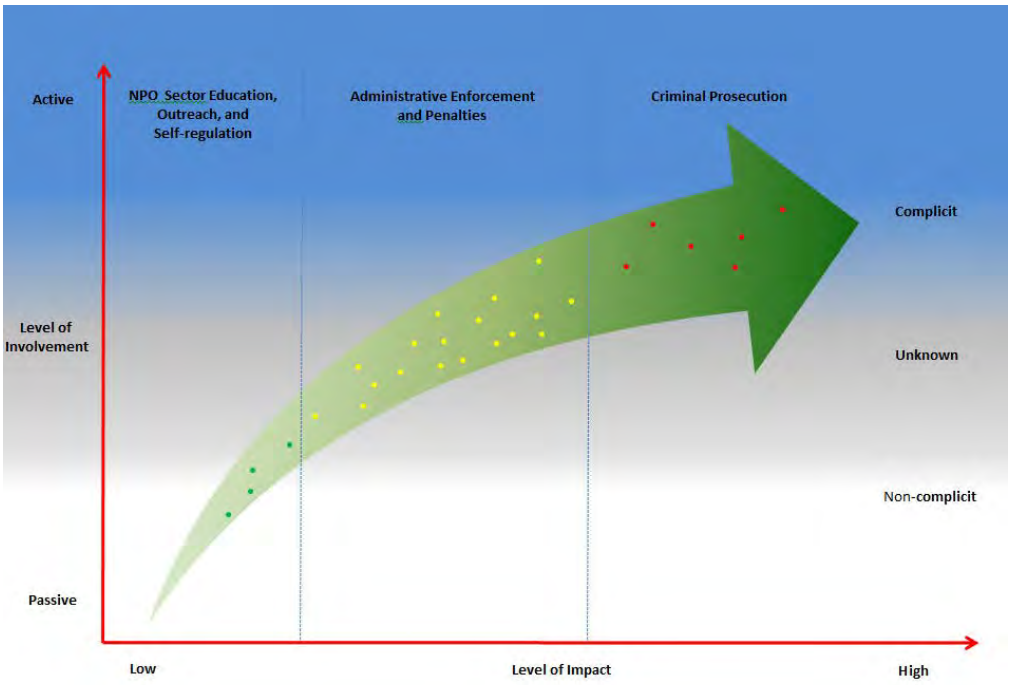
146. Cases at the lower end of the continuum were be disrupted by methods such as sector outreach, education, and self-regulation. These methods of disruption tended to be less intrusive in nature, and therefore less likely to disrupt legitimate NPO operations. Conversely, in high-impact cases of abuse, more intrusive disruption methods, such as criminal prosecutions, were used. In between the two, where the majority of the cases fall, administrative measures were used to disrupt

86 Complicit actors will likely be immune to the types of disruption methods employed here and will thus progress along the continuum.

instances of abuse or substantial risk. The movement along the continuum also illustrates the progression from risk mitigation to disruption of identified abuse.

147. *Figure 5.2* is a proportional representation of the case studies plotted along the continuum, identifying how and when they were disrupted.

Figure 5.2 **Distribution of Case Studies**



Note: The number of dots found in this figure is proportionally representative and not intended to represent specific cases.

SECTOR OUTREACH, EDUCATION, AND SELF-REGULATION

148. The Interpretive Note to Recommendation 8 indicates that any effective approach to identifying, preventing and combatting the misuse of NPOs for terrorist financing purposes needs to include an element of outreach to the sector. As demonstrated by the case studies, these types of measures can prevent or disrupt high-risk activities before they escalate to instances of abuse. The analysis did not attempt to quantify these types of measures; however, all stakeholders, including governmental and non-governmental actors, police, intelligence agencies, and NPO regulators, can be involved in outreach and education. Measures of this type are able to reach the broadest audience.

CRIMINAL PROSECUTION

149. On the other end of the continuum are case studies where the question of complicity is clearer. It is important to realise that at some point along the continuum, a criminal line is crossed. It is at this point when we see law enforcement authorities and the courts as the primary competent

authorities. In 27% of cases, terrorism-related abuse involving NPOs warranted criminal investigation and prosecution. This method of disruption includes case studies involving law enforcement arrests, the laying of criminal charges, criminal prosecution, and cases forwarded to judicial authorities.

150. In the following case study, the principal officials associated with the organisation who were responsible for misusing it were criminally prosecuted. In addition, targeted financial sanctions were used to stop the abuse and provide a deterrent against future abuse.[87]

Case Study 40

Methods of Disruption observed:

Criminal Prosecution

Islamic American Relief Agency (IARA, formerly the Islamic African Relief Agency) is an Islamic charitable organisation with international headquarters in Khartoum, Sudan; its U.S. branch (IARA-USA) was headquartered in Columbia, Missouri. IARA-USA was registered in the U.S. as a tax-exempt charitable non-profit organisation under section 501(c)(3) of the Internal Revenue Code.

On 13 October 2004, the U.S. Department of the Treasury, pursuant to U.S. Executive Order (E.O.) 13224, designated the entire IARA organisation and five of its international representatives for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including Al Qaida. IARA is formerly affiliated with Maktab Al-Khidamat (MK), which was co-founded and financed by Usama bin Laden (UBL) and is the precursor organisation of al Qaida. Records indicate several years of cooperation among IARA, MK, and UBL, starting in 1997, including a fundraising trip in 2000 during which one of IARA's Afghanistan leaders accompanied the Afghanistan MK leader to Sudan and other locations in the Middle East and raised USD 5 million for MK activities. Additional information indicates that an IARA leader was involved in discussions to help relocate UBL to secure safe harbour for him. Among others, these discussions included representatives for UBL and MK, along with Lajnat al-Dawa (LDI). In addition, a Sudanese individual travelled to Mali and stayed with an IARA director while assessing whether Mali could serve as a safe harbour for UBL. Evidence also shows that as of early 2003, IARA was responsible for moving funds to the Palestinian territories for use in terrorist activities, notably serving as a conduit to Hamas in one Western European country. In part, funds were raised through IARA collection boxes marked "Allah" and "Israel," signalling the funds would be directed towards attacks against Israelis.

In addition to the terrorism designation of the IARA organisation, numerous individuals related to the IARA-USA branch have since been convicted of violating US laws. In 2005-2007, IARA unsuccessfully challenged its designation through litigation, losing in both federal district and appellate courts.

IARA-USA violated sanctions prohibiting, among other things, the unauthorized transfer or attempted transfer, directly or indirectly, of money or goods to Iraq by US persons under Iraqi

87 The use of targeted financial sanctions is discussed in more detail under 'Administrative Enforcement, Penalties, and Targeted Sanctions.'

Sanctions Regulations, pursuant to the US International Emergency Economic Powers Act (IEEPA). For the entirety of the Iraqi Sanctions Regulations, IARA solicited donations through various means, including pamphlets, flyers, newsletters and personal correspondence, requesting contributions to pay for projects in Iraq.

In June 2010, defendant Mubarak Hamed, a naturalized US citizen and former Executive Director of IARA-USA, pleaded guilty to conspiracy to violate the IEEPA and additionally obstructing or impeding administration of internal revenue laws. Hamed, as Executive Director, oversaw funding for projects in Iraq for the duration of the Iraqi Sanctions Regulations. Through his guilty plea, Hamed admitted that beginning at least as early as 1 January 1997 through 13 October 2004, he corruptly endeavoured to impair and impede the due administration of the internal revenue laws by using IARA-USA's 501(c)(3) tax-exempt status to solicit funds. He represented the funds as legitimate charitable contributions, and misused part of those funds by transferring them to Iraq. Hamed further admitted that he continued the corrupt endeavour by omitting from IARA-USA's tax forms filed with the IRS, material information regarding IARA-USA's transaction with persons and entities in Iraq, and regarding IARA-USA's control, history and affiliations.

In April 2010, defendant Ali Mohamed Bagegni, a naturalized US citizen, pleaded guilty to conspiracy to violate U.S. sanctions pursuant to IEEPA from 1991 to 2004. Bagegni was associated with IARA, serving on the Board of Directors, which was responsible for overseeing the activities of IARA-USA.

In July 2010, defendant Abdel Azim El-Siddig pleaded guilty to conspiracy to violate the Foreign Agents Registration Act. Through his guilty plea, El-Siddig admitted that he entered into a conspiracy with defendants Siljander and Hamed to hire Siljander to act as the agent of a foreign principal. El-Siddig knew that his conduct was unlawful because Siljander had not registered with the Attorney General, such activities had not been reported to the proper authorities, and because the conspirators concealed the payments for Siljander's advocacy from the US government.

On 17 December 2009, Ahmad Mustafa, a citizen of Iraq and a lawful permanent resident alien of the United States, pleaded guilty to illegally transferring funds to Iraq in violation of US sanctions. Mustafa worked as a fund-raiser for IARA and travelled throughout the US soliciting charitable contributions.

ADMINISTRATIVE ENFORCEMENT, PENALTIES, AND TARGETED SANCTIONS

151. Disruption measures included in this category were mainly administrative in nature and involved regulatory or oversight bodies charged with responsibilities relating to NPOs. This category includes regulatory compliance measures that address abuse and risk by ensuring that NPOs comply, voluntarily or otherwise, with administrative frameworks designed to help combat the risk of terrorist abuse of the NPO sector. One or more of the methods falling under this category were seen in 71% of the case studies.

152. This category also includes the use of targeted sanctions, under international and national frameworks, meant to identify and disrupt the resourcing of entities identified as supporters of terrorist activity. FATF Recommendation 6 supports the use of targeted sanctions, which are also internationally anchored in United Nations Security Council Resolutions, particularly Resolutions

1267 and 1373. *Figure 5.3* contains a list of measures grouped under administrative enforcement, penalties, and sanctions.

Figure 5.3: **Methods of Disruption—Administrative Enforcement, Penalties, and Sanctions**

Methods of Disruption – Administrative Enforcement, Penalties, and Targeted Sanctions	
Regulatory Compliance	• Regulatory authorities issued a letter to an NPO outlining their concerns and providing the NPO with the opportunity to address the concerns • NPO was made to enter into a compliance agreement with regulatory authorities to enforce stricter due diligence and/or accountability standards
Enforcement Action (by competent authorities)	• NPO was denied registration • NPO activities were temporarily suspended • NPO activities are being monitored with the knowledge of the NPO • NPO board of directors was changed • NPO was audited • NPO was levied financial penalties • NPO property was forfeited
Targeted Sanctions	• NPO was listed as a supporter of terrorism • NPO accounts or assets were frozen

153. The following unsanitised case study illustrates the use of administrative enforcement measures and targeted sanctions to halt the abuse of NPO resources for terrorist purposes.

Case Study 41[1]

Methods of Disruption observed:

Administrative Enforcement and Penalties

The Povrel Jerusalem fund for the Afflicted and Needy (JFHS) was established in 1992 and purported to carry out humanitarian activities through partner organisations in the Palestinian Territories. In 1992, JFHS applied for charitable registration to the Canada Revenue Agency (CRA), which is the national regulator of charities in Canada. While reviewing JFHS's application, CRA became concerned that JFHS's purposes and activities were primarily political in nature, and therefore not charitable according to Canadian law. Also, the organisations that JFHS was partnering with in the Palestinian Territories were not considered legal beneficiaries under Canadian law. Information derived from open-source research indicated that some of JFHS's international partners were part of a fundraising network run by Hamas, a listed terrorist entity in Canada.[2] Through multiple communications with CRA, JFHS was repeatedly unable to show that it could maintain the legally required level of direction and control over its resources.

In 1998, CRA notified JFHS that it was unlikely to receive registration. A short time after this notification, a second NPO, the International Relief Fund for the Afflicted and Needy-Canada (IRFAN-Canada), applied for charitable registration. IRFAN-Canada was granted registration in 1999 while JFHS was still pursuing its separate application. When CRA again advised JFHS in 2000 that it was unlikely to receive registration, JFHS abandoned its application. Without notifying CRA, JFHS then turned over its assets to IRFAN-Canada, both organisations passed resolutions formally consolidating their operations, and several directing officials from JFHS began to manage IRFAN-Canada programs.

In 2003, open-source media began to indicate that JFHS and IRFAN-Canada had merged, and that IRFAN-Canada was connected to Hamas. CRA's analysis of IRFAN-Canada's mandatory annual reporting verified that there was reason for further concern. CRA audited IRFAN-Canada in late 2003 and identified several significant compliance problems. IRFAN-Canada was transferring significant resources to foreign organisations without maintaining adequate control of, or accounting for, the final use of the resources. Some of these foreign organisations were believed to be controlled by Hamas. IRFAN-Canada retained its registration after agreeing to put in place changes to their due diligence and accounting activities.

In 2009, CRA began a substantial follow-up audit of IRFAN-Canada to verify that the problems identified in 2003 had been addressed. CRA examined financial records, digital records, and programme material derived from the domestic and international offices of IRFAN-Canada. This material was combined with substantial open source research and assessments provided by partners[3].

CRA's 2009 audit of IRFAN-Canada revealed numerous serious compliance problems. These problems included, but were not limited to, the following:

- Between March 2006 and April 2007, IRFAN-Canada transferred, through a local partner, over USD 500 000 to the HAMAS-controlled Ministry of Telecommunications in Gaza, which was involved with distributing funds to the families of HAMAS fighters through the post office system.
- During the same period, IRFAN-Canada transferred over USD 160 000 through a local partner to the HAMAS-controlled Ministry of Health in Gaza.
- IRFAN-Canada continued funding to the Ramallah Zakat Committee, allocating over USD 77 000 to the Committee in 2007. CRA had notified IRFAN-Canada in 1998 and 2004 that the Committee was believed to be affiliated with Hamas, and IRFAN-Canada had told CRA that cooperation with the Committee had stopped as of 2004. Records showed that they renewed the relationship one month after the end of CRA's original audit.
- In 2007, IRFAN-Canada provided new computers and office equipment to the Al Muntada At-Tahqafi Cultural Forum after the Israeli military raided its offices and the Forum was made an unlawful association in Israel because of its close ties to Hamas. The equipment cost over USD 15 000.
- In 2007, IRFAN-Canada provided resources valued at over USD 8 600 000 to the Zakat Fund, Lebanon, which had been listed as an unlawful association in Israel for supporting

Hamas.

In addition, records obtained during the audit showed that the directing official of IRFAN-Canada's West Bank office, who had signing authority for the organisation's accounts, had misappropriated over USD 100 000 of IRFAN-Canada's funds. This directing official had a known connection with Hamas organisations.

Based on the findings of the 2009 audit, CRA initially suspended and ultimately revoked IRFAN-Canada's charitable registration in 2011.

In 2014, the Government of Canada listed IRFAN-Canada as a terrorist entity under its Criminal Code based in part on CRA's findings that IRFAN-Canada provided support to Hamas, a listed terrorist organisation.

Notes:

1. This case study was developed entirely from the open source documents cited and was not developed from any state's response to the request for case studies. See CRA's administrative fairness letter to IRFAN-Canada dated 2010-12-10, and available at: www.globalphilanthropy.ca/index.php/blog/comments/international_relief_fund_for_the_afflicted_and_needy_canada_irfan-canada_h/ (Accessed 2014-03).
2. al-Muqawama al-Islamiya (Hamas). See Public Safety and Emergency Preparedness Canada's website: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx (Accessed 2014-03).
3. International Relief Fund for the Afflicted and Needy (Canada) v. Canada (National Revenue), 2013 FCA 178 [Docket A-20-13] https://www.canlii.org/en/ca/fca/doc/2013/2013fca178/2013fca178.html (Accessed 2014-06-18).

CONCLUSION

154. Analysis of the information collected during the course of the project demonstrates that competent authorities rely on a wide range of measures to disrupt instances of abuse and substantial risk within the NPO sector. Different methods of disruption proved to be appropriate at different points in time. The case studies demonstrate that it is the specific circumstances surrounding individual organisations, and often the level of complicity of its directing officials, that determine which disruption methods are most appropriate. While low-impact cases were often disrupted by measures that were minimally intrusive to NPO operations, high-impact cases involving complicit NPO officials often warranted more intrusive methods of disruption. Overall, the cases demonstrated that successful disruption depended on the competent authorities' understanding of the risk environment. Consistent with the findings relating to the *Methods of Detection*, the case studies demonstrate that employing a whole-of-government approach, focused on interagency collaboration and information sharing, is key to identifying and implementing the appropriate methods of disruption.

CHAPTER 6
RISK INDICATORS AND TERRORIST ABUSE INDICATORS

155. Indicators are used extensively in sectors where prevention is paramount, such as the business and medical sectors.[88] Indicators can increase forewarning, helping to mitigate risks before they become reality, or help to detect existing abuse. The analysis of the case studies identified numerous elements that indicated existing abuse of an NPO, or substantial risk of abuse. These elements have been compiled in this chapter to help all stakeholders, including NPOs, government actors, financial institutions, and designated non-financial businesses or professions (DNFBPs) identify and investigate possible cases of abuse within a particular NPO or the larger NPO sector. While the list of indicators presented here is substantial and transnational in nature, it is not complete; there are likely additional indicators that are unique to particular contexts identified within particular national jurisdictions, in line with FATF Recommendation 1 (national risk assessment).

THE NATURE OF INDICATORS

156. Indicators are ultimately leads that require further investigation to assess the nature or risk of abuse. This said, it is apparent through the case studies that not all indicators carry an equally strong certainty of a terrorism-related risk. For many of the indicators identified, referred to as 'risk indicators,' support to terrorism is a possible explanation, but not necessarily the only possible explanation. 'Terrorist abuse indicators', a smaller sub-set of indicators, denote a stronger relationship with terrorism-related activities. *Figure 6.1* provides further details on these two types of indicator.

Figure 6.1: **Risk Indicators and Terrorist Abuse Indicators**

Risk Indicator	Terrorist Abuse Indicator
An aspect of an NPO's activities that suggests abuse or a risk of abuse that may be terrorism-related, but also has possible alternative explanations.	An aspect of an NPO's activities that suggests abuse or a risk of abuse that is directly related to terrorist activity. The presence of these indicators would lead to a stronger certainty that the abuse or risk is terrorism-related, as opposed to alternative explanations.

157. Different indicators can be detected by different actors depending on the type of information involved. For instance, government agencies, particularly an FIU, will be better situated to detect NPOs structuring financial transactions because they have access to financial data. Similarly, NPOs

88 See Davies, Jonathan; Finlay, Mike; McLenaghen, Tara and Wilson, Duncan (2006); Balsamo, Richard R and Brown, Max Douglas (2007), *pp.*285-304.

are better placed to detect the diversion of funds because they have ready access to their internal records. A regulator could also gain access to these records during an audit however.

158. Finally, because indicators are leads for further analysis, the existence of indicators must be taken in the context of the case. In some cases, a single indicator or small number of indicators may be enough to prompt substantial investigation. In the case below, the context of the case and the nature of the two indicators are enough to assess that the abuse of the NPO sector in this case is terrorism-related.

Case Study 100

A homemade bomb exploded in a house displaying a banner for an NPO supporting orphan relief. An investigation found that the advertised NPO did not exist and that a terrorist group was disguising its bomb-making facility as an NPO office.

Law enforcement authorities seized a large cache of bomb making supplies and weapons. One member of the terrorist group was charged and convicted of terrorism related offences.

 Criminal activities consistent with terrorist operations are concealed in NPO facilities.

 Advertised NPO is fictitious.

159. Alternatively, in some cases the combination of several indicators can lead to the assessment that the abuse or risk involved in the case is terrorism-related, as seen in the case below. The risk indicators present in the case, taken on their own, indicate the potential for abuse; what kind of abuse is uncertain however. When these three risk indicators are combined with an additional terrorist abuse indicator, it becomes more certain that the abuse or risk is terrorism-related.

Case Study 68

In June 2005, the ISNA Development Foundation (IDF) was registered as a charitable organisation by the Canada Revenue Agency (CRA), which is the government agency responsible for the regulation of charities. IDF was registered with the primary purposes of advancing religion through the establishment and operation of religious facilities in Canada and the relief of poverty through the provision of financial assistance to needy persons in Canada.

In January 2011, IDF's parent organisation, the Islamic Society of North America (ISNA), was the subject of media reporting that detailed the findings of an independent, internal audit. The audit identified serious concerns regarding ISNA's alleged misuse of resources, particularly pertaining to the transfer of funds to improper beneficiaries, improper receipting, and the allocation of a large percentage of resources to activities not permitted under the regulations governing registered charities in Canada. In addition, substantial resources were being transferred to another Canadian NPO, the Kashmir Relief Fund of Canada (KRFC), presumably in order to undertake activities in Kashmir.

