EGMONT GROUP

OF FINANCIAL INTELLIGENCE UNITS

REPORT ON FIUS' ROLE IN THE FIGHT AGAINST THE ABUSE OF NPOS FOR TERRORIST FINANCING ACTIVITIES

Information Exchange Working Group

Abstract

The EG IEWG developed this Report to support ongoing efforts in the fight against the abuse of NPOs for TF activities by identifying, updating, and expanding on existing information to develop new knowledge on typologies and financial threats.

Public Summary

April 2024

The Egmont Group is a united body of 174 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF).

The Information Exchange Working Group (IEWG) is a forum for Egmont Group FIUs and Observers to leverage synergies associated with operational and strategic activities to enhance cooperation and information exchanges and address challenges.

Project Leads: FIU Israel (IMPA) and FIU Nigeria (NFIU)

Project team member FIUs: Australia (AUSTRAC), Canada (FINTRAC), Finland (RAP), Greece (Hellenic FIU), Mauritius (FIU-Mauritius), the Netherlands (FIU-NL), South Africa (FIC) and United Kingdom (UK-FIU)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
AQAP	Al-Qaeda in the Arabian Peninsula
CTF	Counter Terror Financing
DNFBs	Designated Non-Financial Businesses
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IEWG	Information Exchange Working Group
ISIC	International Standard Industrial Classification of All Economic Activities
ISIL	Islamic State of Iraq and the Levant
ISWAP	Islamic State West Africa Province
IVTS	Informal Value Transfer System
KYC	Know Your Customer
LEA	Law Enforcement Agency
MENA	Middle East and North Africa
ML	Money Laundering
MSB	Money Services Business
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
NRA	National Risk Assessment
OFAC	Office of Foreign Assets Control
STR	Suspicious Transaction Report
TBTF	Trade-Based Terrorist Financing
TF	Terrorist Financing
UK	United Kingdom
UNSC	United Nations Security Council
UNSD	United Nations Statistics Division
US	United States
VASP	Virtual Asset Service Provider

EXECUTIVE SUMMARY

The objective of the Project is to support ongoing efforts in the fight against the abuse of Non-Profit Organizations (NPOs) for TF activities. This is achieved by identifying, updating, and expanding on existing information to develop new knowledge on typologies and financial threats. Additionally, the Project aims to provide an overview of how FIUs make the best use of international cooperation by sharing financial information and intelligence to enhance detection and achieve better results in disrupting the abuse of NPOs to finance terrorism.

INTRODUCTION

The NPO sector poses great challenges for FIUs due to its scale, distinctive structures and nature of the work undertaken. NPOs often work internationally, in or adjacent to conflict-afflicted areas, with those involved in humanitarian missions operating in the same environments and vulnerable populations as terrorist entities. This can render NPOs susceptible to exploitation and even have them be complicit with terrorist organizations and their TF activities.

The exploitation of NPOs for TF activities is acknowledged by the FATF, which has established Recommendation 8 specifically for NPOs. This recommendation outlines measures aimed at preventing the misuse of NPOs for Terrorist Financing purposes. However, concerns have been raised regarding the unintended consequences of these measures, which may result in de-risking and financial exclusion in the sector. Consequently, the FATF initiated a project to update the Best Practices Paper on Combatting the Abuse of NPOs, which has led to amendments to Recommendation 8 and its interpretative note.

This report supplements the FATF's work by providing a refined understanding of how NPOs are exploited for TF purposes. With a more detailed and nuanced view of NPO risk, this report should also contribute to broader initiatives aimed at preventing unintended consequences for NPOs that are at low or no risk of abuse.

The level of understanding of threats targeting NPO abuse for TF purposes is uneven among FIUs. Some threats persist while others evolve. Terrorist organizations have evolved their TF typologies partly in response to counter measures, including the abuse of NPOs through modern and sophisticated fundraising methods, such as DeFi, virtual assets, and FinTech platforms, to raise and transfer funds.