The CRA conducted an audit of IDF's operations in December 2011. The audit revealed that IDF had

entered into a funding arrangement with KRFC and its sister organisation, the Kashmiri Canadian Council (KCC), with the ultimate goal of sending the raised funds to a Pakistan-based NPO named the Relief Organisation for Kashmiri Muslims (ROKM). Under the arrangement, KCC/KRFC raised funds for "relief work" in Kashmir; the IDF supplied official donation receipts to the donors and disbursed over USD 250 000 to ROKM, either directly, or via KCC/KRFC. During the audit of IDF, the directing officials of IDF stated that they knew nothing about ROKM or the specific nature of the activities towards which the funds were to be directed. The above-noted receipting arrangements are not allowed under Canadian regulations. In addition, IDF failed to maintain direction or control of the funds transmitted and was unable to substantiate the nature of the programs towards which its resources were directed.

A review of IDF's electronic documentation allowed CRA to determine that documentation professing to indicate IDF's control over the Kashmiri projects had been fabricated. As an example, forensic analysis by the Government of Canada of photographs provided to the CRA to demonstrate IDF's direction and control over the activities being undertaken in Kashmir, had been digitally altered through the addition of a banner bearing the name IDF.

The CRA's research indicated that ROKM is a charitable arm of Jamaat-e-Islami, a political organisation that actively contests the legitimacy of India's governance over the state of Jammu and Kashmir, including reportedly through the activities of its armed wing Hizbul Mujahideen. Hizbul Mujahideen is listed as a terrorist entity by the Council of the European Union and is declared a banned terrorist organisation by the Government of India, Ministry of Home Affairs, under the *Unlawful Activities (Prevention) Act of 1967*.

Given the commonalities in directorship between ROKM and Jamaat-e-Islami, the apparent participation of these same individuals in the establishment and high-level control of Hizbul Mujahideen, and the numerous public declarations of support provided by many of them for the armed militant movement in Kashmir, it was the CRA's expressed concern that the IDF's resources may have been used to support the political efforts of Jamaat-e-Islami and/or its armed wing, Hizbul Mujahideen.

Based on the findings of the audit, IDF's charitable status was revoked in September 2013. The revocation was the subject of multiple media reports in Canada, the United States, and India. Subsequently, ROKM's website was taken down.

- NPO transfers resources or conducts activities in an area where terrorist entities are known to have a substantial presence.
- NPO has unreported activities, programmes, or partners.
- NPO is unable to account for the final use of all of its resources.
- Falsified or conflicting documentation is used by an NPO or by NPO representatives.
- Existence of reliable information indicating an NPO or its representatives are linked to third parties that support or are engaged in terrorist activity.

Note:

This case study was developed entirely from the open source documents cited and was not developed from any state's response to the request for case studies. See CRA's administrative fairness letter to IDF dated 2013-

05-28, and available at www.thestar.com/news/canada/2013/07/25/star_investigation_federal_audit_raises_concern_that_canadian_charity_funded_terror.html.

INDICATOR CATEGORIES

160. The indicators reflected in the case studies are grouped under seven general categories. However, many indicators can fall under numerous categories. For the sake of simplicity, this report lists them only once under the most applicable category based on the analysis. The categories of indicators do not directly mirror the typologies of abuse because multiple types of indicators can fall under a single typology. For instance, the typology of *False Representation and Sham NPOs* could incorporate indicators from all categories. Attempting to directly link particular indicators to particular types of abuse may cause false assumptions in analysis, and therefore it has been avoided here.

161. The indicators have been broken down between those that are most *applicable to government actors*, and those that are *applicable to both government actors and NPO sector actors*. The utility of these indicators to the NPO sector is dependent on the premise that NPOs are not complicit in abuse, otherwise the level of deception employed would make detection by other NPO actors very difficult.

CATEGORY 1: FINANCIAL SUPPORT TO KNOWN OR SUSPECTED TERRORIST ENTITIES

162. The direct abuse of NPO financial resources is what most often comes to mind when considering abuse or risk in the NPO sector. This type of abuse can occur many ways, as discussed in Chapter 3.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: ⚑ Use of cash couriers to transfer NPO funds into areas with known terrorist activity. ⚑ NPO transactions are structured to avoid transaction reporting. ⚑ Requests to transfer NPO funds are accompanied by vague justifications. ⚑ NPO uses a shell organisation as a funding conduit. ⚑ NPO representatives fail to declare large currency amounts at international borders. *Applicable to both government and NPO actors:* ⚑ NPO bank accounts are used by entities whose own accounts are under restrictions.	*Applicable to both government and NPO actors :* ⚠ NPO funds are transferred to other entities believed to be engaged in, or supporting, terrorist activities. ⚠ NPO receives funds from entities believed to support terrorist activities.

Risk Indicators	Terrorist Abuse Indicators
NPO funds are comingled with personal or private business funds. Bank accounts related to some programmes or activities are concealed. NPO funds are transferred to entities not associated with declared programmes or activities.	

CATEGORY 2: MATERIAL SUPPORT TO KNOWN OR SUSPECTED TERRORIST ENTITIES

163. NPOs are abused by terrorist organisations because of their access to material resources as well as financial resources. These material resources can range widely from facilities to dual-use equipment. Warning indicators are more prevalent in this category because the category itself applies to known or suspected terrorist entities.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: NPO facilities are frequented by individuals believed to support terrorist activities. *Applicable to both government and NPO actors:* NPO procures dual-use equipment.	*Applicable to both government and NPO actors:* Resources of an NPO are transferred to an entity known to be engaged in, or supporting, terrorist activity. NPO receives resources from an entity believed to support or be engaged in terrorist activities. NPO shares property with another organisation believed to support terrorist activity.

CATEGORY 3: FINANCIAL, MATERIAL, OR LOGISTICAL SUPPORT TO PROSCRIBED TERRORIST ENTITIES

164. The identification of proscribed entities (often termed 'listed' entities) in association with NPOs appeared consistently throughout the case studies. Often, the presence of proscribed entities was an indicator of wider compliance failures that could have been intentional or unintentional. Warning indicators are more prevalent in this category because the category itself applies to proscribed terrorist entities.

Risk Indicators	Terrorist Abuse Indicators
Applicable to both government and NPO actors: NPO activities are found to support individuals or organisations whose identities correspond to those of listed entities.	*Applicable to government actors:* Existence of reliable information indicating an NPO or its representatives are engaged in supporting terrorist activity. Existence of reliable information indicating an NPO or its representatives are linked to third parties that support or are engaged in terrorist activity. *Applicable to both government and NPO actors:* The identities of proscribed terrorist entities are found to match the identities of NPO directing officials or employees.

CATEGORY 4: OPERATIONS IN AREAS WHERE THERE ARE ACTIVE TERRORIST THREATS

165. Often, NPO operations in areas of conflict are viewed as the most high-risk for terrorist abuse because of the low governance capacity in such areas. However, in reviewing the case studies it became apparent that, while areas of conflict did present higher risk, the existence of an active terrorist threat was the important factor in determining risk. The indicators below reflect this analytic finding. Also, it was apparent in the analysis of case studies that identifying direct interconnection between NPO activities and terrorist movements became more difficult in foreign jurisdictions. In these instances, ground-level information that would verify the involvement of a terrorist entity, and thus provide a warning indicator, becomes more difficult to obtain and international cooperation and information-sharing takes on new importance. The ability to audit an NPO's foreign activities is more difficult given distance, and the ability to monitor resources and networks becomes dependent on the cooperation of multiple jurisdictions. This difficulty is reflected in the absence of warning indicators.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: Entities operating in areas with known terrorist activity transfer funds into the bank accounts of an NPO, directing officials, or employees. *Applicable to both government and NPO actors:* NPO transfers resources or conducts activities in an area where terrorist entities	

Risk Indicators	Terrorist Abuse Indicators
are known to have a substantial presence. NPO records are maintained in an area where terrorist entities are known to have a substantial presence. NPO representatives travel frequently into areas where terrorist entities are known to have a substantial presence.	

CATEGORY 5: GENERAL OPERATIONS AND GOVERNANCE

166. Several indicators arise from the general operations and governance of NPOs. Several of these indicators stem from attempts by complicit actors (either internal or external to an NPO) to disguise their actions, such as the concealment of information on programmes, activities, or funding. Other indicators in this category stem from attempts by complicit actors to gain influence or control of non-complicit NPOs.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: NPO has unreported activities, programmes, or partners. NPO uses an unusually complex financial network for its operations. NPO avoids mandatory reporting requirements. NPO programmes and activities are vaguely explained to oversight or regulatory bodies. Third parties are used to open NPO bank accounts or carry out some transactions. *Applicable to both government and NPO actors:* NPO expenditures are not consistent with its programmes and activities. NPO is unable to account for the final use of all of its resources. NPO is unable to account for the origin of its	*Applicable to government actors:* A lead from the public alleges that an NPO is engaged in activities related to terrorism. NPO merges with another organisation believed to support terrorist activities. NPO humanitarian assistance is targeted towards supporting individuals directly linked to terrorist entities. *Applicable to both government and NPO actors:* Directing officials of an NPO are, or have been, directing officials of other organisations believed to support terrorist activity. NPO suffers from an internal conflict, where one faction is known to be sympathetic or actively supportive towards terrorist entities.

Risk Indicators	Terrorist Abuse Indicators
income. NPO has inconsistencies in its accounting and/or mandatory reporting. NPO has opaque leadership or decision-making structures. NPO or NPO representatives use falsified or conflicting documentation.	

CATEGORY 6: SUPPORT FOR RECRUITMENT

167. In several cases, NPO resources are committed towards activities that support the recruitment of followers by terrorist movements. The case studies indicated that activities in support of recruitment are often connected to further risks to financial or material resources. Also, otherwise legitimate charitable programmes meant to further religious or educational purposes can be corrupted to support recruitment activities.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: Individuals involved in terrorist activities are linked to an NPO. *Applicable to both government and NPO actors:* NPO publications or speakers support terrorism or terrorist entities.	*Applicable to both government and NPO actors:* Directing officials or employees of an NPO engage in activities that support recruitment to violence.

CATEGORY 7: OTHER CRIMINAL ACTIVITIES

168. Abuse of NPOs for terrorist purposes can come to the attention of government authorities or the NPOs themselves because of other criminal activities. Research has indicated linkages between criminality and terrorism, which some case studies illustrated. [89] Previous FATF typologies reports have also highlighted the use of criminal activities to finance terrorism.[90] As in the cases of terrorism, NPOs may not be complicit in these criminal activities, but may be victims themselves of external or internal actors. The presence of other criminal activities, especially in conjunction with indicators specific to terrorism, presented a strong sign of risk in the case studies.

89 For instance, see Gomez, Juan Miguel del Cid (2010), *pp.*3-27.

90 FATF (2008), *pp.*15-19.

Risk Indicators	Terrorist Abuse Indicators
Applicable to government actors: Advertised NPO is fictitious. *Applicable to both government and NPO actors:* NPO facilities conceal criminal activities. NPO directing officials or employees are engaged in other criminal activities.	*Applicable to both government and NPO actors:* Criminal activities consistent with terrorist operations are concealed in NPO facilities. NPO directing officials or employees are engaged in other criminal activities consistent with terrorist operations.

CHAPTER 7
CONCLUSION

169. The goal of this typologies project is to provide analytical findings to help national and international policymakers, government agencies, and non-profit organisations protect the NPO sector from abuse by terrorist entities. The principal findings of the report are summarised in *Figure 7.1*.

Figure 7.1: **Summary of Analytic Findings**

1. The NPO sector has interconnected vulnerabilities, and terrorist entities seek to exploit more than one type of vulnerability. In the cases analysed for this project, the diversion of NPO funds by terrorist entities was a dominant method of abuse. However, other types of non-financial abuse such as the abuse of programmes or the support for recruitment appeared regularly as well.
2. The NPOs most at risk appear to be those engaged in 'service' activities, and who operate in a close proximity to an active terrorist threat. This may refer to an NPO operating in an area of conflict *if* there is an active terrorist threat. However, this may also refer to an NPO that operates domestically, but within a population that is actively targeted by a terrorist movement for support and cover. In both cases the key variable of risk is not geographic, but the proximity to an active threat.
3. Because of the nature of the threat and the resulting nature of state responses, cases of substantial risk are an important source of information for typologies analysis.
4. The amalgamation of many types of information held by different actors was an important factor in detecting cases of abuse or identifying substantial risk.
5. Disruption of abuse, or the mitigation of substantial risk, was dealt with through multiple means including, but not limited to, criminal prosecution. Administrative enforcement, financial penalties, and targeted financial sanctions played important roles in disruption of abuse.

170. In Chapter 1, several key questions were introduced that addressed both operational and strategic research requirements. Through the research and analysis conducted for this typologies project, we can begin to answer these questions and hence provide a better understanding of the threat posed to the NPO sector by terrorist entities.

STRATEGIC CONSIDERATIONS

171. At a strategic level, the analysis indicated that the complexities inherent in the NPO sector, the terrorist threat, and national or international responses to terrorism, humanitarianism and governance create several key drivers that shape the overall environment:

Environmental Driver	Explanation
Driver 1: Necessity for effective CFT measures because of damage caused by terrorist entities	Driver 1 refers to the requirement for national and international governmental bodies to respond to the terrorist threat in order to protect civilians.
Driver 2: Operational efficacy of the NPO sector	Driver 2 refers to the maintenance of the NPO sector's effectiveness and efficiency in the delivery of programmes and activities.
Driver 3: Duty to donors to maintain accountability in humanitarian operations	Driver 3 refers to the duty of the NPO sector and other stakeholders to ensure that funds or materiel entrusted to the sector by donors are used for the purposes they were intended.
Driver 4: Duty to beneficiaries to provide assistance	Driver 4 refers to the duty of the NPO sector and other stakeholders to ensure that assistance is provided to beneficiaries in a manner consistent with international humanitarian standards.
Driver 5: Collective action of international regimes	Driver 5 refers to the rules and standards set by international bodies (such as the FATF 40 Recommendations) in an effort to ensure collective prosperity and security.
Driver 6: Independent action of national states	Driver 6 refers to the ability of a state to act in accordance with, or at odds with, international norms based on the state's status as a sovereign entity.

172. These key drivers, equally necessary in their own right but also interdependently, impose competing demands on all actors involved. Because each driver is equally necessary, effectively navigating the competing demands becomes an exercise in balance.

ANALYTIC FINDINGS

What…	…is the nature of the threat posed by terrorist entities to the NPO sector?

173. Perhaps most importantly, the typologies report found that more than a decade after the abuse of NPOs by terrorist entities was formally recognised as a concern, the threat remains. While the abuse of the NPO sector by terrorist entities is, in the context of the global NPO sector, a low-probability risk, the impact of such abuse on the NPO sector goes beyond the narrow consideration of monetary value. Donors trust that resources provided to NPOs, either financial or material, will be used for good works; this trust is the foundation for the NPO sector. The diversion of these resources to benefit entities whose principal goal is to harm, undermines the public's trust in the NPO sector, which will have a disproportionate impact on NPO operations.

174. At an operational level, the analysis indicates that NPOs can be targeted by numerous types of terrorist entities. Traditional transnational terrorist organisations still comprise a substantial portion of the threat to the NPO sector. These traditional terrorist organisations attempt mainly to exploit legitimate NPOs, or to undermine the integrity of the sector as a whole through the creation of illegitimate 'sham NPOs.'

175. In addition to the traditional transnational terrorist organisations, the analysis indicates that homegrown and self-starter entities also pose a threat to the NPO sector, and are a growing element of the threat environment. The analysis indicated that these entities, being domestic themselves, can exploit the domestic operations of NPOs. These instances indicate that a focus on foreign activities or foreign entities risks leaving domestic NPO activities open to abuse.

Who…	…are the NPOs that are most at risk of abuse for terrorist abuse?

176. While the global NPO sector is massive in scope, the analysis indicates that organisations engaged in particular types of activities and in particular environments are most vulnerable to abuse. Specifically, 'service NPOs' principally engaged in the provision of humanitarian services present the most desirable targets for terrorist entities because of the types of resources involved in their operations, the geographic breadth of their operations, and their access to vulnerable populations. None of the case studies analysed showed terrorist entities targeting 'expressive NPOs,' principally engaged in political, advocacy, or similar types of expressive activities.

177. NPOs operating in environments or populations that terrorist movements also actively target are at a higher risk of abuse. Importantly, this does not always correspond to geographic areas of conflict or low-governance. In areas of conflict or low-governance where terrorist movements do not or cannot operate, NPOs may face risks associated with corruption or criminality, but not terrorism. Conversely, populations within relatively stable environments may still be actively targeted by terrorist movements for support because of their association to a particular conflict. For example, the Irish Republican Army consistently targeted Irish immigrant communities for support and

fundraising, particularly in the Eastern United States.[91] NPOs operating in these stable environments are therefore still at a higher risk. Ultimately, the principal considerations for determining which NPOs are at a higher risk of abuse are the value of their resources or activities to terrorist entities, and the proximity to an active terrorist threat that has the capability and intent to abuse NPOs.

When…	…are NPOs most at risk of abuse by terrorist entities?

178. As explained earlier, the analysis indicates that NPOs are most at risk of abuse by terrorist entities when they conduct service activities in environments where there is also an active terrorist threat. Additionally, there is evidence that, for service NPOs operating in these environments, strategic shocks, such as natural disasters, that result in a spike in demand for NPO funds and services increases vulnerabilities. Personnel become stretched when demand for services grows rapidly, straining internal oversight or forcing directing officials to reallocate personnel otherwise focused on due diligence. While there appears to be a correlation between strategic shocks and NPO vulnerability, further research would be needed to validate this link.

Where…	…are NPOs most at risk of abuse by terrorist entities?

179. The analysis showed that NPO activities can be vulnerable at multiple points throughout the general model of operations (refer to *Figure 2.6*). Cases of abuse were observed at all phases of the model dealing with resources: collection, transfer, retention, and expenditure. Also, cases of abuse were observed during the programme delivery phase, where the activities of the NPO were legitimate up to the point when they were provided to beneficiaries. A good example is the abuse of an educational programme to promote recruitment for terrorist entities, a scenario reflected in several case studies. In these instances, the collection, retention, transfer, and expenditure of resources are all in line with the nature of an educational programme. However it is the very delivery of the programme that is abused for terrorist purposes. Abuse at the programme delivery phase indicates that focusing purely on NPO resources may fail to detect some serious cases of abuse, and that knowledge of programmes can be as important as knowledge of resource flows.

Why…	…are NPOs at risk of abuse by terrorist entities?

180. NPOs and terrorist entities operate in the same global environment. They often seek to access the same communities, just with very different intents. The NPOs are the repairers of vulnerable communities. The terrorist entities are the exploiters and aggravators. NPOs seek to be highly mobile, well-resourced, with low levels of external scrutiny, in order to enable their operations. Analysis at the strategic and operational levels indicates that these are also organisational qualities

[91] See Horgan, John and Taylor, Max (1999, 2003). A similar example concerns the LTTE which targeted Sri Lankan communities for support (see Chapter 2).

valued by terrorist entities, but for very different ends. NPOs are targeted by terrorist entities because NPOs can easily and legitimately access materials, funds, and networks. Terrorist entities seek access to these same materials, funds, and networks but, being illegitimate entities, must do so clandestinely. This means that terrorist entities place a high value on exploiting legitimate sectors that already have access to these benefits, and also have operations that are difficult to scrutinise.

How…	…are NPOs vulnerable to terrorist abuse?

181. The analysis indicates that NPOs are vulnerable to terrorist financing activity because of several organisational trends within the NPO sector. Extended logistical networks make oversight difficult, particularly in international programmes. A large transitory workforce within the sector makes it difficult for organisations to effectively vet personnel and attract staff with a technical knowledge of due diligence and compliance operations. A high operational capacity in terms of resources, access to networks, and substantial public trust, also leaves NPOs vulnerable. Finally, the high emphasis placed on achieving goals within the organisational culture of NPOs can leave them vulnerable because, in some cases, it can lead directing officials or employees to ignore acute risks in favour of delivering programmes.

182. Goal orientation is not necessarily a fault though; goal orientation is often what makes NPOs very effective. However, in instances where there is a substantial risk, this must be balanced against the need to maintain the integrity of the NPO sector as a whole.

How…	…do terrorist actors abuse the NPO sector?

183. The analysis of the case studies showed the abuse of NPOs, or the risk of abuse, manifesting in five different ways:

Methods/Risks of Abuse
Diversion of Funds
Affiliation with a Terrorist Entity
Abuse of Programming
Support for Recruitment
False Representation

How…	…have cases of abuse been detected and disrupted?

184. The analysis also examined how instances of abuse or risks of abuse have been detected. The detection of abuse and the ability to investigate potential abuse is dependent on levels of access to different types of information, each with its own costs and benefits. Significant due diligence can be achieved through the use of open-source, regulatory, and financial information. However, in cases where complicit actors engage in deception, the case study analysis indicates that access to law enforcement and national security information derived from domestic agencies or foreign partner agencies was required. Ultimately, the NPO sector's efforts to increase donor confidence through transparency are complimentary to efforts to protect the sector from terrorist abuse. Making more information on programmes and activities openly available results in better transparency, and this ultimately benefits efforts to detect abuse. However, as previously discussed, the research done for this report indicates that in instances where complicit organisations or individuals employ deception, the efforts of multiple actors, both domestic and foreign, are necessary to understand and halt significant cases of abuse.

Methods of Detection
NPO regulatory information
Open-source information
FIU and other financial information
National security information
Law enforcement information
Foreign information

185. Chapter 5 addresses the disruption of abuse. A substantial amount of abuse or risk of abuse is handled through administrative means or through preventive outreach, education, and self-regulation. Additionally, targeted sanctions have played a significant role in disrupting ongoing abuse, and mitigating the potential for future abuses. Given that only a small portion of abuse cases are dealt with through criminal prosecution, metrics relating to prosecutions are not reliable indicators of the total level of risk to the sector.

Methods of Disruption
Sector outreach, education and self-regulation
Criminal prosecution
Administrative enforcement, penalties, and sanctions

FUTURE WORK

186. This typologies report represents a substantial increase in our understanding of the threat posed by terrorist entities to the NPO sector. Additional research efforts can expand this understanding still further. For instance, there is a need for national-level studies of abuse in order to increase our understanding of individual jurisdictions, particularly those at a higher risk of terrorist activity. FATF Recommendation 1, which requires all member states to complete a national risk assessment, already supports this type of study. These studies will help determine unique indicators and examine further correlations. Additionally, there is a need to better assess the different threats (in terms of both risks and vulnerabilities) between jurisdictions that are net beneficiaries of NPO services and jurisdictions that are net donors. Finally, and not unrelated to the preceding observation, there is an emphasis on scrutinising outgoing NPO resources to guard against diversion. However, further research and analysis could be considered relating to incoming NPO resources in order to ensure that there is no affiliation with terrorist entities or terrorist activity, and thus continuing to protect the integrity of the NPO sector.

BIBLIOGRAPHY

WEB

1. BBC (2013), *Birmingham Men Guilty of Mass Bomb Plot,* BBC News (online), 2013-02-21, www.bbc.com/news/uk-21534048, accessed 2014-03.
2. Birmingham Mail (2013), 'Birmingham Terror Plot could have been 'Another 7/7'', *Birmingham Mail*, 2013-02-21, www.birminghammail.co.uk/news/local-news/birmingham-terror-plot-could-been-1337863, accessed 2014-03.
3. Dodd, Vikram and Taylor, Richard Norton (2011), 'Six Arrested in Birmingham Counter-terrorism Raids', *The Guardian*, 2011-09-19, www.theguardian.com/uk/2011/sep/19/anti-terrorist-police-arrest-birmingham, accessed 2014-03.
4. 'Jihadist Group says it Kidnapped ICRC Team' *SwissInfo* (Swiss Broadcasting Corporation,2014) www.swissinfo.ch/eng/politics/Jihadist_group_says_it_kidnapped_ICRC_team.html?cid=37935364 Accessed 2014-06.
5. LaVille Sandra (2013), 'Birmingham Terror Plotters' Profiles', *The Guardian*, 2013-02-21, www.theguardian.com/uk/2013/feb/21/birmingham-terror-cell-plotters-profiles, accessed 2014-03.
6. Mohammed, Arsham and Zakaria, Tabassum (2013), *US Issues Global Travel Alert, Cites Al Qaeda Threat*, Reuters (online), 2013-08-02, www.reuters.com/article/2013/08/02/us-usa-embassies-idUSBRE9710V320130802, accessed 2014-03.
7. Moor, Keith (2010), 'Charity used as a front to finance Sri Lanka's Tamil Tigers', *Herald Sun*, 2010-04-01, www.heraldsun.com.au/news/charity-used-as-front-to-finance-sri-lankas-tamil-tigers/story-e6frf7jo-1225848229678, accessed 2014-04.
8. Munro, Alan (1999), 'Humanitarianism and Conflict in a Post-Cold War World,' *International Review of the Red Cross, No.835*, www.icrc.org/eng/resources/documents/misc/57jq2s.htm, accessed 2014-03.
9. Pollinger, Zachary A. (2008), *From Balenciaga to Bombs: How Terrorist Groups are Exploiting the Global Counterfeit Goods Trade for Profit and Murder*, Harvard University, http://isites.harvard.edu/fs/docs/icb.../Pollinger%202490%20FINAL.doc, accessed 2014-03.
10. Office of the United Nations High Commissioner for Human Rights (2012), Press Release, "New Restrictions on NGOs are undermining human rights: Pillay" (Geneva, 25 April 2012) www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=12081&LangID=E, accessed 2014-05.
11. Samuels, David (2012), 'The New Mastermind of Jihad', *The Wall Street Journal* (Online), 2012-04-06,

http://online.wsj.com/news/articles/SB10001424052702303299604577323750859163544, accessed 2014-03.

12. SITE Monitoring Service (2014), *Shabaab Calls American Youth to Join them in Mujahideen Moments 5*, 2014-05-13, https://news.siteintelgroup.com/Jihadist-News/shabaab-calls-american-youth-to-join-them-in-mujahideen-moments-5.html, accessed 2014-05.
13. Stalinsky, Steven (2011), 'Al-Qaeda Military Strategist Abu Mus'ab Al-Suri's Teachings on Fourth-Generation Warfare (4GW), Individual Jihad and the Future of Al-Qaeda', *Inquiry & Analysis Series Report No. 698*, Middle East Media Research Institute, 2011-06-22, www.memri.org/report/en/0/0/0/0/0/0/5395.htm, accessed 2014-03.
14. Swissinfo (2014), 'Jihadist Group says it Kidnapped ICRC Team' *SwissInfo* (Swiss Broadcasting Corporation,2014) www.swissinfo.ch/eng/politics/Jihadist_group_says_it_kidnapped_ICRC_team.html?cid=37935364 Accessed 2014-06
15. West Midlands Policy Counter-Terrorism Unit (2012), *Plotters Accused of 'Pocketing' Charity Money*, media release, 2012-10-23, www.muslimaid.org/images/stories/pdfs/trial_update.pdf, accessed 2014-03.
16. Willets, John (2012), *Alleged Bomb Plot Surveillance Photo Released*, ITV, 2012-10-23, www.itv.com/news/central/topic/trial/?page=2, accessed 2014-03.
17. Young, Nicki May (2013), *Charity Commission Condemns 'Abhorrent' Abuse of Muslim Aid by Terror Plotters*, CivilSociety.co.uk, 2013-02-22, www.civilsociety.co.uk/fundraising/news/content/14526/charity_commission_condemns_abhorrent_abuse_of_muslim_aid_by_terror_plotters, accessed 2014-03.
18. Zelin, Aaron Y. (2013), *Meeting a Returned Tunisian Foreign Fighter from the Syrian Front*, Syria Deeply, 2013-11-08, http://beta.syriadeeply.org/op-eds/meeting-returned-tunisian-foreign-fighter-syrian-front/, accessed 2014-03.

BOOKS

19. Apuzzo, Matt and Goldman, Adam (2013), *Enemies Within: Inside the NYPD's Secret Spying Unit and Bin Laden's Final Plot Against America,* Touchstone, New York.
20. Balsamo, Richard R. and Brown, Max Douglas (2007), 'Risk Management' in Legal Medicine, 7th Ed. Moseby Elsevier, Philadelphia.
21. Bishop, Toby J.F. and Hydoski, Frank E. (2009), *Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption,* Wiley & Sons, Hoboken, USA.
22. Davies, Jonathan; Finlay, Mike; McLenaghen, Tara and Wilson, Duncan (2006), *Key Risk Indicators—Their Role in Operational Risk Management and Measurement*, ARM and Risk Business International Ltd, Prague.
23. Kepel Gilles (2002), *Jihad: The Trail of Political Islam*, I.B. Tauris and Co. Ltd., London.

24. Lia, Brynjar (2008), *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab Al-Suri,* Oxford University Press, Oxford, UK.

25. Michael, George (2012), *Lone Wolf Terror and the Rise of Leaderless Resistance,* Vanderbilt University Press.

26. Napoleoni, Loretta (2013), 'The Evolution of Terrorist Financing Since 9/11: How the New Generation of Jihadists Fund Themselves', *Terrornomics*, David Gold and Sean S. Costigan, eds., Ashgate Publishing, Aldershot, UK.

27. Sagemen, Marc (2008), *Leaderless Jihad: Terror Networks in the Twenty-First Century,* University of Pennsylvania Press.

28. Salamon, Lester M., *et al* (2003), *Global Civil Society: An Overview*, Centre for Civil Society Studies, Johns Hopkins University, Baltimore, USA.

29. Salamon, Lester M., *et al*. (2013), *The State of Global Civil Society and Volunteering: Latest Findings of the Implementation of the UN Nonprofit Handbook*, Centre for Civil Society Studies, Johns Hopkins University, Baltimore, USA.

30. Salamon, Lester M., *et al* (1999), *Global Civil Society: Dimensions of the Non-Profit Sector*, Centre for Civil Society Studies, Johns Hopkins University, Baltimore, USA.

31. Smith, Clifton and Brooks, David J. (2013), *Security Science: The Theory and Practice of Security* Elsevier, Oxford, UK.

32. Sparrow, Malcolm K. (2000), *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance*, Brookings Institution Press, Washington D.C.

33. Wittig, Timothy (2011), *Understanding Terrorism Financing*, Palgrave Macmillan, New York.

REPORTS AND OTHER PUBLICATIONS

34. Anheier, Helmut K. (2000), *Managing Non-Profit Organisations: Towards a New Approach, Civil Society Working Paper 1,* LSE Centre for Civil Society, London.

35. Asia/Pacific Group on Money Laundering [APG] (2011), *Typologies Report: NPO Sector Vulnerabilities*, Sydney, Australia.

36. Basile, Mark (2004), 'Going to the Source: Why Al Qaeda's Financial Network is Likely to Withstand the Current War on Terrorist Financing', *Studies in Conflict and Terrorism*, 27:3.

37. Carothers, Thomas and Brechenmacher, Saskia (2013) *Closing Space: Democracy and Human Rights Support under Fire* (Carnegie Endowment for International Peace, 2013) http://carnegieendowment.org/files/closing_space.pdf (Accessed 2014-04)

38. Center on Global Counterterrorism Cooperation *et al.* (2013), *To Protect and Prevent: Outcomes of a Global Dialogue to Counter Terrorist Abuse of the Nonprofit Sector*, CNGCC, United States, *p.v.* www.globalcenter.org/wp-content/uploads/2013/06/Protect-Prevent_Final.pdf

39. Crone, Manni and Harrow, Martin, 'Homegrown Terrorism in the West, 1989-2008', *DIIS Working Paper 2010:30,* Danish Institute for International Studies, Copenhagen.
40. de Schutter, Olivier; Ramastry, Anita; Taylor, Mark B. and Thompson, Robert C. (2012), *Human Rights Due Diligence: The Role of States*, International Corporate Accountability Roundtable/European Coalition for Corporate Justice/Canadian Network on Corporate Accountability.
41. Development, Concepts and Doctrine Centre (2013), *Global Strategic Trends Out to 2040*, 4th ed., Ministry of Defence, London.
42. Eurasian Group on Combating Money Laundering and Financing of Terrorism [EAG] (2012), *Misuse of Non-profit Organisations for Money Laundering,* Moscow.
43. FATF (2012a), *International Standards on Combating Money Laundering and the Financing ofTerrorism & Proliferation – the FATF Recommendations, (Recommendation 8 and Interpretive Note to Recommendation 8), FATF,* Paris.
44. FATF (2004), *Report on Money Laundering Typologies 2002-2003*, Paris.
45. FATF (2013b), *International Best Practices: Combating the Abuse of Non-Profit Organisations*, Paris.
46. FATF (2008), *Terrorist Financing*, Paris.
47. FATF (2012b), *Operational Issues—Financial Investigations Guidance*, Paris.
48. FATF (2013a), *National Money Laundering and Terrorist Financing Risk Assessment*, Paris.
49. Gomez, Juan Miguel del Cid (2010), 'A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates', Perspectives on Terrorism, 4:4.
50. Hegghammer, Thomas (2013), 'Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting', *American Political Science Review*, 107:1.February 2013.
51. Horgan, John and Taylor, Max, 'Playing the 'Green Card'—Financing the Provisional IRA, Part 1' *Terrorism and Political Violence*, 11:2, 1999.
52. Horgan, John and Taylor, Max, 'Playing the 'Green Card'—Financing the Provisional IRA, Part 2' *Terrorism and Political Violence*, 15:2, 2003.
53. Independent National Security Legislation Monitor (2013), *Annual Report 2013*, Commonwealth of Australia, Canberra.
54. Jenkins, Brian Michael (2011), *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism since 9/11,* RAND Corporation.
55. Mackintosh, Kate and Duplat, Patrick (2013), *Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action*, UN Office of the Coordinator of Humanitarian Affairs/Norwegian Refugee Council.

56. Mackintosh, Kate and Duplat, Patrick (2013), *Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action*, UN Office of the Coordinator of Humanitarian Affairs/Norwegian Refugee Council, 2013.

57. Makarenko, Tamara (2012), *Europe's Crime-Terror Nexus: Links between Terrorist and Organised Crime Groups in the European Union*, Directorate General for Internal Policies, European Parliament, Brussels.

58. Malet, David (2013), *Foreign Fighters: Transnational Identities in Civil Conflicts*, Oxford University Press, New York.

59. National Intelligence Council (2012), *Global Trends 2030: Alternative Worlds,* Office of the Director of National Intelligence, Washington DC.

60. Noble, Ronald K. (2003), The Links Between Intellectual Property Crime and Terrorist Financing, Public Testimony, House Committee on International Relations, 108th Congress, United States House of Representatives.

61. Precht, Tomas (2007), Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism, Ministry of Justice, Denmark.

62. *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/23/39 (United Nations General Assembly, 2013)

63. Rollins, John; Wyler, Liana Sun and Rosen, Seth (2010), *International Terrorism and Transnational Crime: Security Threats, US Policy, and Considerations for Congress*, Congressional Research Service, Washington DC.

64. Tonkiss, F. and Pacey, A. (1999), 'Trust, Confidence and Voluntary Organisations: Better Values and Institutions', *Sociology*, 33:2.

65. UK House of Commons (2006), Report of the Official Account of the Bombings in London on 7th July 2005, The Stationary Office, London, UK.

66. United Nations Office on Drugs and Crime (2012), *The Use of the Internet for Terrorist Purposes,* United Nations, New York.

67. Van der Does de Willebois, Emile (2010), 'Non-profit Organisations and the Combatting of Terrorism Financing: A Proportionate Response', *World Bank Working Paper No.208*, The World Bank, Washington D.C.

68. von Behr, Ines; Reding, Anais; Edwards, Charlie and Gribbon, Luke (2013), *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism,* RAND Europe, Cambridge.

OTHER LITERATURE REVIEWED

69. European Commission Directorate-General Justice, Freedom & Security (2008), *Study to Assess the Extent of Abuse of Non-Profit Organisations for Financial Criminal Purposes at EU Level*, Matrix Insight, 2008-04-03.

70. UK Home Office (2007), *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse, A Consultation Document*, May 2007.

71. UK Home Office and HM Treasury (2007), *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse, Summary of Responses and Next Steps*, December 2007.

72. UN Counter -Terrorism Implementation Task Force (CTITF), *Tackling the Financing of Terrorism*, October 2009.

APPENDIX A – CASE STUDIES

187. Research for this typologies report was conducted through multiple methods. The core of the research effort was the collection and analysis of case studies drawn mainly from FATF member states, but also through open-source research.

188. In response to a request for case studies that was distributed to FATF member states and FATF-style regional bodies (FSRBs), a total of 102 case studies were received from 14 states. The case study sample geographically spans Europe, North America, Africa, the Middle East, South East Asia, and Oceania. Additionally, case studies originated from different agencies, such as law enforcement, intelligence, and regulatory agencies.

189. Both sanitised and unsanitised case studies have been included in this report, in an effort to capture the benefits of both approaches.

190. The analysis of the case studies demonstrated several ways through which NPOs could be abused by terrorist entities. These methods and risks of abuse are:

- Diversion of Funds
- Affiliation with a Terrorist Entity
- Abuse of Programming
- Support for Recruitment
- False Representation

191. The 102 cases studies examined during this project are presented below. They have been grouped based on the methods and risks of abuse identified for each case study. Case studies often represented multiple methods of abuse and/or risk. However, for ease of reference, each case study has been placed in only one group, the method or risk of abuse deemed to be the most significant.

DIVERSION OF FUNDS

Case Study 1 - Diversion of Funds

A company, established in an offshore centre by a foreign individual, held a business account at a domestic bank. Cheques totalling USD 1.6 million were deposited to the account and invested long-term. The bank requested the identity of the ultimate benefactor but the account holder refused to provide this information.

Shortly afterwards, the account holder requested by fax that the bank transfer half of the funds to an account in his name at a foreign bank. Finding the case suspicious, the domestic bank disclosed STRs to the national FIU. Because of the urgent nature of the transfer request, the FIU instructed the bank to decline the transfer for a period of five days while it investigated.

The FIU's investigation revealed that the company had no formal domestic connections. Some of the cheques involved in the case had been written out by the account holder's brother who also resided abroad. The remaining cheques were in the names of foreign companies, all with connections to the

account holder's brother.

The transaction that was temporarily denied was ultimately not processed and law enforcement information stated that the account holder's brother was the founder of a foreign NPO, and that this NPO was believed to be involved in terrorism financing activities.

The investigation concluded that the account holder had likely acted as a nominee in order to conceal transactions ultimately carried out by his brother. This was done to obstruct further investigations into the brother's activities.

Case Study 2 - Diversion of Funds

A large foreign NPO with activities in more than 160 countries was raising funds with the official goal of supporting various social causes. The NPO was previously suspected of having close ties with terrorist groups throughout the world. More recently, a number of countries publicly accused the NPO of having diverted funds from donations intended for humanitarian aid projects to the benefit of a long-established terrorist organisation.

The bank of the NPO's domestic office sent STRs to the national FIU on a suspicious transactions made by the NPO and other organisations. Investigation by the bank and the FIU revealed that transactional links existed between all three NPOs. Doubts were raised as to the end use of the funds and the possibility that they had not been used to finance charitable work. Rather, it appeared that the funds had been used to finance terrorism, specifically to support the orphaned children and families of so-called martyrs.

Law enforcement authorities are investigating the case.

Case Study 3 - Diversion of Funds (Reproduced in Chapter 3)

STRs were submitted to the national FIU on the domestic branch of a foreign-based NPO, which was listed locally. The domestic NPO transferred funds to the banned foreign-based NPO through a bank account in a third country. It also transferred funds to NPOs in high risk areas and made cash withdrawals of large banknotes.

An investigation by the FIU revealed that directing officials of the domestic NPO carried large amounts of cash out of the country. In the financial intelligence reports relating to the cross-border movement of physical currency, the directing officials indicated that the funds were donations destined for charities located in both high risk and low risk areas.

The domestic NPO also transferred funds to a second local NPO. STRs submitted on the second NPO indicated that its directing officials transferred funds to individuals in developed countries in a region not related to the NPO's area of operation.

As a result of the investigation, the domestic NPO was listed as a supporter of terrorism and its assets were frozen.

Case Study 4 - Diversion of Funds

The national NPO regulatory body opened an investigation following media allegations that a domestic NPO had made payments to foreign organisations with alleged links to terrorism, including domestically and internationally listed organisations.

Scrutiny of the domestic NPO's books and records identified that funds had been set aside for payment to a listed organisation, though not yet transferred. While the NPO had provided funding to the same organisation, it was done so prior to its being listed. Had funds been paid out after the listing of the organisation, directing officials of the domestic NPO could have been subject to criminal charges.

In light the information arising from the investigation, previously approved payments to the listed organisation were not carried out.

Case Study 5 - Diversion of Funds

Two foreign nationals were directing officials of a domestic NPO. The bank at which the NPO's account was held noted that while making transactions, the individuals did not know the correct name of the account. Additionally, they had made deposits to the accounts with references in a foreign language, some of which made mention of terrorist activities.

An investigation by the national FIU found that the NPO account had received a number of donations in the form of transfers and cash deposits for humanitarian work in an area of conflict. It was further revealed that some of these NPO funds were withdrawn in cash.

Law enforcement authorities confirmed they had been investigating the NPO for alleged terrorism financing as funds were suspected of being transferred to support foreign terrorist training camps.

Case Study 6 - Diversion of Funds

An NPO applied to the national regulator for registration, stating that its purpose was to support and carry out religious, educational and humanitarian programs. The national regulator's attention was drawn by the fact that the NPO shared a name with a foreign organisation identified in open-source material as a supporter of foreign terrorist groups. Access to national security intelligence indicated that the NPO was connected to a network of organisations that were used to provide resources to foreign terrorist groups. However, the NPO was ultimately registered due to a lack of corroborating material.

While monitoring the NPO's registration, the regulator noted that the NPO had submitted incomplete and inconsistent mandatory reporting. As a result, an audit was conducted and revealed that much of the NPO's funds had come from a foreign organisation known to be a front for terrorist groups. Additionally, the NPO had consistently sent resources to two organisations that were listed terrorist entities. More generally, the NPO was unable to account for the final use of many of its resources, particularly those sent abroad.

As a result of these findings, the NPO was deregistered and the regulator shared material from the case with law enforcement and national security partners.

Case Study 7 - Diversion of Funds

A large number of cash deposits and wire transfers were made to the bank account of a local individual. The deposits and transfers were made by several individuals based locally and in the country of origin of the account holder. All the funds were withdrawn in cash by the account holder.

An investigation by the national FIU revealed that there was no apparent justification for the transactions, as the individual performed no commercial or other activities and received only a

small income from social benefits. One of the largest payments was from a directing official of a domestic NPO. Law enforcement information indicated that the directing official of the NPO was linked to a terrorist group.

It was determined through the investigation that the funds being transferred into the individual's account were intended for terrorism financing, with a portion of these funds being diverted from charitable donations to the domestic NPO.

Case Study 8 - Diversion of Funds

A domestic NPO was raising funds for charitable activities in foreign areas of conflict by way of donations.

An STR was filed by a bank after one of the directing officials of the NPO exchanged a large number of small banknotes into fewer large banknotes. The directing official stated that the funds were to be sent to 'a militant NPO'.

An investigation revealed that the funds were donations made to the NPO in cash, by bank transfers and credit card payments, and through alternative payment methods such as PayPal. Further investigation showed that the directing official travelled to an area of conflict soon after conducting the banknote exchange and did not declare the exportation of cash when leaving the country as required by law.

Case Study 9 - Diversion of Funds

A directing official of a domestic NPO, with signing authority on the NPO's account, attempted to make a large cash deposit into the NPO's account. The individual indicated that the funds were to be transferred to a lawyer for a real estate purchase. He was vague as to the origin of the funds, but made an indirect reference to donations. The bank refused to accept the deposit on the grounds that the branch where the deposit was attempted did not hold the account, and proceeded to file an STR which alerted the national FIU.

The FIU's investigation found that the same individual had made a number of large cash deposits directly into the NPO's account. But the FIU also found multiple cash deposits into the individual's personal account corresponding to NPO donations from private donors. The individual had made a number of international transfers from his personal account to a foreign individual with known links to a foreign terrorist group.

The FIU investigation determined that the NPO was used to raise funds that were then partially diverted to support terrorist activities overseas. The file was passed on to the appropriate law enforcement and judicial authorities for further investigation.

Case Study 10 - Diversion of Funds

A bank filed an STR following a transfer of funds made by a domestic NPO to a foreign-based NPO which was listed as a terrorist entity because of its fundraising efforts for a listed terrorist organisation.

A law enforcement investigation, conducted in cooperation with several domestic government agencies, concluded that the domestic NPO had transferred USD 800 000 to the listed foreign NPO. Directing officials of the domestic NPO admitted to providing funds for humanitarian relief. It was

determined, however, that the directing officials were unaware of the foreign NPO's status as a listed entity.

Authorities did not seek to prosecute the NPO's directing officials. However, to mitigate future risk of abuse, the directing officials increased their due diligence by becoming familiar with the list of designated terrorist entities and by seeking guidance from authorities on the transfer of funds to certain jurisdictions.

Case Study 11 - Diversion of Funds (Reproduced in Chapter 3)

A domestic company was established with very broad commercial purposes. Numerous small deposits were made to the company's account by the individual who had signing authority on the account. The funds were immediately transferred to foreign-based companies.

An investigation by the national FIU revealed that the individual with signing authority on the company's account was also a directing official of an NPO. It was suspected that the small deposits made on the company's account originated from fundraising by the NPO.

Law enforcement information indicated that the NPO was known to have ties to a terrorist group. A second directing official of the NPO, who was also a manager of the company, also had ties to the terrorist group.

The investigation concluded that the domestic company was a front company being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

Case Study 12 - Diversion of Funds

An individual's personal bank account received a large transfer of funds from a foreign national. After the transfer, the funds were gradually being withdrawn in cash. The individual was not known to be involved in business transactions and the amount of funds transferred was unusual for the account.

An investigation by the national FIU revealed that a directing official of an NPO held power-of-attorney privileges over the individual's account, and that numerous cash deposits had also been made to the account. Neither the NPO directing official nor the individual had incomes corresponding to the transfers and deposits on the account. Additionally, the NPO had previously come to the FIU's attention in relation to terrorism financing and money laundering investigations.

Law enforcement information indicated that the NPO, and this particular directing official, were already under investigation for activities connected to terrorism financing and money laundering. Based on the FIU investigation, it was determined that the NPO directing official was using the individual's account to mask his own transactions.

Case Study 13 - Diversion of Funds

A bank filed an STR after receiving information indicating that foreign nationals were obtaining funds to support a terrorist organisation in their country of origin. According to the information, the funds were received by cash deposit or wire transfer in varying amounts and from various individuals. They were then sent by courier or other means to the country in question or its neighbouring countries.

An investigation by the national FIU included analysis of the account of a directing official of a domestic NPO which was suspected of supporting the terrorist organisation in question. The investigation found that the activity on the official's account was consistent with the information received by the bank: small cash deposits were made by various individuals. The funds were then sent by wire transfer to the country in question or its neighbouring countries. Cash withdrawals were also made.

The case was transferred to law enforcement authorities who were conducting a concurrent investigation.

Case Study 14 - Diversion of Funds (Reproduced in Chapter 4)

A domestic NPO engaged in humanitarian activities abroad was sending money to a foreign partner in an area of conflict. A lead from the public to the national NPO regulator identified that the NPO had received a small donation from a known front organisation of a foreign terrorist group. Information contained in the NPO's obligatory reporting to the national regulator confirmed that the NPO had received this donation.

A short time later, a document obtained during an unrelated audit identified the NPO as a preferred funding conduit for the front organisation. The document's date corresponded with a dramatic increase in the NPO's donations. Open-source research and national security intelligence identified three of the NPO's representatives as being supporters of the foreign terrorist group, and identified the NPO's foreign partner as another front for that terrorist group.

A subsequent audit of the NPO by the national regulator found that the NPO had donated USD 700 000 to its foreign partner but was unable to account for the final use of these resources. The NPO was ultimately deregistered by the national regulator.

Case Study 15 - Diversion of Funds

A domestic NPO held several accounts on which the NPO's founder had signing authority. Cash deposits and transfers were made into the accounts by donors, and the transfers always indicated that the funds were destined for an area of conflict. The domestic NPO then sent large wire transfers to a foreign-based international NPO.

An investigation by the national FIU revealed that the founder of the domestic NPO wilfully used his role to facilitate the financing of terrorism and that the international NPO was the parent organisation of the domestic NPO. In addition, the international NPO was suspected of being linked to a terrorist network and one if its contacts had been listed as a supporter of terrorism.

Case Study 16 - Diversion of Funds

The national FIU received STRs from a bank concerning the accounts of several domestic NPOs. Numerous small deposits and transfers were being credited to the NPOs' accounts.

Law enforcement information indicated that one of the NPOs was suspected of having links to a terrorist organisation. An investigation by the FIU revealed that the small amounts credited to the NPOs' accounts were donations from individuals who wanted to send funds to an area of conflict for humanitarian purposes. The majority of the funds credited to the accounts were sent to the personal account of a directing official of one of the NPOs. The directing official then withdrew all

the funds in cash, making it difficult to determine the ultimate beneficiary of the funds.

It was believed that the financial system was being used to put funds into circulation, presumably to finance terrorist activities. The information was shared with investigating authorities for possible prosecution.

Case Study 17 - Diversion of Funds

An NPO carrying out domestic and international humanitarian and cultural work applied for and received registration from the national NPO regulator. One of the NPO's core activities was to run a domestic religious school. The regulator subsequently became concerned when the NPO's mandatory reporting indicated that the NPO had transferred funds to international organisations that were not legally approved beneficiaries.

The NPO was audited by the national regulator and it was determined that there were a number of compliance and risk-related issues. Examination of the NPO's programme information revealed that it was part of a network of domestic NPOs that often shared directing officials and acted collaboratively on projects. Some of the domestic organisations that the NPO was collaborating with were known to be associated with foreign terrorist entities. One individual employed as a directing official of the religious school was known to the regulator for engaging in activities that could encourage recruitment to terrorist activities. Some community groups also registered concern over elements of the school's curriculum, but a local law enforcement investigation determined that there was no intent on the part of the NPO to engage in activities supporting recruitment.

It was also determined that the NPO was not operating as an independent entity (as legally required), but as a branch of two larger foreign organisations. A substantial amount of the NPO's funds were transferred to the foreign organisations, and the books and records accounting for the subsequent use of the funds were kept by the foreign organisations rather than the NPO.

The national regulator determined that the compliance and due diligence shortcomings, lack of control of international operations, and collaboration with other organisations and individuals of interest left the NPO very vulnerable to exploitation. The regulator educated the NPO as to its legal and compliance obligations, and drafted a compliance agreement with the NPO to strengthen accountability and monitoring. The case is ongoing.

Case Study 18 - Diversion of Funds

A foreign individual held power-of-attorney privileges over a domestic NPO. The individual held two domestic personal bank accounts and was receiving funds from social service payments and cash deposits. The bank noted that the deposits to the individual's accounts were inconsistent with the fact that the individual had no known profession, and that most of the deposits referenced the telecommunications industry.

The national FIU began an investigation and determined that deposits into the NPO's account were consistent with donations. Also, most of the funds deposited into both the personal accounts and the NPO account were withdrawn in cash by the individual.

Law enforcement information revealed that the NPO was run by the individual as a religious institution, and that the individual performed religious services at the NPO. Law enforcement information also indicated that the NPO was linked to terrorist activity.

Case Study 19 - Diversion of Funds

Locally-based individuals were suspected of fundraising and procurement activities on behalf of a foreign terrorist organisation. A joint FIU and law enforcement investigation established that multiple individuals (the suspects) were sending large international wire transfers, ultimately intended to benefit a terrorist organisation abroad.

The investigation revealed that the majority of the funds raised by the suspects were by way of cash donations raised under the guise of charitable activities. Legitimate businesses, such as grocers, restaurants and hospitality venues, were also used for to raise funds for. The funds raised were transferred via direct debit into a central bank account held by the supposed NPO, an account opened by third- party nominees. The fundraising efforts were financed by cash, cheques and credit cards linked to the same account.

Examination of the NPO's main bank account activity also uncovered incoming funds transfers from other third-party individuals, as well as outgoing transfers to personal accounts, allegedly to cover expenses relating to the administration of the NPO. Funds from the central account were distributed by various means, including person-to-person, bank deposits and real estate purchases.

Also, international wire transfers were frequently ordered from the account, commonly via internet banking. The suspects were sending large international wire transfers to businesses abroad, businesses believed to be front organisations used to control funds for a terrorist organisation. The businesses would subsequently send wire transfers to the terrorist organisation in a third country.

Information from the national FIU identified numerous structured wire transfers to avoid reporting requirements, including more than USD 300 000 transferred by one individual in this manner. The international wire transfers were sent to several different bank accounts in the second country rather than to a central account.

The majority of the transactions were conducted in the suspects' own names. However, third parties were used to send wire transfers and conduct purchases using funds withdrawn from the central account.

As a result of the investigation, authorities arrested and charged several individuals with being members of a terrorist organisation, providing support or resources to a terrorist organisation, and making funds available to a terrorist organisation.

Case Study 20 - Diversion of Funds

Mehrdad Yasrebi was born in Iran and was a permanent resident of the United States. During 1994 Yasrebi started a NPO in the U.S., the Child Foundation, which was allegedly founded to care for impoverished orphans all over the world. Based upon an application by the subject, the IRS recognized the Child Foundation as a tax-exempt charitable non-profit organisation under section 501(c)(3) of the Internal Revenue Code in January 1995.

Because the Child Foundation received tax-exempt status, it was required to file a Form 990, Return of Organisation Exempt from Income Tax, with the IRS each year in which its gross receipts exceeded a minimum threshold. One purpose of the Form 990 information return was to enable IRS to exercise oversight authority over tax-exempt organisations.

Despite its claim that the Child Foundation was established to provide for impoverished orphans,

the investigation determined that it was, in fact, a means to transport funds to Iran to make investments in property and other items, as well as provide a portion of the funds directly to the Government of Iran, violating U.S. sanctions laws prohibiting the provision of funds to Iran, due to its ongoing support of international terrorism and other illicit activities. Yasrebi and the Child Foundation pleaded guilty to conspiracy on January 10, 2011.

Dr. Hossein Lahiji, a former Iranian citizen based in the U.S. was the largest donor to the Child Foundation. From approximately 1998 through 2007, Lahiji and his wife Najmeh Vahid contributed approximately USD 1.8 million to the Child Foundation. Lahiji and his Vahid deducted the "donations" on their tax returns for those years. Lahiji and Vahid were convicted of conspiracy to money laundering and conspiracy to defraud the U.S. after a two-week trial on June 27, 2013; they were subsequently sentenced to 12 months and a day imprisonment and required to forfeit USD 600 000. On December 30, 2013, Lahiji and Vahid pled guilty to additional charges in a separate matter and were sentenced to 12 months and a day imprisonment (served concurrently with the sentence in the prior matter), along with fines and restitution.

Case Study 21 - Diversion of Funds (Reproduced in Chapter 4)

An NPO was formed with the stated purpose of funding foreign humanitarian activities in an area of conflict. While analysing the NPO's obligatory reporting, the national regulator noted that the NPO had contravened its registration requirements by providing funds to organisations considered to be outside of the legally prescribed set of beneficiaries.

The national regulator audited the NPO while concurrently accessing national security intelligence. Intelligence material indicated that the NPO was suspected of belonging to a network of humanitarian organisations that was sympathetic to, and influenced by, a foreign terrorist organisation operating in the same area of conflict. The audit revealed that the NPO had sent over USD 600 000 to a known front organisation for a foreign terrorist group. The front organisation itself was a listed terrorist entity in several countries. Additionally, the audit found that the NPO was unable to account for the ultimate use of much of its donated resources.

Based on its investigation, the national regulator deregistered the NPO and shared relevant material with national security partners.

Case Study 22 - Diversion of Funds (Reproduced in Chapter 3)

A domestic NPO was established to support charitable work in foreign areas of conflict.

An investigation by the national FIU, initiated by suspicious transaction reporting, revealed that locally collected funds were being transmitted to foreign-based charitable organisations. The investigation also uncovered that, once the funds were received by the foreign-based charitable organisations, they were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation.

While there were established connections between the foreign-based charitable organisations and the terrorist organisation, direct links between the domestic NPO and the terrorist organisation could not be substantiated.

Case Study 23 - Diversion of Funds

A bank filed an STR pertaining to a returned payment made on a transaction by a humanitarian relief NPO to a foreign organisation. The transaction was declined because the NPO, which initiated the transaction, was on a watch list of entities suspected of financing terrorist activities.

Most of the funds received by the NPO appeared to be donations from individuals wanting to support a legitimate humanitarian cause. The funds were therefore assumed to be of legal origin. However, further analysis revealed that the president of the NPO was also treasurer of a second foreign organisation, which was also on several watch lists. This individual had previously been identified because of anti-government activities in his country of origin and because he had made radical statements on a number of occasions.

Bank transactions made by the NPO, as well as those made by the second foreign organisation, were suspected of being linked to terrorist activities. The case was referred to law enforcement authorities for further investigation.

Case Study 24 - Diversion of Funds

According to media reporting, a domestic organisation was soliciting donations for, and participating in, an 'aid convoy' abroad.

While the organisation did not recognise itself as an NPO, having reviewed the terms upon which its funds were being raised, the national regulator determined that the organisation was, in fact, an NPO and was legally required to register as such.

However, the regulator had concerns that the organisation would not satisfy the statutory requirements to be registered as an NPO. The regulator was concerned with the political nature of the aid convoy. Specifically, the regulator was concerned that the NPO's directing officials could carry out NPO activities in support of the political arm of a terrorist organisation.

The regulator identified that funds donated to the organisation through its website were transferred to the account of a non-charitable entity established to campaign against wars. The regulator was concerned that a significant funds were being held and controlled by a non-charitable organisation that ostensibly had political objectives, and was potentially sympathetic to the terrorist organisation that controlled much of the territory that the aid was being transferred into.

Case Study 25 - Diversion of Funds

Representatives of a foreign-based listed terrorist organisation were raising funds from members of the local diaspora through several domestic NPOs established as community and cultural centres.

A law enforcement investigation revealed these individuals, who were also from the local diaspora, transferred funds through the NPOs to entities affiliated with the terrorist organisation which were located in a foreign jurisdiction.

The wire transfers were structured to avoid reporting thresholds and the generation of financial intelligence reports. The transaction information was nevertheless captured by the national FIU, enabling authorities to follow the flow of funds and identify the individuals involved.

Case Study 26 - Diversion of Funds

The domestic branch of an international NPO used its provision of social services to solicit donations and public support. As part of its operations, the domestic branch solicited donations in response to a natural disaster in a foreign country where a listed terrorist group is active. The domestic branch was identified to the national FIU by law enforcement authorities as a possible front for the listed terrorist group.

Large cash transactions reported to the FIU in the immediate aftermath of the natural disaster indicated that the domestic branch deposited approximately USD 100 000 into its account. Given the timing of these deposits, it is believed that the funds were likely solicited as donations for disaster relief. The domestic branch then ordered an EFT of approximately the same amount to the benefit of the international NPO's branch in the foreign country affected by the disaster.

Analysis by the FIU uncovered links between the international NPO and a group of individuals involved in a suspected procurement scheme on behalf of the listed terrorist group. Open source information indicated that one of the individuals involved in the procurement scheme had solicited donations on behalf of the international NPO. Another individual involved in the procurement scheme was a director of an NPO that had transferred over USD 20 000 to a third-party organisation linked to the international NPO.

According to suspicious transaction reporting, following the listing of this international NPO by a foreign country in relation to terrorist financing activity, the domestic branch issued a cheque for a large amount of funds to a known fundraiser for the international NPO.

Case Study 27 - Diversion of Funds

A registered domestic NPO provided a group of its volunteers with fundraising materials including collection buckets, identity badges and letters of credential. These individuals purported to raise funds and other goods in support of individuals affected by a humanitarian crisis on behalf of the NPO. In addition to fundraising, the volunteers were tasked with distributing the donations to those in need.

The NPO's directing officials had minimal oversight of the activities of its volunteers including the distribution of donations, evidenced by a lack of records. The directing officials were unable to show that the funds and goods raised were distributed for the intended purposes and could only rely on the accounts provided by its volunteers.

A national NPO regulator examination found that one of the volunteers retained control over the NPO's fundraising material in contravention of a domestic designation, which included financial sanctions, based on suspected links to terrorism. The NPO regulator alerted the NPO's directing officials to the designation and advised them to take action to ensure that any property belonging to the NPO was recovered and to prevent further financial activity in breach of domestically-imposed sanctions.

The possibility of the designated individual having used the NPO's fundraising materials to collect and solicit donations in support of terrorism cannot be discounted.

Case Study 28 - Diversion of Funds (Reproduced in Chapter 3)

A domestic NPO was raising funds ostensibly for humanitarian relief in an area of conflict. The NPO used collection boxes outside religious institutions to solicit donations. The funds raised were held in a domestic bank account.

The founder of the NPO is suspected of diverting the funds raised to facilitate terrorism rather than using them for the stated humanitarian activities.

A law enforcement investigation resulted in the arrest of the founder of the NPO for terrorism facilitation offences. The case is still under investigation. While to date there has been no conviction, USD 60 000 in collected funds were seized.

Case Study 29 - Diversion of Funds

Over a period of three days, three domestic citizens, arriving at the airport, declared a total of USD 120 000 in cash to customs officials. All three individuals indicated that the funds originated from a foreign NPO, doing humanitarian work in areas of conflict, an area where terrorist groups were known to be active.

The customs officials forwarded disclosures to the national FIU regarding the cash importations. An investigation by the national FIU determined that all three individuals had accounts with domestic banks, and that funds has previously been transferred into their accounts from a domestic extremist religious organisation connected to the foreign NPO.

Over a year, nearly USD 27 000 cash was withdrawn from the individuals' accounts, and subsequently transferred to different jurisdictions with movements supported by the domestic extremist religious organisation. National security intelligence indicated that the three individuals were active members in a local extremist religious movement. Additionally, the FIU in the foreign jurisdiction where the foreign NPO was based shared information indicating that the foreign NPO shared directing officials with, and was closely connected to, a second NPO that had been listed as a supporter of terrorism.

Based on the investigation, the national FIU forwarded the case to judicial prosecutors. After forwarding the case, the national FIU received several more disclosures regarding similar suspected cash couriers carrying funds for the same NPO. These funds were bound for other areas of conflict, in support of similar religious movements.

Case Study 30 - Diversion of Funds (Reproduced in Chapter 4)

A domestic NPO was one of many branches of a foreign-based, international NPO established to help rehabilitate people affected by internal conflict in the foreign country.

When the foreign country was affected by a natural disaster, the domestic branch collected and transferred funds back to the international NPO's home office in the affected area.

International press reports identifying an affiliation between the international NPO and a terrorist group led to an investigation by the national FIU. The investigation revealed that a significant sum of funds had been transferred from the domestic NPO, through several intermediary accounts, to accounts belonging to members of the terrorist group.

The investigation, however, was unable to determine whether the directing officials of the domestic NPO had knowledge of the ultimate destination of the funds transfers.

Case Study 31 - Diversion of Funds

A domestic NPO with international operations was raising funds through public solicitations and donations from other international organisations. The NPO was suspected of transferring funds to an international partner organisation that was suspected of providing assistance to terrorist combatants.

An investigation by law enforcement authorities and the national NPO regulator uncovered that the directing officials of the domestic NPO also managed an unrelated business. Funds from the NPO's accounts were being diverted into the business' account, providing the directing officials with income. The directing officials were subsequently charged with various offences relating to fraud.

Case Study 32 - Diversion of Funds (Reproduced in Chapter 3)

A domestic NPO was established to provide a place of religious worship for a diaspora community that had come from an area of conflict, and to raise and disburse funds for humanitarian causes.

The national NPO regulator became suspicious when the NPO's mandatory reporting indicated that it had sent funds to organisations that were not legally prescribed beneficiaries. These funds were sent ostensibly in response to a natural disaster that had affected the diaspora community's homeland. One of the beneficiary organisations, however, was believed to be the domestic branch of an international front organisation for a foreign terrorist group operating in the diaspora community's homeland.

The regulator audited the NPO and discovered that it had sent funds to five organisations or individuals that were not legally prescribed beneficiaries. This included USD 50 000 sent to the international front organisation through the domestic branch, and USD 80 000 sent directly to the front organisation's headquarters branch located in the area of conflict.

While the audit was ongoing, the regulator received two leads from the public regarding the NPO. Both leads cited concerns regarding the opacity of the NPO's leadership, and that decisions to send funds overseas had circumvented normal accountability procedures set out in the NPO's governing documents. One of the leads indicated that a shift in the demographic of the diaspora community had meant a new faction had gained control of the NPO's board of directors. This faction was more sympathetic to the cause of the foreign terrorist organisation. While these issues had already been noted through the regulator's audit, the leads supported the regulator's concerns regarding the NPO's management.

The NPO leadership replied to the regulator's concerns by stating that the exigencies of responding to a natural disaster had led the NPO to bypass some internal procedures and to work with whichever organisations could operate in the affected areas. Taking this into consideration, the NPO retained its registration but was forced to pay penalties. The NPO also entered into a compliance agreement with the regulator that would enforce strict due diligence and accountability standards.

Case Study 33 (Reproduced in Chapter 2)

In 2011, West Midlands Police, in collaboration with the British Security Service and the London Metropolitan Police Service, began an investigation into several individuals based in Birmingham. [1] Two of the principal subjects of the investigation, Irfan Naseer and Irfan Khalid, had made trips to Pakistan in 2009 and 2010, where they had recorded suicide videos and attended training in preparation for terrorist activity.[2] Physical and technical surveillance of Naseer, Khalid, and co-plotter Ashik Ali uncovered a significant plot to detonate up to eight explosive devices in crowded places around Birmingham.

Physical surveillance revealed that Naseer, Khalid, and Ali were engaged in street fundraising for the large UK charity Muslim Aid.[3] Investigators found that the plotters had volunteered with Muslim Aid as fundraisers, obtaining donation buckets and high-visibility vests with the charity's name on them. The three men gathered donations over the course of a single day and had returned USD 2 500 in donations to Muslim Aid.

However, before returning the donation buckets and vests, and unbeknownst to Muslim Aid, the three men continued to fundraise for several more days posing as Muslim Aid volunteers. The donations collected over these subsequent days were deposited into the plotters' personal bank accounts. In total, they diverted USD 23 000[4] in donations to finance the bomb plot.[5] A similar scheme was also used to defraud a second charity, Madrasah-e-Ashraful Uloom.[6]

In September 2011, police disrupted the bomb plot, arresting Naseer, Khalid, Ali, and several other suspects. The three were convicted on terrorism charges in February 2013, and sentenced to prison terms ranging from 15 years to life.7

After the 2011 arrests, police made Muslim Aid aware that the organisation had been abused by the bomb plotters. Muslim Aid filed a serious incident report with the Charity Commission of England and Wales, which is the national regulator of charities in the UK.[8] The Commission worked with the charities involved to review and strengthen their safeguards to mitigate the risk of future abuses.

Notes:

1. Dodd, Vikram and Taylor, Richard Norton (2011); Birmingham Mail (2013).
2. LaVille, Sandra (2013).
3. Willets, John (2012).
4. For the purposes of consistency, all currencies in this report have been converted to US dollars (USD).
5. West Midlands Policy Counter-Terrorism Unit (2012).
6. Young, Nicki May (2013).
7. BBC (2013).
8. Young, Nicki May (2013).

Case Study 34 - Diversion of Funds

A domestic NPO, established to support the humanitarian needs of orphans, was subject to an inspection visit by the national NPO regulator.

The national regulator uncovered multiple legislative violations that led to the suspicion of support for terrorism financing. The NPO began operations before being licensed and failed to file the required financial statements with the competent authorities. It raised funds and sent and received funds transfers without appropriate approval. In addition, the NPO failed to use banks approved by the national regulator and used personal bank accounts belonging to directing officials and staff when conducting transactions relating to the NPO's activities. The regulator's investigation also

revealed that the NPO had undertaken projects and activities, including political activities, which were inconsistent with its reported purposes. It also had unreported foreign partners.

In light of these findings, the national regulator froze the bank accounts of the NPO, temporarily shut down its operations, and changed its board of directors.

Case Study 35 - Diversion of Funds

An NPO came to the attention of the national NPO regulator after transferring significant funds into a foreign area of conflict through organisations outside its legally prescribed set of beneficiaries.

The national regulator audited the NPO and determined that on multiple occasions it had provided significant funds to a known terrorist front organisation that was operating in the area of conflict. It was also determined that the NPO could not adequately account for the final use of these resources.

After completing its audit, the national regulator levied financial penalties on the NPO. The regulator also entered into a compliance agreement with the NPO, stipulating stricter due diligence and accounting requirements.

Case Study 36 - Diversion of Funds (Reproduced in Chapter 3)

In response to a humanitarian disaster, a large international NPO was providing aid by way of cash payments to beneficiaries in areas controlled by a terrorist organisation. The NPO delivered the cash payments through a local MSB.

An examination of the humanitarian relief programme, carried out by one of the NPO's partner organisations on its behalf, raised concerns. The examination revealed that in certain instances the MSB was deducting a 'tax' to be passed on to a listed organisation. In other instances, the beneficiaries of the charitable funds were being 'taxed' by representatives of the terrorist organisation themselves following the receipt of the financial aid. The examination also found that there was a general understanding and acceptance that a proportion of charitable funds would be diverted for terrorist purposes and that this was common practice amongst NPOs and related organisations working in the area.

Following a joint investigation by the national NPO regulator, the national FIU and law enforcement, the NPO was advised of its responsibilities with regards to reporting such incidents, and training for its staff in order to better safeguard against similar future incidents.

Case Study 37 - Diversion of Funds

According to an STR, an individual was operating an online account that accepted donations then distributed them to donors' NPOs of choice. The individual was a directing official of numerous for-profit businesses as well as two NPOs that were benefitting from online account.

The STR was reported based on the fact that one of the two NPOs did not declare income or expenditure until 2011, even though it was established in 2007 and the subject had made substantial donations to this organisation. Also, the second NPO was religious-based organisation that operated domestically and abroad, in areas of conflict with known terrorist activity.

Case Study 38 - Diversion of Funds

A domestic bank filed an STR after receiving information from a foreign authority that a domestic NPO was raising funds for a foreign-based terrorist organisation and that a directing official of the NPO publicly supported one of the conflicting parties in the country where the terrorist organisation was based. The information received by the bank also indicated that, to support the terrorist organisation, funds received by the NPO were being sent via courier or other means directly to the country where the terrorist organisation is located or to one of its neighbouring countries.

An investigation by the national FIU found that the financial transactions on the NPO's account were consistent with the information provided by the foreign authority: funds received by the NPO from a number of individuals were transferred to the above-mentioned neighbouring countries. It was therefore suspected that the funds raised by the NPO were being used to support terrorist activities.

The case was transferred to law enforcement authorities who incorporated it into an ongoing investigation.

Case Study 39 - Diversion of Funds

An NPO conducting humanitarian activities abroad applied for registration to the national NPO regulator. While reviewing the NPO's application, the regulator noted that there was very little information provided regarding the applicant NPO's activities. From the information that was provided, it became clear that the applicant NPO's principal purpose was to fundraise domestically, and turn over the funds to a foreign organisation, which operated in an area of conflict where a listed terrorist group was known to have substantial control.

The regulator was also able to determine that the applicant NPO was cooperating with an already-registered organisation. Cash donations meant for the applicant NPO were being accepted by the registered organisation who could then issue receipts to donors. The registered organisation then forwarded the funds to the applicant NPO. The registered organisation had been recently audited, and found to have transferred funds to a known front for the same listed terrorist group. A directing official of the applicant NPO had formerly been a directing official of the registered organisation. Similarly, another of the applicant NPO's directing officials was associated with a second registered organisation that had been audited and found to have transferred funds to the same front for the listed terrorist group.

The national regulator replied to the applicant NPO stating that it required further detailed information regarding the NPO's activities and its cooperation with foreign and domestic partners. The NPO subsequently withdrew its application for registration.

AFFILIATION WITH A TERRORIST ENTITY

Case Study 40 - Affiliation with a Terrorist Entity (Reproduced in Chapter 5)

Islamic American Relief Agency (IARA, formerly the Islamic African Relief Agency) is an Islamic charitable organisation with international headquarters in Khartoum, Sudan and its US branch (IARA-USA) was headquartered in Columbia, Missouri. IARA-USA was registered in the U.S. as a tax-

exempt charitable non-profit organisation under section 501(c)(3) of the Internal Revenue Code.

On October 13, 2004 the entire IARA organisation, along with five of its international representatives, were designated by the U.S. Department of the Treasury pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including al Qaida. IARA is formerly affiliated with Maktab Al-Khidamat (MK), which was co-founded and financed by Usama bin Laden (UBL) and is the precursor organisation of al Qaida. Records indicate several years of cooperation among IARA, MK, and UBL, starting in 1997, including a fundraising trip in 2000 during which one of IARA's Afghanistan leaders accompanied the Afghanistan MK leader to Sudan and other locations in the Middle East and raised USD 5 million for MK activities. Additional information indicates an IARA leader was involved in discussions to help relocate UBL to secure safe harbour for him. Among others, these discussions included representatives for UBL and MK, along with Lajnat al-Dawa (LDI). In addition, a Sudanese individual travelled to Mali and stayed with an IARA director while assessing whether Mali could serve as a safe harbour for UBL. Evidence also shows that as of early 2003, IARA was responsible for moving funds to the Palestinian territories for use in terrorist activities, notably serving as a conduit to Hamas in one Western European country. In part, funds were raised through IARA collection boxes marked “Allah” and “Israel ,” signalling the funds would be directed towards attacks against Israelis. Within the last year, IARA was reportedly linked to the Belgium office of the Al-Aqsa Foundation.

In addition to the terrorism designation of the IARA organisation, numerous individuals related to the IARA-USA branch have since been convicted of violating U.S. laws. In 2005-2007, IARA unsuccessfully challenged its designation through litigation, losing in both federal district and appellate courts.

IARA-USA violated sanctions prohibiting, among other things, the unauthorized transfer or attempted transfer, directly or indirectly, of money or goods to Iraq by U.S. persons under Iraqi Sanctions Regulations, pursuant to the U.S. International Emergency Economic Powers Act (IEEPA). For the entirety of the Iraqi Sanctions Regulations, IARA solicited donations through various means, including pamphlets, flyers, newsletters and personal correspondence, requesting contributions to pay for projects in Iraq.

In June of 2010, Defendant Mubarak Hamed, a naturalized U.S. citizen and former Executive Director of IARA-USA, pleaded guilty to conspiracy to violate the IEEPA and additionally obstructing or impeding administration of internal revenue laws. Hamed, as Executive Director, oversaw funding for projects in Iraq for the duration of the Iraqi Sanctions Regulations. Through his guilty plea, Hamed admitted that beginning at least as early as January 1, 1997 through October 13, 2004, he corruptly endeavoured to impair and impede the due administration of the internal revenue laws by using IARA-USA’s 501(c)(3) tax-exempt status to solicit funds, representing that they were legitimate charitable contributions, and to misuse part of those funds by transferring those funds to Iraq. Hamed further admitted that he continued the corrupt endeavour by omitting from IARA-USA’s tax forms filed with the IRS, material information regarding IARA-USA’s transaction with persons and entities in Iraq, and regarding IARA-USA’s control, history and affiliations.

In April of 2010, Defendant Ali Mohamed Bagegni, a naturalized U.S. citizen, pleaded guilty to conspiracy to violate U.S. sanctions pursuant to IEEPA from 1991 to 2004. Bagegni was associated with IARA, serving on the Board of Directors, which was responsible for overseeing the activities of

IARA-USA.

In July of 2010, Defendant Abdel Azim El-Siddig pleaded guilty to conspiracy to violate the Foreign Agents Registration Act. Through his guilty plea El-Siddig admitted that he entered into a conspiracy with Defendants Siljander and Hamed, to hire Siljander to act as the agent of a foreign principal. El-Siddig knew that his conduct was unlawful because Siljander had not registered with the Attorney General, such activities had not been reported to the proper authorities, and because the conspirators concealed the payments for Siljander's advocacy from the U.S. government.

On December 17, 2009 Ahmad Mustafa, a citizen of Iraq and a lawful permanent resident alien of the United States, pleaded guilty to illegally transferring funds to Iraq in violation of U.S. sanctions. Mustafa worked as a fund-raiser for IARA and travelled throughout the U.S. soliciting charitable contributions.

Case Study 41[1] (Reproduced in Chapter 5)

Methods of Disruption observed:

Administrative Enforcement and Penalties

The Povrel Jerusalem fund for the Afflicted and Needy (JFHS) was established in 1992 and purported to carry out humanitarian activities through partner organisations in the Palestinian Territories. In 1992, JFHS applied for charitable registration to the Canada Revenue Agency (CRA), which is the national regulator of charities in Canada. While reviewing JFHS's application, CRA became concerned that JFHS's purposes and activities were primarily political in nature, and therefore not charitable according to Canadian law. Also, the organisations that JFHS was partnering with in the Palestinian Territories were not considered legal beneficiaries under Canadian law. Information derived from open-source research indicated that some of JFHS's international partners were part of a fundraising network run by Hamas, a listed terrorist entity in Canada.[2] Through multiple communications with CRA, JFHS was repeatedly unable to show that it could maintain the legally required level of direction and control over its resources.

In 1998, CRA notified JFHS that it was unlikely to receive registration. A short time after this notification, a second NPO, the International Relief Fund for the Afflicted and Needy-Canada (IRFAN-Canada), applied for charitable registration. IRFAN-Canada was granted registration in 1999 while JFHS was still pursuing its separate application. When CRA again advised JFHS in 2000 that it was unlikely to receive registration, JFHS abandoned its application. Without notifying CRA, JFHS then turned over its assets to IRFAN-Canada, both organisations passed resolutions formally consolidating their operations, and several directing officials from JFHS began to manage IRFAN-Canada programs.

In 2003, open-source media began to indicate that JFHS and IRFAN-Canada had merged, and that IRFAN-Canada was connected to Hamas. CRA's analysis of IRFAN-Canada's mandatory annual reporting verified that there was reason for further concern. CRA audited IRFAN-Canada in late 2003 and identified several significant compliance problems. IRFAN-Canada was transferring significant resources to foreign organisations without maintaining adequate control of, or accounting for, the final use of the resources. Some of these foreign organisations were believed to be controlled by Hamas. IRFAN-Canada retained its registration after agreeing to put in place changes to their due diligence and accounting activities.

In 2009, CRA began a substantial follow-up audit of IRFAN-Canada to verify that the problems identified in 2003 had been addressed. CRA examined financial records, digital records, and programme material derived from the domestic and international offices of IRFAN-Canada. This material was combined with substantial open source research and assessments provided by partners[3].

CRA's 2009 audit of IRFAN-Canada revealed numerous serious compliance problems. These problems included, but were not limited to, the following:

- Between March 2006 and April 2007, IRFAN-Canada transferred, through a local partner, over USD 500 000 to the HAMAS-controlled Ministry of Telecommunications in Gaza, which was involved with distributing funds to the families of HAMAS fighters through the post office system.
- During the same period, IRFAN-Canada transferred over USD 160 000 through a local partner to the HAMAS-controlled Ministry of Health in Gaza.
- IRFAN-Canada continued funding to the Ramallah Zakat Committee, allocating over USD 77 000 to the Committee in 2007. CRA had notified IRFAN-Canada in 1998 and 2004 that the Committee was believed to be affiliated with Hamas, and IRFAN-Canada had told CRA that cooperation with the Committee had stopped as of 2004. Records showed that they renewed the relationship one month after the end of CRA's original audit.
- In 2007, IRFAN-Canada provided new computers and office equipment to the Al Muntada At-Tahqafi Cultural Forum after the Israeli military raided its offices and the Forum was made an unlawful association in Israel because of its close ties to Hamas. The equipment cost over USD 15 000.
- In 2007, IRFAN-Canada provided resources valued at over USD 8 600 000 to the Zakat Fund, Lebanon, which had been listed as an unlawful association in Israel for supporting Hamas.

In addition, records obtained during the audit showed that the directing official of IRFAN-Canada's West Bank office, who had signing authority for the organisation's accounts, had misappropriated over USD 100 000 of IRFAN-Canada's funds. This directing official had a known connection with Hamas organisations.

Based on the findings of the 2009 audit, CRA initially suspended and ultimately revoked IRFAN-Canada's charitable registration in 2011.

In 2014, the Government of Canada listed IRFAN-Canada as a terrorist entity under its Criminal Code based in part on CRA's findings that IRFAN-Canada provided support to Hamas, a listed terrorist organisation.

Notes:

1. This case study was developed entirely from the open source documents cited and was not developed from any state's response to the request for case studies. See CRA's administrative fairness letter to IRFAN-Canada dated 2010-12-10, and available at www.globalphilanthropy.ca/index.php/blog/comments/international_relief_fund_for_the_afflicted_and_needy_canada_irfan-canada_h/ (Accessed 2014-03).
2. al-Muqawama al-Islamiya (Hamas). See Public Safety and Emergency Preparedness Canada's website: www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx (Accessed 2014-03).
3. International Relief Fund for the Afflicted and Needy (Canada) v. Canada (National Revenue), 2013 FCA 178 [Docket A-20-13] https://www.canlii.org/en/ca/fca/doc/2013/2013fca178/2013fca178.html (Accessed 2014-06-18).

Case Study 42 - Affiliation with a Terrorist Entity

Through monitoring the development of a foreign court case, the national NPO regulator was alerted to the fact that a domestic organisation had significant ties to a foreign network suspected of funding terrorist entities. Based on this linkage, the regulator began to examine a sub-network of domestic NPOs that shared directing officials, properties, and other resources. At the same time, the regulator received a lead from the public concerning the foreign connections of the same group of organisations.

Further public leads identified one directing official in particular as engaging in suspicious financial activity, including keeping undisclosed bank accounts for foreign currencies, misappropriating NPO funds, and supporting speakers that promoted recruitment to violence. As part of the wider investigation, one of the NPOs was audited and problems were noted with the NPO's control of its resources. It was also assessed that some of the NPO's leadership were deceptive with information provided during the audit. Additionally, a foreign organisation being funded by the NPO was believed to be connected to terrorist entities in a foreign area of conflict. Based on these findings, the NPO was deregistered and material from the investigation was provided to other national security partners.

Case Study 43 - Affiliation with a Terrorist Entity

A domestic NPO carrying out cultural activities applied for registration to the national NPO regulator. Upon reviewing the NPO's application, the regulator became concerned that the NPO's actual intent was to carry out political activities.

Access to national security intelligence revealed that the NPO was part of a larger network of organisations with overlapping directing officials. Several of these directing officials were known to be associated with prominent members of a listed terrorist organisation. Several of the organisations in this network were believed to be run under the auspices of an international NPO that was a known front for the same listed terrorist organisation. Additionally, the NPO's reported premises were a known meeting place for supporters of the listed terrorist organisation.

After a substantial review of the NPO's application, the national regulator determined that while there were several significant areas of risk, there was, at that point, no verified information linking the NPO to terrorist activity. The regulator notified the NPO of its concerns and the NPO made changes to its purposes and activities, and was subsequently registered. Because of the identified risks however, the NPO's mandatory reporting and activities were regularly reviewed by the regulator.

During the course of reviewing the NPO's activities, open source research determined the identity of the NPO's religious leader, and national security intelligence indicated that this individual was closely associated with the listed terrorist organisation. Additional information from foreign partners also indicated that a senior member of the same listed terrorist organisation had, in the period since the NPO's registration, become involved with the NPO. The case is being reviewed by the national regulator and is ongoing.

Case Study 44 - Affiliation with a Terrorist Entity (Reproduced in Chapter 3)

In January 2005, the Australian Federal Police (AFP) received a letter of complaint from the Sri Lankan High Commission requesting that the AFP investigate alleged fundraising activity in Australia by the Liberation Tigers of Tamil Eelam (LTTE). The letter contained references to an international network of 'special task forces' fundraising by the LTTE under the guise of the Asian tsunami disaster relief, involving persons in France, Italy, Denmark, Norway, Germany, England, Switzerland, Sweden, the Netherlands and Australia. As a result of the letter, the AFP Joint Counter Terrorism Team in Melbourne commenced an investigation into the allegations.

An investigation ascertained that the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was a cover organisation for the LTTE. The TCC solicited funds from, and coordinated radio and print material for, the Tamil community in Australia. It also lobbied politicians regarding Tamil independence in Sri Lanka and procured electronic and marine equipment on behalf of the LTTE. Hundreds of Australian-based Tamils were persuaded to contribute monthly direct-debit payments to the TCC. The TCC also used charity tins to collect money roadside, and in shopping centres.

Reportedly, the Australian arm of the LTTE was run by three men: courier Aruran Vinayagamoorthy, Tamil community newspaper editor Sivarajah Yathavan and accountant Arumugan Rajeevan. The same men also were involved in directing the operation of the TCC. Raids on their homes uncovered video footage of Rajeevan and Yathavan firing a machine gun on board an LTTE gunboat in Sri Lanka and visiting one of the group's terrorist training camps. Also uncovered were photographs of Vinayagamoorthy and Rajeevan posing with LTTE founder Velupillai Prabhakaran. Vinayagamoorthy was recorded telling an associate that "[the] TCC are the Tigers and the Tigers are TCC."

Vinayagamoorthy and Yathavan ultimately plead guilty to providing the LTTE with more than USD 1 million. Vinayagamoorthy also admitted to providing the LTTE with electronic devices, at least one of which was used to make and detonate a bomb used in a terrorist attack.

From an NPO regulatory perspective, the TTC case encompassed multiple (red flag) indicators of risk: it facilitated the transfer of funds to a developing country with an established presence of terrorism; it collected funds in relation to disaster situations; and it was an ethnocentric organisation whose members and supporters did not approve of the listing of an organisation.

This case involved the use of financial intelligence from Australian Transaction Reports and Analysis Centre (AUSTRAC) to monitor the flow of funds out of Australia.

Note:

This case is drawn from a state submission in addition to the following open source article: Keith Moor, 'Charity used as a front to finance Sri Lanka's Tamil Tigers' *Herald Sun* (online), 2010-04-01 www.heraldsun.com.au/news/charity-used-as-front-to-finance-sri-lankas-tamil-tigers/story-e6frf7jo-1225848229678 (Accessed 2014-04).

Case Study 45 - Affiliation with a Terrorist Entity

A public complaint made to the national NPO regulator alleged that multiple directing officials of a domestic NPO were working on behalf of, and had met with members of, an organisation listed both domestically and internationally as a supporter of terrorism.

An investigation by the regulator found that prior to the formation of the NPO, two of its directing

officials had travelled abroad to meet with the members of the listed organisation. One of the directing officials had played an active role in trying to encourage peace negotiations abroad and had been approached by a representative of the listed organisation asking him to continue in this role. The same directing official declined to speak at a demonstration because of the presence of flags of the listed organisation at the event.

The regulator's investigation found no evidence that the directing officials had made any public statements in support of the listed organisation. However, a review of the NPO's books and records identified some areas of potential weakness in the NPO's financial procedures and concluded that the NPO and its directing officials were unnecessarily exposed to undue risk through failing to follow its internal financial policies and procedures.

Case Study 46 - Affiliation with a Terrorist Entity

A proscribed terrorist organisation, based domestically, is known to have misused NPOs to support terrorism-related activities. The terrorist organisation controls a network of over 100 NPOs registered with the state as cultural associations. The NPOs are used to support its operations and otherwise advance its interests. Specifically, the NPOs provide the terrorist organisation with logistical and financial support, and spread messaging consistent with its espoused ideology.

The network of NPOs was observed carrying out business-related activities, including operating restaurants and bars, and providing business management and consulting services. The NPOs also collected voluntary donations and sold publications and merchandise in support of the terrorist organisation. Lastly, the network used their NPO status to earn public grants.

Currently, more than 25 individuals related to the network of NPOs are being tried criminally. Measures have also been taken to confiscate and freeze assets of over 100 NPOs and related individuals, and suspend and/or terminate NPO operational activities.

Case Study 47 - Affiliation with a Terrorist Entity

A well-known domestic NPO was operating as an online, third-party facilitator for individuals wishing to donate to other domestic NPOs via their payroll.

Under domestic terrorism legislation, the NPO submitted a series of STRs on individuals donating to organisations within the NPO sector that were suspected of being linked to terrorism as well as the organisations themselves. Reportedly, the organisations were large scale NPOs associated with one-another.

As part of its due diligence, the NPO that filed the STRs identified that one of the organisations was subject to sanctions for suspected links to terrorism.

Case Study 48 - Affiliation with a Terrorist Entity

A domestic NPO wishing to carry out orphan relief programmes applied for registration to the national NPO regulator. The application indicated that the NPO would send resources into a foreign area of conflict, and specifically into cities known to have active terrorist organisations.

Open-source research revealed that one of the NPO's directors had been implicated in a terrorism prosecution in a foreign jurisdiction. According to court documents, the NPO's director had been in communication with a known member of a foreign terrorist group. Also, open-source research

indicated that the NPO was carrying out foreign activities that were not in line with the programmes outlined in its application.

National security intelligence provided to the regulator indicated that the director did in fact have links to the foreign terrorist group, and was also a director for several other high-risk organisations believed to be linked to the same terrorist group. National security intelligence also indicated that the NPO had some operational links to other high-risk organisations believed to be sympathetic to the same terrorist group.

Based on these findings, the national regulator denied the NPO registration and shared relevant details with other national security authorities to further their respective mandates. The NPO appealed the regulator's decision, but was unsuccessful in its appeal.

Case Study 49 - Affiliation with a Terrorist Entity

An international NPO headquartered in an area of conflict sought to open an account at a domestic bank, in a country where a terrorist organisation operates. The bank's due diligence revealed that the NPO and one of its directing officials had been indicted in a case involving terrorist financing activities in two countries. The bank filed an STR with the national FIU, who conducted an investigation.

The investigation revealed that the NPO had been operating in the country for an extended period and had maintained multiple accounts at three different banks. The transactions on those accounts were inconsistent with the account profiles. There had been frequent cash deposits and withdrawals, including from domestic banking machines, by individuals with no apparent connection to the NPO and mostly in areas where terrorist organisations maintain substantial activities. Funds had also been transferred from the NPO's accounts to individuals with no apparent relationship with the organisation. Cash deposits were structured through multiple branches of the same bank, and funds were transferred from a foreign jurisdiction into the NPO's accounts by a national of a country known to be a state supporter of terrorism. In addition, a series of transfers were made into the NPO's accounts by its headquarters office in the area of conflict.

Further investigation established that the NPO was affiliated with an organisation known to have supported terrorist groups, and that its operations had supported two foreign terrorist movements. The NPO claimed to be paying the salaries of itinerant clerics in the country.

Case Study 50 - Affiliation with a Terrorist Entity (Reproduced in Chapter 3)

A boarding school, registered as a religious NPO, hired an individual on a terrorist watch-list. This individual was responsible for harbouring fugitives from a terrorist bombing.

Using fraudulent identification, the individual obtained residence and employment as an English language teacher at the boarding school. The director of the school was unaware of the individual's true identity or that he was on the terrorist watch-list.

The individual was subsequently charged and convicted of terrorism-related offences.

Case Study 51 - Affiliation with a Terrorist Entity

An NPO applied to the national NPO regulator for registration, indicating that its intent was to carry out religious and cultural activities. While reviewing the NPO's application and conducting open-

source research, the regulator noted that some of the NPO's activities appeared to extend beyond its stated purposes. Concurrently, the regulator became aware of national security intelligence reporting that indicated one of the NPO's directing officials was closely associated with a known state supporter of terrorism.

The regulator responded to the NPO's application by explaining its concerns and requesting further information on the NPO's activities and its relationships with other organisations. The NPO subsequently abandoned its application, and never obtained registration.

Case Study 52 - Affiliation with a Terrorist Entity

A foreign-based NPO, listed in multiple countries due to its suspected links to a listed terrorist organisation, transferred funds to several domestic NPOs. Information provided to the national FIU by law enforcement and national security authorities indicated that the domestic NPOs were suspected of providing ideological and financial support to extremist groups, including domestically listed terrorist organisations.

According to financial intelligence, the foreign-based NPO transferred over USD 100 000 to a domestic religious centre. A director of the religious centre was suspected of having used both his personal bank accounts and those of the religious centre to provide financial support to extremist groups, including domestically listed organisations. Information provided to the FIU indicated that this individual had previously spoken in favour of terrorist activity.

The FIU also found that an international NPO controlled by the foreign-based NPO transferred over USD 150 000 to a second domestic religious centre. This second centre was identified to the FIU as being linked to a domestic terrorism plot.

In addition, the foreign-based NPO and its affiliated organisations transferred approximately USD 120 000 to a third domestic NPO. The third NPO was already a subject of interest of the FIU as it had transferred funds to foreign NPOs known to be front organisations for terrorist groups. According to information provided to the FIU by a partner in the domestic security and intelligence community, a directing official of the third NPO used his position to promote a radical ideology. The third NPO was also the recipient of an EFT from a second international NPO for nearly USD 1 000 000. According to information provided to the FIU, the second international NPO was seeking to further its radicalisation agenda by providing financial assistance to domestic entities with links to extremism.

Case Study 53 - Affiliation with a Terrorist Entity

A domestic small business owner was also a directing official of a domestic NPO. According to law enforcement, the domestic NPO was a branch of an international NPO, suspected of financially supporting a terrorist organisation and potential suicide bombers.

FIU investigations found that substantial amounts of funds were regularly deposited into the small business' account. Some of deposited funds were subsequently transferred to individuals in an area of conflict abroad. The nature of the transactions did not correspond to the company's activities. One of the foreign beneficiaries of the small business' transfers was a directing official of the international, terrorism-linked NPO.

The domestic NPO had previously been a subject of interest of the FIU, relating to a terrorism financing investigation.

Case Study 54 - Affiliation with a Terrorist Entity

An NPO applied to the national NPO regulator for registration. The applicant NPO indicated that its principle activity was the running of a religious institution and associated educational and cultural programmes. On reviewing the applicant NPO's material, the regulator noted that the applicant NPO appeared to be very closely tied to another registered organisation. The applicant NPO shared an address, contact information, and directing officials with the registered organisation, and also had very similar financial statements. The registered organisation had already come to the regulator's attention because of concerns relating to terrorism, including receiving funding from foreign actors known to support terrorist activity. National security intelligence had also indicated that several directing officials shared by the applicant NPO and the registered organisation were believed to be linked to activities supporting terrorism.

The regulator replied to the applicant NPO requesting further clarification on its relationship with the registered organisation. The applicant NPO replied that it was a direct subsidiary of the registered organisation, essentially acting as its religious institution. The applicant NPO and the registered organisation were essentially different elements of the same overall organisation. The reply also indicated that the applicant NPO would be funding foreign actors, an activity not stated in its original application that raised new compliance concerns.

While these concerns were being assessed by the regulator, open source media reported on an independent audit of the registered organisation. The audit had been conducted by a chartered accountant at the request of the board of directors after indications of financial malpractice by some directing officials. The audit uncovered substantial compliance issues, including:

- Unreported bank accounts for foreign currency
- Incomplete accounting for funds transfers
- Incomplete accounting for claimed foreign travel
- Delayed depositing of donated funds
- Donated funds being deposited to different organisations' accounts

Based on the compliance problems identified by the independent audit and the existing concerns regarding links to terrorism, the national regulator initiated its own audit of the registered organisation and included its subsidiaries, including the applicant NPO. The applicant NPO subsequently withdrew its application for registration.

Case Study 55 - Affiliation with a Terrorist Entity

Tamils Rehabilitation Organisation (TRO) was designated pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations on November 15, 2007 for serving as a front to facilitate fundraising and procurement for the U.S. designated terrorist group Liberation Tigers of Tamil Eelam (LTTE). In the United States, TRO was a tax-exempt charitable non-profit organisation under section 501(c)(3) of the Internal Revenue Code, and had raised funds on behalf of the LTTE through a network of individual representatives. TRO had also facilitated LTTE procurement operations in the United States, including the purchase of munitions, equipment, communication devices, and other technology for the LTTE. TRO's efforts worldwide reportedly had allowed the LTTE to use

humanitarian aid, which TRO collected from the international community after the December 2004 tsunami, to launch new campaigns to strengthen LTTE's military capacity. Additional information indicated that the LTTE ordered international NGOs operating in its territory to provide all project funding through local NGOs, which are managed collectively by TRO. This arrangement allows TRO to withdraw money from the local NGO accounts and to provide a portion of the relief funds to the LTTE.

U.S.-based Tamil Foundation was designated pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations by the U.S. on February 11, 2009 for serving as a front to facilitate fundraising for LTTE. Over the course of many years, the Tamil Foundation, based in Cumberland, Maryland, and the TRO had comingled funds and carried out coordinated financial actions. The LTTE, like other terrorist groups, has relied on so-called charities to raise funds and advance its violent aims. The head of the Tamil Foundation was also president of the TRO in the United States. The TRO was named a Specially Designated Global Terrorist (SDGT) under Executive Order 13224 on November 15, 2007. Over the course of many years, the Tamil Foundation and the TRO have co-mingled funds and carried out coordinated financial actions. Additional information links the Tamil Foundation to the TRO through a matching gift program. The common leadership of the TRO and the Tamil Foundation has facilitated these activities.

A number of TRO affiliated criminal prosecutions also took place between 2006 and 2009. Indictment documents charged over 10 defendants with a range of legal violations including conspiracy to provide material support to a designated foreign terrorist organisation (LTTE), conspiracy to bribe a public official, attempt to obtain classified material, violation of IEEPA, conspiracy to export prohibited arms and munitions, attempt to export prohibited arms and munitions, international money laundering and possession of arms in the commission of a felony.

For example, on January 27, 2009, in the Eastern District of New York, Thiruthanikan Thanigasalam and Sahilal Sabaratnam pleaded guilty to conspiracy and attempt to provide material support to the Liberation Tigers of Tamil Eelam, also known as Tamil Tigers, a designated foreign terrorist organisation, and to conspiracy and attempt to purchase and export anti-aircraft missiles.

On January 26, 2009, defendant Sathajhan Sarachandran pleaded guilty to providing, conspiring to provide, and attempting to provide material support to the LTTE, and conspiring and attempting to acquire guided aircraft missiles, and defendant Nadarasa Yogarasa pleaded guilty to attempting to provide material support to the LTTE and conspiring to do so. Thanigasalam,Sabaratnam, and Sarachandran face statutory sentences of 25 years to life in prison and a sentencing guideline range of life. Yogarasa faces a statutory sentence and guideline range of up to 30 years in prison.

In another LTTE material support case, in the District of Maryland, Haniffa Bin Osman was sentenced on October 30, 2008, to 37 months in prison and three years of supervised release for conspiracy to provide material support to the LTTE and for money laundering. From April to September 29, 2006, Osman conspired with Haji Subandi, Erick Wotulo and Thirunavukarasu Varatharasa to provide state-of-the-art firearms, machine guns and ammunition, surface-to-air missiles, night vision goggles and other military weapons to the LTTE operating within Sri Lanka, to be used to fight against Sri Lankan government forces. The three other defendants pleaded guilty and all have been sentenced. On December 14, 2007, Subandi was sentenced to 37 months in prison and three years of supervised release. On January 3, 2008, Varatharasa was sentenced to 57 months in prison and on July 10, 2008, Wotulo was sentenced to 30 months in prison.

Case Study 56 - Affiliation with a Terrorist Entity

In October 2012, the U.S. Department of the Treasury designated two Lebanon-based charities, pursuant to Executive Order (E.O.) 13224, for being controlled by, acting on behalf of, and providing financial support to a U.S. designated terrorist organisation, Hamas. The Beirut-based Al-Waqfiya and Al-Quds exist to support the families of Hamas fighters and prisoners and to raise money for programs and projects in the Palestinian territories intended to spread the influence and control of the terrorist organisation Hamas.

Al-Waqfiya was a central component of the Union of Good, which was designated by the U.S. in November 2008 pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to Hamas, a U.S. designated terrorist organisation. Al-Waqfiya was established by Hamas in 2000 to financially support the families of Hamas terrorists. The organisation has been run by senior Hamas leadership for years, and several senior Hamas leaders play a dominant role within the organisation. Al-Waqfiya has facilitated the collection of money on Hamas's behalf, and has used its ties with money remitters and merchants in the Middle East to transfer funds to Hamas in Gaza. When delivering funds to Gaza, Al-Waqfiya obscures the sources of the money so that donations appear as innocuous charitable contributions. Portions of funds sent by Al-Waqfiya to Hamas were used by Hamas military operatives, and have financed the Hamas infrastructure and operations in the Palestinian territories.

Al-Quds was established in 2001 in Beirut by members of Hamas in order to raise funds for Hamas projects in Jerusalem through the cover of charity. Hamas's leadership runs all of the foundation's affairs through Hamas members who serve on the Board of Trustees, the Board of Directors, and other administrative committees. All documents, plans, budgets, and projects of Al-Quds are drafted by Hamas officials. Several senior Hamas officials, including U.S. designated terrorists Musa Abu-Marzuq and Usama Hamdan, served on Al-Quds' Board of Trustees. Representatives at an Al-Quds conference were told to consider themselves unofficial ambassadors for Hamas in their respective countries.

Case Study 57 - Affiliation with a Terrorist Entity

A domestic NPO carrying out cultural and religious activities, including running a religious institution, applied for registration to the national NPO regulator. While reviewing the NPO's application, the regulator became concerned because the NPO's stated activities and purposes were vaguely explained and appeared to include political activity. Additionally, one of the individuals listed as a directing official was known to be engaged in activities supporting terrorism.

National security intelligence provided to the regulator indicated that this directing official had travelled abroad on several occasions in order to maintain connections with foreign organisations known to be fronts for listed terrorist entities. The directing official was also tied to several other domestic organisations that were believed to support terrorist activity. The NPO itself received support in the form of funding and materiel from foreign donors who were known to sympathise with listed terrorist entities and provide educational and promotional material in line with this sympathy.

The regulator replied to the NPO's application indicating concerns about the nature of the activities being carried out by the NPO, as well as its independence from foreign donors. The NPO was given the opportunity to further explain its position regarding these concerns, but no reply was forthcoming. The NPO's application for registration was subsequently denied.

Case Study 58 - Affiliation with a Terrorist Entity

A long-registered NPO carrying out cultural and humanitarian activities domestically and abroad lost registration due to its failure to submit mandatory reporting to the national NPO regulator. The NPO subsequently re-applied for registration.

The NPO's re-application instigated an audit of the NPO's activities by the national regulator. On examining the NPO's re-application and audit material the regulator became concerned that its activities were vaguely explained and indicated a political, rather than humanitarian, intent. Open source research combined with material from the regulator's audit showed that the NPO acted as the domestic branch office of a larger foreign organisation (the parent organisation) that was suspected of being a front for several foreign terrorist groups. Nearly all of the NPO's funding came from the parent organisation, staff salaries were underwritten by the parent organisation, and many guest speakers were provided by the parent organisation.

National security intelligence accessed by the regulator indicated that the NPO was part of a network of branch offices that linked back to the international parent organisation. The parent organisation was known to be actively engaged in activities beneficial to terrorist organisations' recruitment efforts. Also, programmatic direction and materiel for the branch offices was known to come from the parent organisation. Open source research and national security intelligence also indicated that several of the NPO's directors had been actively involved with other foreign organisations that were believed to support listed terrorist entities. One of these foreign organisations had itself been listed as a supporter of terrorism.

The national regulator replied to the NPO's re-application explaining its concerns that the NPO was essentially controlled by the foreign parent organisation, engaged in programmes that appeared political in nature, and that there was insufficient information provided on its activities. The NPO was given the opportunity to address these concerns, but no reply was forthcoming. The NPO was subsequently denied registration.

Case Study 59 - Affiliation with a Terrorist Entity

An NPO applied to the national NPO regulator for registration, citing cultural and religious activities as their principal purposes. The national regulator became suspicious because one of the NPO's directing officials was concurrently a directing official for another organisation that was believed to support terrorist activities. Additionally, the NPO regulator received a lead from a member of the public that outlined several suspicious accountability practices within the NPO. These included maintaining two sets of governing documents (one shown to the regulator, and one shown to the public), disallowing all but a small group of individuals from becoming board members, and not maintaining any minutes of meetings.

The national regulator outlined their concerns to the NPO, indicated that the concerns would need to be addressed prior to registration, and gave the NPO the opportunity of addressing the concerns. The NPO did not respond, effectively abandoning its application for registration.

Case Study 60 - Affiliation with a Terrorist Entity (Reproduced in Chapter 4)

A domestic NPO received a large sum of funds, from a foreign NPO operating in an area of conflict. A directing official of the domestic NPO tried to withdraw most of the funds in cash. After the bank

advised against this, a portion of the funds was withdrawn through banking machine withdrawals. In addition, another individual, unassociated with the NPO, made large cash withdrawals.

The domestic NPO's bank filed an STR with the national FIU. An investigation by the national FIU revealed that the foreign NPO was linked to a listed terrorist entity. It was also determined that a leading member of the domestic NPO was also a prominent figure in a foreign militant organisation with links to a foreign terrorist group.

Case Study 61 - Affiliation with a Terrorist Entity

An NPO applied for registration to the national NPO regulator, stating that the NPO's intent was to provide humanitarian relief to victims of a foreign conflict, and to help integrate refugees of the conflict into the domestic environment. Upon reviewing the NPO's application, the regulator was concerned that some of the NPO's activities and objectives were too vague or did not fulfil charitable purposes. The NPO indicated that its activities and objectives were identical to a sister organisation that had previously been registered. The NPO proceeded to amend its purposes and objectives and was registered, however the regulator continued to monitor the organisation.

In response to a general concern about terrorist activity emanating from the aforementioned foreign conflict, the regulator later began examining the activities of several high-risk organisations that were carrying out activities in the area of conflict. Analysis of the NPO's obligatory reporting revealed that it was in fact co-located with its sister organisation and shared at least two directing officials. National security intelligence reporting stated that the sister organisation was believed to be a front organisation for a foreign terrorist group operating out of the area of conflict. Additionally, national security intelligence revealed that one of the shared directing officials was believed to be the domestic leader of the foreign terrorist group.

The regulator proceeded to audit the NPO and discovered several areas of non-compliance. The NPO had transferred USD 20 000 to foreign organisations or individuals in the area of conflict that were not legally prescribed beneficiaries. Additionally, the NPO did not have proper accounting for USD 10 000 it had disbursed, leaving questions as to the final beneficiaries for the funds. The NPO had also failed to keep adequate records of meetings of the board of directors, raising questions about the transparency of decision-making in the NPO.

Because the NPO had already begun to reform several administrative practices and had changed several directing officials, the NPO avoided deregistration but entered into a compliance agreement with the regulator that would enforce strict due diligence and accountability standards.

Case Study 62 - Affiliation with a Terrorist Entity (Reproduced in Chapter 4)

An NPO carrying out international humanitarian work in a foreign area of conflict applied to the national NPO regulator for registration. On reviewing the NPO's application, the regulator became concerned that some of the NPO's purposes and activities were considered to be outside of those legally prescribed. Also, the foreign organisations that the NPO was partnering with in the foreign area of conflict were not legal beneficiaries.

While reviewing the NPO's application, the regulator accessed national security intelligence indicating that the NPO was believed to act as a domestic front organisation for a listed terrorist group operating in the foreign area of conflict. It was identified that the NPO would transfer resources, through legitimate means, to several organisations operating in the area of conflict. Some

of these foreign organisations were themselves identified as being part of the infrastructure of the same listed terrorist group.

Two foreign partners also provided information that the national regulator was able to draw on during its review of the application. One foreign partner indicated that the NPO had been the subject of investigation in its jurisdiction in relation to terrorist activities.

The regulator informed the NPO of its concerns. The NPO attempted to address some aspects of the regulator's concerns, including opening up a branch office within the foreign area of conflict in an attempt to demonstrate better control of resources and oversight of programs. However, further investigation by the regulator indicated that the core risks were not being addressed and notified the NPO of this.

As a result of the NPO regulator's investigative efforts and administrative actions, the NPO abandoned its application for registration. Information regarding the regulator's review was passed on to national security partners to facilitate their own investigations.

Case Study 63 - Affiliation with a Terrorist Entity

An NPO applied to the national NPO regulator for registration, indicating that its purpose was to provide humanitarian services to domestic and foreign communities. The NPO's name was identical to a much larger organisation operating in a foreign area of conflict with several active terrorist groups. The NPO had entered into an operating agreement with this foreign organisation to fund activities overseas in this area of conflict. The NPO received registration and operated for several years. However, the NPO was audited and subsequently deregistered for administrative reasons; specifically, it failed to file mandatory reporting with the national NPO regulator.

The NPO reapplied for registration and the application was screened for further analysis by the NPO regulator because of the NPO's prior deregistration. The regulator was concerned that the NPO's application was vague in regard to its activities, particularly those carried out in conjunction with its larger foreign partner, and that the NPO was not retaining adequate control of the funds that it sent overseas. The regulator requested and was provided with further information from the NPO on both these points.

In the meantime, the regulator received a disclosure from the national FIU regarding the same NPO's financial activities, and those of its three principal directing officials. The financial intelligence revealed some links to domestic organisations that were suspected of supporting foreign terrorist organisations. However, the NPO regulator's principal concern continued to be that the NPO was unable to adequately indicate control of the funds once sent overseas. Because of this, the NPO was denied registration.

Case Study 64 - Affiliation with a Terrorist Entity

Law enforcement information indicated that individuals related to a domestic NPO conspired to commit an act of terror on home soil. Reportedly, one of the conspirators' close relatives was the founder of the NPO and there was suspicion that they had used the NPO for illegal purposes.

The national NPO regulator exercised legal powers to freeze the NPO domestic bank accounts. The regulator also requested that the NPOs directing officials provide information relating to the NPO's assets held abroad.

Although national security intelligence suggested that it was possible that NPO funds were being transferred abroad to be used for unlawful purposes, the regulator found no direct evidence that the NPO's directing officials had diverted NPO funds for illegal or non-charitable purposes. However, the regulator did conclude that the NPO's directing officials were unable to show that they maintained a sufficient level of direction and control over funds sent to two foreign countries. In general, very little monitoring was being conducted by the NPO. The directing officials were often largely dependent on feedback from the third parties in the foreign countries, including from individuals who were receiving the funds.

Ultimately, the NPO's directing officials were unable to satisfactorily verify that funds sent to the foreign countries had been used legitimately and in accordance with furthering the NPO's objectives, as required by law.

Case Study 65 - Affiliation with a Terrorist Entity

In August 2013 the U.S. Department of the Treasury designated the Jamia Taleem-Ul-Quran-Wal-Hadith Madrassa, also known as the Ganj Madrassa, pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to al-Qa'ida and other designated terrorist organisations. The Ganj Madrassa is a school in Peshawar, Pakistan that was found to be serving as a training centre for, and facilitating funding for UN and U.S.-designated terrorist organisations including al-Qa'ida, Lashkar-e Tayyiba and the Taliban. The activities of the Ganj Madrassa exemplify how terrorist groups, such as al-Qa'ida, Lashkar-e Tayyiba and the Taliban, subvert seemingly legitimate institutions, such as religious schools, to raise and divert charitable donations meant for education to support terrorist training and violent acts. The action did not target all madrassas, which often play an essential role in improving literacy and providing humanitarian and developmental aid in many areas of the world; it only identified this specific madrassa as supporting terrorism and terrorist financing.

The Ganj Madrassa is controlled by UN-designated al-Qa'ida facilitator Fazeel-A-Tul Shaykh Abu Mohammed Ameen Al-Peshawari, also known as Shaykh Aminullah. Shaykh Aminullah was designated by both the United States pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations and the United Nations (UN) in 2009 for providing material support to al-Qa'ida and the Taliban.

The Ganj Madrassa serves as a terrorist training centre where students, under the guise of religious studies, have been trained to conduct terrorist and insurgent activities. In some cases, students were trained to become bomb manufacturers and suicide bombers. Shaykh Aminullah has directed donations provided for the school to terrorist groups such as the Taliban, which use the money to fund the ongoing violence in Afghanistan.

Case Study 66 - Affiliation with a Terrorist Entity

Large cash deposits and wire transfers from a foreign-based international NPO were regularly made to the account of a domestic NPO. The funds were immediately transferred to the accounts of other foreign-based NPOs.

Information provided by foreign authorities to the national FIU revealed that both the domestic and international NPOs, as well as a founding official common to both organisations, were linked to a law enforcement investigation in the foreign jurisdiction relating to terrorism. In addition, the

accounts of the international NPO had been frozen.

The FIU's analysis indicated that the international NPO was operating locally through the domestic NPO. The FIU referred the case to prosecutors. As a result of the investigation, both NPOs were listed as supporters of terrorism.

Case Study 67 - Affiliation with a Terrorist Entity

An international NPO, headquartered domestically, used its cover as a social services provider to raise funds and procure material resources for a terrorist organisation. While the NPO did conduct limited social services, the majority of its efforts were focused on carrying out activities in support of terrorism.

The funds raised in support of terrorism were distributed to members of the terrorist organisation to support operational needs as well as to pay salaries and loans. Material resources procured in support of terrorism included military equipment and communication such as surface to air missiles; assault rifles; unmanned aerial vehicles; submarine and warship design software; GPS, radio and satellite equipment; and night vision glasses.

Domestic and international fundraising efforts involved soliciting voluntary and involuntary donations, hosting fundraising events and selling goods such as mobile phone cards. Only a small percentage of money received through fundraising efforts was spent on social services. The balance was diverted to finance terrorism.

An investigation, which included the analysis of financial intelligence, uncovered that the NPO and its international branches used a web of personal and business bank accounts, as well as cash, cheques and informal money services businesses to transmit funds for the purpose of supporting terrorism. The investigation resulted in NPO bank accounts being frozen and the NPO being deregistered domestically.

Case Study 68 - Affiliation with a Terrorist Entity (Reproduced in Chapter 6)

In June 2005, the ISNA Development Foundation (IDF) was registered as a charitable organisation by the Canada Revenue Agency (CRA), which is the government agency responsible for the regulation of charities. IDF was registered with the primary purposes of advancing religion through the establishment and operation of religious facilities in Canada and the relief of poverty through the provision of financial assistance to needy persons in Canada.

In January 2011, IDF's parent organisation, the Islamic Society of North America (ISNA), was the subject of media reporting that detailed the findings of an independent, internal audit. The audit identified serious concerns regarding ISNA's alleged misuse of resources, particularly pertaining to the transfer of funds to improper beneficiaries, improper receipting, and the allocation of a large percentage of resources to activities not permitted under the regulations governing registered charities in Canada. In addition, substantial resources were being transferred to another Canadian NPO, the Kashmir Relief Fund of Canada (KRFC), presumably in order to undertake activities in Kashmir.

The CRA conducted an audit of IDF's operations in December 2011. The audit revealed that IDF had entered into a funding arrangement with KRFC and its sister organisation, the Kashmiri Canadian Council (KCC), with the ultimate goal of sending the raised funds to a Pakistan-based NPO named the Relief Organisation for Kashmiri Muslims (ROKM). Under the arrangement, KCC/KRFC raised funds

for "relief work" in Kashmir; the IDF supplied official donation receipts to the donors and disbursed over USD 250 000 to ROKM, either directly, or via KCC/KRFC. During the audit of IDF, the directing officials of IDF stated that they knew nothing about ROKM or the specific nature of the activities towards which the funds were to be directed. The above-noted receipting arrangements are not allowed under Canadian regulations. In addition, IDF failed to maintain direction or control of the funds transmitted and was unable to substantiate the nature of the programs towards which its resources were directed.

A review of IDF's electronic documentation allowed CRA to determine that documentation professing to indicate IDF's control over the Kashmiri projects had been fabricated. As an example, forensic analysis by the Government of Canada of photographs provided to the CRA to demonstrate IDF's direction and control over the activities being undertaken in Kashmir, had been digitally altered through the addition of a banner bearing the name IDF.

The CRA's research indicated that ROKM is a charitable arm of Jamaat-e-Islami, a political organisation that actively contests the legitimacy of India's governance over the state of Jammu and Kashmir, including reportedly through the activities of its armed wing Hizbul Mujahideen. Hizbul Mujahideen is listed as a terrorist entity by the Council of the European Union and is declared a banned terrorist organisation by the Government of India, Ministry of Home Affairs, under the *Unlawful Activities (Prevention) Act of 1967*.

Given the commonalities in directorship between ROKM and Jamaat-e-Islami, the apparent participation of these same individuals in the establishment and high-level control of Hizbul Mujahideen, and the numerous public declarations of support provided by many of them for the armed militant movement in Kashmir, it was the CRA's expressed concern that the IDF's resources may have been used to support the political efforts of Jamaat-e-Islami and/or its armed wing, Hizbul Mujahideen.

Based on the findings of the audit, IDF's charitable status was revoked in September 2013. The revocation was the subject of multiple media reports in Canada, the United States, and India. Subsequently, ROKM's website was taken down.

Note:

This case study was developed entirely from the open source documents cited and was not developed from any state's response to the request for case studies. See CRA's administrative fairness letter to IDF dated 2013-05-28, and available at www.thestar.com/news/canada/2013/07/25/star_investigation_federal_audit_raises_concern_that_canadian_charity_funded_terror.html.

Case Study 69 - Affiliation with a Terrorist Entity

A number of foreign individuals opened bank accounts on behalf of two regional private companies and one domestic NPO. The companies and the NPO were related to film production and the telecommunications sector. The individuals were listed as managers or staff members in all three organisations.

The two companies and the domestic NPO received large deposits from foreign nationals amounting to several million US dollars. Some of this money was forwarded on by international transfer to other organisations working in film production.

Information provided by law enforcement authorities indicated that some of the individuals were

known to be linked to an organisation involved in terrorist activity. It was determined through the investigation that funds used to finance the NPO and private companies likely originated with organisations involved in terrorist activity.

The case was forwarded to judicial authorities for further investigation.

Case Study 70 - Affiliation with a Terrorist Entity

The national NPO regulator opened an investigation following media allegations that a domestic NPO had links to a terrorist organisation. Allegedly, the domestic NPO had diverted funds to foreign NPOs operating in an area where a terrorist organisation was known to operate. These foreign NPOs were an integral part of a terrorist organisation and its political arm, and they supported terrorism-related activities including the indoctrination of children and the promotion of violent extremism. It was also alleged that the foreign NPOs were distributing resources to families of suicide bombers as opposed to distributing resources on the basis of charitable need.

Another key allegation was that one of the directing officials of the domestic NPO had attended meetings hosted by the aforementioned terrorist organisation's political arm and had made public statements in support of violent extremist activity. Also, the domestic NPO was linked to a second domestic NPO, the president of which had purportedly voiced support for suicide bombings.

The domestic NPO had been the subject of a previous investigation conducted by the national regulator. This earlier investigation was based on allegations that the NPO had funded a terrorist organisation and had connections to a number of former militants linked to a political party considered to be the political arm of a terrorist organisation. This investigation did not, however, uncover evidence of NPO donations being used to support terrorism or political activities.

Similarly, the more recent NPO regulator investigation was unable to uncover sufficient evidence to support the media allegations linking the domestic NPO to terrorism. However, the investigation did find that the domestic NPO's directing officials had not adequately fulfilled their duties and responsibilities in respect of their due diligence and monitoring procedures for their foreign partners.

To address the regulator's findings, the domestic NPO was instructed to formulate guidelines setting out the criteria upon which charitable beneficiaries should be selected, and to take steps to ensure that their foreign NPO partners strictly apply this criterion. Lastly, the domestic NPO was required to disassociate itself from the second domestic NPO based on established links between the second domestic NPO and a listed entity.

Case Study 71 - Affiliation with a Terrorist Entity

An NPO applied for registration with the national NPO regulator, citing its activities as helping refugee populations from an area of conflict. During the course of reviewing the NPO's application, the national regulator accessed national security intelligence that indicated that several of the NPO's directing officials were connected to a listed foreign terrorist organisation. The intelligence also revealed that the NPO shared premises and directors with another supposedly-defunct organisation that was known to have provided resources to the same listed terrorist organisation.

The national regulator's review of the NPO's application identified several other problems, including very vague programs and activities and contradictory or inaccurate statements about the NPO's relationships with other organisations. Based on its review of the NPO's application and the resulting concerns, the national regulator did not approve the NPO's registration.

Case Study 72 - Affiliation with a Terrorist Entity

An NPO applied to the national NPO regulator for registration, indicating that its purposes were to support refugees of a foreign civil war both domestically and within the area of conflict.

The regulator became concerned when a review of the application found that the NPO had no set activities, particularly for its operations abroad. The regulator requested further information several times from the NPO regarding its purposes and activities; however the NPO provided very little information about its activities and changed its purposes several times. Although the NPO continually revised its purposes, the purpose of conducting operations in the area of conflict remained constant, leading the regulator to believe that the principal goal of the organisation was to conduct activities in the area of conflict. The regulator's investigation confirmed that the NPO was being used as a funding conduit when an audit of a related organisation uncovered receipts indicating transfers from the NPO to a branch office of a foreign terrorist organisation operating in the area of conflict.

A parallel national security investigation indicated that the NPO was a front for a foreign terrorist organisation operating in the area of conflict, and that the NPO's directing official was the domestic representative for the same terrorist organisation. Additionally, national security intelligence indicated that the NPO was a point of contact for two other terrorist entities operating abroad. This national security information was passed to the regulator. However, the regulator had already determined that the NPO would not qualify for registration.

Based on its investigation, the regulator informed the NPO that it was unlikely to receive registration unless the purposes of the organisation changed substantially, and further information as provided regarding its activities. The NPO subsequently abandoned its application.

Case Study 73 - Affiliation with a Terrorist Entity

The founder of a domestic NPO was also the owner of a small business. The individual had control over a business and a personal account at Bank A. The balance of the business account was transferred to the personal account or withdrawn in cash. This led Bank A to send STRs to the national FIU.

A foreign individual residing domestically was an associate of the small business and held a personal account at Bank B. This individual deposited cash into the Bank B account, and then ordered wire transfers to another entity in a foreign area of conflict. The vague justification for the transfer led Bank B to send suspicious transaction reports to the national FIU.

The FIU's investigation of the small business' account showed that several transfers had been made to the foreign individual's personal account and subsequently withdrawn in cash. The FIU's analysis found that withdrawals from the small business' account corresponded with deposits on the foreign individual's account.

Law enforcement information indicated that the NPO founder and small business owner was an active member of a terrorist organisation. Law enforcement also confirmed that the small business

was known through an investigation into counterfeiting. It was determined that the funds moved from the small business account, through the foreign individual's accounts, to the area of conflict, may have originated from illicit activities and ultimately been used to finance foreign terrorist activities.

Case Study 74 - Affiliation with a Terrorist Entity

An NPO applied for registration to the national NPO regulator, ostensibly to carry out domestic humanitarian work. On reviewing the NPO's application, the regulator noted that the NPO's purposes and activities were very vague, leaving open the possibility of non-charitable activities being carried out. Also, it was noted that the NPO was meant to exclusively target a diaspora from a foreign area of conflict. Open source information also indicated that there were links between the NPO and individuals who supported a terrorist organisation.

The regulator received national security intelligence indicating that at least two directing officials of the NPO were known supporters of a listed terrorist organisation operating in the same foreign area of conflict. One directing official was identified as a relative of a high-ranking member of the political wing of the terrorist organisation. The same directing official also had known connections to individuals engaged in terrorism financing. Another of the directing officials was known to be involved in several other organisations that were believed to support the same listed terrorist organisation.

The regulator replied to the NPO's application, outlining its concerns regarding vague or broad goals and possible political activities. The NPO was given the opportunity to provide further clarification, but no reply was forthcoming. The NPO did not receive registration.

ABUSE OF PROGRAMMING

Case Study 75 - Abuse of Programming (Reproduced in Chapter 3)

A domestic NPO was the subject of negative open source information suggesting it was condoning suicide bombers on its website.

A review of the NPO's website by the national NPO regulator found that the NPO had published a list of 'martyrs' online, including a number of suicide bombers. Engagement by the NPO regulator resulted in the removal the inappropriate content from the website.

The investigation by the NPO regulator concluded that the NPO had inadequate governance procedures and an ineffective risk management system in place. The NPO was directed to review its governance structure to effectively manage the risks to the NPO.

Case Study 76 - Abuse of Programming

A domestic NPO was formed with the stated purpose of carrying out educational, religious and cultural programs. However, while reviewing the NPO's application for registration, the national regulator became concerned that the NPO had unstated purposes that supported a foreign terrorist movement. The NPO was registered but monitored.

A subsequent audit identified that the NPO was unable to account for the origin or final use of its resources on multiple occasions. Open source research raised further suspicion that the NPO was

engaged in political activities in support of a foreign terrorist group. Research also uncovered a parallel set of records that had not been provided to the national regulator. Law enforcement information revealed that the NPO had engaged in activities supporting a terrorist movement and national security intelligence revealed that several directors were associated with foreign terrorist groups.

Based on these findings, the NPO was deregistered and the national regulator shared the case information with law enforcement and national security partners to further their own investigations.

Case Study 77 - Abuse of Programming

The national NPO regulatory body opened an investigation following media allegations that a domestic NPO, established to advance education, was being run by senior members and activists of a group that promoted violent extremism. Reportedly, these individuals were using the NPO's schools to teach and promote extremism that was known to result in violence.

The regulator accessed and considered multiple sources of information including information provided by the media outlet in support of its allegations, information provided by the NPO itself and material provided by the board of education.

The regulator's investigation uncovered that one of the NPO's directing officials was formerly a member of an organisation that was engaged in radicalisation towards violence. However, the directing official's membership had ceased several years earlier and they no longer agreed with some of the radical organisation's political views.

The regulator also uncovered that one of the NPO's directing officials was married to an individual who acted as the media representative for the radical organisation. However, that relationship had also ended since the media report was published.

Case Study 78 - Abuse of Programming (Reproduced in Chapter 3)

An NPO was carrying out religious and educational activities domestically, with no foreign activities. Information provided by the national FIU indicated that the NPO had received over USD 13 000 from a foreign organisation known to provide support to a foreign terrorist group.

Subsequent open source research indicated that the NPO's education programs espoused an ideology that was shared by several foreign terrorist groups. Concerns arose that this shared ideology was being exploited for recruitment purposes for a terrorist organisation. It was subsequently revealed that a former student of the NPO's school had been charged in another country with terrorism offences. The student had also met with several other individuals who were later convicted of terrorism offences.

The NPO was audited by the national regulator, and the audit found that the NPO could not account for the origin of much of its income and expenditures. Based on this, the NPO was deregistered.

Case Study 79 - Abuse of Programming

Law enforcement information provided to the national NPO regulator indicated that a domestic NPO's website contained radical content that could promote violence.

While law enforcement was unable to engage directly with the NPO, the NPO regulator's dealings

with the organisation established that the NPO did not have sufficiently effective governance related to managing its website content. Following instruction from the regulator, the NPO removed the questionable content from its website.

SUPPORT FOR RECRUITMENT

Case Study 80 - Support for Recruitment (Reproduced in Chapter 3)

On November 4, 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including al Qaida and affiliated organisations.

Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for a UN designated terrorist organisation, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UN 1267-designatated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas. As of early 2009, Al Rehmat Trust had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, al Rehmat Trust was raising funds on behalf of Khudam-ul Islam, an alias for JEM.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including financial support to wounded Taliban fighters from Afghanistan.

Case Study 81 - Support for Recruitment

A domestic NPO was found to have arranged and hosted events and retreats attended by speakers known to promote violent extremism. Audiences for the events numbered in the hundreds and the events were the subject of media reporting.

Following a deconfliction process involving multiple domestic government agencies, a national NPO regulator investigation was launched. The investigation concluded that the NPO had inadequate processes to assess the suitability of speakers or run events. Following regulator engagement with the NPO, the NPO ceased its activities while the directing officials undertook a complete review of its governance arrangements.

The NPO's activities remain suspended and the NPO is being monitored by the regulator.

Case Study 82 - Support for Recruitment

An NPO engaged in cultural, religious, and educational activities came to the attention of the national NPO regulator when it submitted revised purposes for review, as required by the regulator. The regulator noted that the NPO's new purposes were very vaguely stated.

Additionally, open-source research revealed that one of the principal directors of the NPO had made statements and speeches supporting violent action, promoting recruitment to violence, and dehumanizing other ethnic and religious groups. Also, the NPO had hosted a speaker that had been

banned from other speaking venues because of similar speeches and statements. When confronted with these concerns, the NPO provided redrafted purposes and indicated that the director and speaker were no longer associated with the NPO.

In response, the regulator audited the NPO and entered into a compliance agreement ensuring strict operational accountability and reporting.

Case Study 83 - Support for Recruitment

An NPO carrying out domestic and international humanitarian and cultural activities applied for registration to the national NPO regulator. On reviewing the NPO's application, the regulator noted that the NPO's activities and purposes were vaguely explained, leaving room for non-compliant activities. When the NPO was unable to address these concerns, the application was denied.

Subsequently, national security intelligence indicated that the NPO's facilities were used as a meeting place for supporters of a listed terrorist organisation. One of the NPO's former board members, who also acted as a guest speaker for the NPO, was known for engaging in activities promoting recruitment to violence.

Sometime later, the regulator received an application from an NPO bearing a similar name to the first organisation. The new NPO wanted to conduct similar activities that were, again, vaguely defined. Research conducted by the regulator showed that the new NPO applicant was in fact the same as the original applicant. The two applicants shared an address, phone number, and bank account, and documentation regarding the NPO's activities used both the original and new name interchangeably.

The regulator notified the NPO of its concerns and gave it the opportunity to address them. When the NPO failed to address the concerns, it was denied registration.

Case Study 84 - Support for Recruitment

A foreign national ordered a wire transfer from his personal account at a foreign bank, to the account of a domestic NPO. When justifying the request, the foreign national made reference to sponsoring an individual. Specifically, funds were meant to provide for the individual's living expenses.

An investigation by the national FIU found that the individual to be sponsored was on a terrorism watch-list. The investigation also revealed that the NPO was closely linked to a network of groups that financed terrorist activity.

Case Study 85 - Support for Recruitment

A newly established domestic NPO appeared to be organising and/or hosting lectures that were led or attended by speakers known to promote violent extremism.

Following a deconfliction process involving multiple domestic government agencies, a national NPO regulator investigation was launched. The investigation concluded that the NPO had not, in fact, hosted the events itself, but was closely associated with a non-charitable educational institute which had hosted the events.

The regulator established that the directing officials of the NPO were also directors of the non-charitable educational institute. To the regulatory body, this was an unresolvable conflict of interest.

Case Study 86 - Support for Recruitment

National media publicly linked a domestic NPO to the perpetrators of terrorist attacks. Reportedly, two suicide bombers were directing officials of a domestic NPO at the time of the attacks. Also, extremist material was found on the NPO's premises.

Separately, two other former directing officials of the domestic NPO were previously convicted of terrorism-related offences. One was convicted based on possession of a document containing information likely to be useful to a person committing or preparing an act of terrorism, and the other on conspiracy to attend a place used for terrorist training.

An investigation conducted by the national NPO regulator considered whether the NPO may have been used to facilitate terrorist, violent extremist or other inappropriate activities. The investigation considered whether there was evidence that the NPO's funds were used to facilitate the attacks, whether inappropriate or violent extremist material was at the NPO's premises, and/or whether the NPO's premises were used as a meeting place to plan the attacks. The regulator exercised its legal powers and froze the NPO's bank account pending the findings of the investigation.

The regulator's investigation included the examination of material removed from the NPO's premises by police during a concurrent investigation. While the majority of the material was deemed appropriate, approximately one fifth of the material was considered to be political, biased, propagandist or otherwise inappropriate for an NPO of such nature to hold. No criminal charges were brought in respect of the material removed from the NPO's office.

Overall, the investigation was unable to determine what role, if any, the NPO and its offices had played in financing or facilitating terrorist, extremist, or otherwise inappropriate activities. However, after the attacks, the NPO was abandoned.

Case Study 87 - Support for Recruitment

An NPO purchased property paying 80% of the selling price prior to the execution of the deed. The remaining amount was paid with a domestic bank transfer. The suspicious financial activity related to the property purchase was reported to the national FIU by the bank in the form of an STR.

The FIU's investigation revealed that the transfer for the remainder of the selling price originated from the personal account of one of the NPO's directing officials. Prior to the transfer, a substantial cash deposit had been made to the directing official's account, making the origin of the funds difficult to determine.

The directing official held the same position at a second NPO, which law enforcement information indicated was suspected of supporting a terrorist organisation. The directing official was believed to be involved in the recruitment of combatants for the terrorist organisation and was closely associated with another individual who was an active member of the same terrorist organisation.

It was also determined that a second directing official was similarly involved in the organisation supporting terrorist activity.

Case Study 88 - Support for Recruitment

A domestic NPO applied for registration to the national NPO regulator, indicating that its intention was to run a religious and cultural centre for the benefit of a specific diaspora community. A short time before the NPO's application, the regulator had received a disclosure from national security

intelligence authorities indicating that the NPO was believed to be overseen by an individual known to be associated with a listed terrorist group.

The regulator noted that the NPO's stated purposes and activities were vague and requested further information regarding the NPO's management and activities. Open-source research conducted by the regulator revealed that the NPO was promoting a political cause consistent with the views of several known terrorist organisations. The NPO was using rhetoric and imagery that mirrored material used by the same terrorist organisations to promote their cause within the diaspora community, including images of deceased terrorists. Also, it was revealed that the NPO had hosted events organised and sponsored by a foreign organisation that was known to promote the same political cause as these terrorist organisations.

The regulator determined that there was an unacceptable risk that the NPO was being used to support recruitment to violence and therefore denied the NPO registered status.

Case Study 89 - Support for Recruitment

A partner agency referral to the national NPO regulator alleged that a domestic NPO appeared to support a listed terrorist organisation. Open source information supported the allegations.

By engaging with the NPO itself, the regulator identified that the NPO's location was linked to various marches that involved supporters of the listed organisation. An inspection of the NPO's premises identified that there were numerous pictures of, and political paraphernalia relating to, members of the listed organisation displayed on the premises.

The NPO's directing officials were instructed to remove all such pictures and paraphernalia, to sever all links with the listed organisation and to actively manage the NPO's premises and activities.

Case Study 90 - Support for Recruitment

An NPO carrying out cultural and religious activities applied for registration to the national NPO regulator. As part of its activities, the NPO ran a religious institution and organised guest lectures by numerous speakers.

While conducting open-source research in the process of reviewing the NPO's application, the regulator became concerned that some of the speakers that had been hosted by the NPO were engaging in activities that could be beneficial to recruitment by terrorist organisations. Additional open source material indicated that an individual with significant influence over the NPO (but who was not listed as a directing official in the NPO's application for registration) was believed to be connected to a listed terrorist organisation.

According to national security intelligence provided by partner organisations, the diaspora community that the NPO primarily targeted with its activities was particularly vulnerable at that time to recruitment activities by the same listed terrorist organisation.

Based on these factors, the regulator denied the NPO registration.

Case Study 91 - Support for Recruitment

A directing official of a domestic NPO was arrested and subsequently charged following a fire bomb attack on the home of the owner of a publishing company. The company was due to publish a book,

considered by some to be offensive to a particular religion.

Following the publication of media reports relating to the fire bomb attack, the national NPO regulator identified the attacker as being a directing official of a domestic NPO. The regulator engaged with the other directing officials of the NPO and was informed of the decision by its Board of Directors to suspend the relationship with the attacker while the police investigation was on-going. The NPO's Board of Directors later proposed to remove the individual from the directing official position within the NPO.

The attacker was later found guilty of the criminal offence of conspiracy to damage property and being reckless as to whether life would be endangered. Following the conviction, the individual resigned from the NPO's Board of Directors. Had the individual not willingly resigned, the regulator would have called for his resignation.

FALSE REPRESENTATION AND SHAM NPOS

Case Study 92 – False Representation and Sham NPOs

Two individuals were raising funds domestically to support a listed terrorist organisation operating in their country of origin. They solicited funds in person within the diaspora of their home country and through teleconferences featuring speakers who encouraged donations from the public to support the listed terrorist group. One of the individuals raised funds under the false pretence that the funds were for humanitarian relief. The individuals transferred the funds to the terrorist organisation, including through various money remittance companies, using false names to conceal the true identity of the recipients.

The Justice Ministry criminally convicted the individuals and sentenced them to prison terms of 10 years and 20 years.

Case Study 93 - False Representation and Sham NPOs (Reproduced in Chapter 4)

A domestic NPO established as a cultural youth association was the recipient of several government grants.

A law enforcement investigation into the operations of the NPO found that it was a front organisation for a terrorist group. The real activities of the NPO included raising and managing funds for the terrorist group, and disseminating the group's extremist message through the Internet.

While the NPO had a formally constituted governing body, it was created and directed by members of the terrorist group. The principle individuals involved were arrested and the NPO and its website were shut down.

Case Study 94 - False Representation and Sham NPOs

Media reporting suggested that a registered NPO was operating on behalf of a state supporter of terrorism, and was being used to channel funds to other domestic organisations in order to promote that state's interests.

The national regulator examined the NPO's obligatory reporting and determined that the NPO had no discernible activities except for receiving large amounts of money from a foreign organisation and distributing this money to sympathetic domestic organisations. Open-source research indicated that

the foreign organisation was in fact a branch of the state supporter of terrorism and had been used to support terrorist activities, intelligence-gathering, and political influence. The national regulator audited the NPO and uncovered that all the NPO's funding and directions were coming from the same overseas organisation. The NPO admitted that it had no control over its funding operations.

Based on these findings, the national regulator deregistered the NPO and shared relevant material with national security partners.

Case Study 95 - False Representation and Sham NPOs

Domestic law enforcement arrested an individual in a part of the country where there is a high incidence of terrorist activity. The individual stated that a domestic terrorist organisation, of which he was a member, solicited donations from the public by using vulnerable persons such as children, the physically challenged and the elderly to appeal for donations, essentially as a charitable cover for their fundraising activities. The donations were used to support the terrorist organisation's operations.

Case Study 96 - False Representation and Sham NPOs (Reproduced in Chapter 3)

A bomb blast occurred at a religious boarding school being operated as an unregistered NPO. The ensuing investigation found that the school was being used by members of a radical group to recruit students for attacks against local police, prosecutors and judges and for the manufacture of homemade bombs.

The director of the school was convicted of terrorism-related offences.

Case Study 97 - False Representation and Sham NPOs (Reproduced in Chapter 3)

Two individuals were raising funds domestically for a family member who was fighting alongside a listed terrorist organisation abroad. The individuals, claiming to be representatives of a well-known domestic humanitarian aid NPO, were raising the funds by way of public street collections. The collection efforts were in breach of the domestic law.

The individuals in question did not have the consent of the domestic NPO to solicit donations on its behalf nor did they deliver to funds raised to the NPO. Once a sizeable amount of money had been collected, it was sent to the family member abroad using wire transfers.

As a result of a joint investigation between the FIU, NPO regulator, and law enforcement authorities, the two individuals were arrested and convicted of terrorist fundraising and sentenced to jail.

Case Study 98 - False Representation and Sham NPOs

Domestic law enforcement arrested an individual in a part of the country where there is a high incidence of terrorist activity. The individual, who subsequently admitted to being a treasurer for a terrorist organisation, was in possession of mandatory donations collected from members of the terrorist organisation, as well as voluntary public donations meant to support humanitarian relief efforts. All of the funds were, however, used to support the activities of the terrorist organisation.

Case Study 99 - False Representation and Sham NPOs

An NPO was formed ostensibly to assist educational, religious and cultural programs. In reality however, the NPO was one of several organisations set up to fund the activities of a foreign terrorist group and promote the group's cause through supporting recruitment activities.

National security intelligence obtained during the course of an investigation into the terrorist group indicated that the NPO had harboured a wanted terrorist suspect in one of its buildings and had provided financial assistance to the family of a convicted terrorist. Additionally, open-source and law enforcement information revealed that the director of the NPO was himself a suspect in the investigation of a terrorist act.

The NPO was audited several times by the national regulator and was consistently unable to account for the origin and destination of significant portions of its funding. Additionally, there were indications that documents provided to the national regulator during one of the audits had been doctored. The audits revealed that the NPO had transferred funds to a known charitable front for the terrorist group, and that the NPO's educational and cultural programs promoted the goals of the foreign terrorist group.

The NPO was deregistered and information was passed to law enforcement and national security partners to further the existing investigation.

Case Study 100 - False Representation and Sham NPOs (Reproduced in Chapter 6)

A homemade bomb exploded in a house displaying a banner for an NPO supporting orphan relief. An investigation found that the NPO did not exist and that a terrorist group was disguising its bomb-making facility as an NPO office.

Law enforcement authorities seized a large cache of bomb making supplies and weapons. One member of the terrorist group was charged and convicted of terrorism related offences.

Case Study 101 - False Representation and Sham NPOs

A group of people formed an NPO to raise funds, through the sale of t-shirts, for the benefit of two foreign terrorist organisations. The NPO also sought to spread the view that the two foreign terrorist organisations were not in fact terrorist organisations, but rather, legitimate freedom fighters. The t-shirt sales were the subject of media reporting.

A law enforcement investigation, initiated by press reports, ultimately resulted in the main organisers receiving prison sentences for terrorist financing.

Case Study 102 - False Representation and Sham NPOs

Domestic law enforcement arrested an individual known to be a member of a domestic terrorist organisation. In addition to soliciting donations under the pretext of providing humanitarian relief, the individual stated that the terrorist organisation used subtle negotiations and intimidation to obtain protection fees from the state. While one state official refused to be coerced into making payments, other officials made personal donations to the terrorist organisation. The arrested individual's bank account showed monthly deposits, which were used to support the terrorist organisation's operations.