Considering the high risk and considerable global growth of the NPO sector, FIUs play a vital role in identifying and detecting transactions related to TF activities. Moreover, the international nature

of NPOs' activity highlights the importance of international cooperation and timely information sharing between FIUs. This requires the establishment of effective long-term CTF strategies and preventive measures by FIUs and their partner agencies, focusing on operational exchanges, strategic intelligence and analysis.

METHODOLOGY

The objectives for the Project were implemented in five stages:

i. Assessment of existing information/knowledge produced by relevant international organizations.
ii. A questionnaire about the abuse of the non-profit sector for TF was sent to all Egmont Group members.
iii. A call for sanitized operational cases. Please note that these case studies are not included in this sanitised version of the report.
iv. Analysis of the information received in responses from FIUs.
v. Delivery of a report examining NPO abuse for TF purposes and the role FIUs play in the fight against such abuse was then compiled.

LITERATURE REVIEW

Since 2001, the FATF has prioritized combatting TFi, including TF activity in the non-profit sector. As part of the inter-governmental body's efforts to mitigate the risks, it has held numerous consultations and published several reports about NPO abuse for TF purposes over the last two decades. In June 2014, the FATF published a typologies reportii on the risk of terrorist abuse in NPOs, with red flag indicators to assist stakeholders to identify and investigate possible cases of abuse. In 2016, FATF also revised the international standard on protecting NPOs from misuse shifting from a blanket approach to a targeted focus on the 'subset' of NPOs at most risk of misuse. It recognised that not all NPOs are exposed to risk, with some (or many) posing little or no risk for TF. Subsequent revisions targeted at mitigating the abuse of at risk NPOs are;

- In November 2023, the FATF published the updated standards in which the wording of sections of Recommendation 8 and its interpretive notes were revised to address the issue of excessive use of preventive measures on the NPO sector in some countries[iii].

- Also, in November 2023, the FATF's ongoing updates on the 'FATF Best Practices Paper on Combatting the Terrorist Financing Abuse of Non-Profit Organisations[iv].

Based on the literature available on NPO abuse for TF purposes, it can be concluded the phenomenon is a global concern with many sources of information found at the international and regional level.

NPO DEFINITION

Given the variety of legal forms that NPOs can have, depending on the country, the FATF has adopted a functional definition of NPO[v]. This definition is based on those activities and characteristics of an organization which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. According to the FATF, an NPO refers to *a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".*

The terms NPO and Non-Governmental Organization (NGO) are often used interchangably due to the fact that both are non-profit orientated and are often engaged in charitable work. However, the two terms are slightly different with regards to the scope of their operations. NGOs tend to have a broader operational and outreach footprint than NPOs[vi], with the former defined by the UN

as “is any non-profit, voluntary citizens' group which is organized on a local, national or international level[vii]”.

PROMINENT TYPOLOGIES

This literature identifies six methods prevalent in the abuse of NPOs for TF purposes :

1. Diversion of funds
2. Affiliation with a terrorist entity
3. Abuse of NPO programs
4. Providing support for recruitment
5. False representation
6. Fundraising through social media.

Diversion of funds[viii] is the most commonly observed typology and occurs when actors within or outside of an NPO divert the funds raised for humanitarian purposes towards terrorist activities with or without the NPO's knowledge. Fund transfers can also be made by using third parties such as sham organizations and through TBTF as highlighted in Section 2 of the 2020 FATF – Egmont Group publication on the subject.

The second most commonly observed method is NPO’s **affiliation with a terrorist entity**. This affiliation translates into the provision of financial and/or operational support for a terrorist group. Such connections range from NPO officials and employees having suspected or established ties to a terrorist entity, to more formalized relationships between the two parties[ix].

Terrorist entities can **abuse NPO programs** at the point of delivery to support terrorism by 'skimming'[x] off charitable donations and sending or using them to support terrorist activities.

NPO-funded programs or facilities can be exploited to create an environment which knowingly or unknowingly **provides support for recruitment** efforts by terrorist organizations.

False representation refers to when organizations or individuals falsely raise money for charitable purposes when in reality, the funds are used to support terrorism. False representation is divided into two categories:

1) Groups or individuals that falsely claim to act on behalf of existing NPOs. For example, UK intelligence and security services thwarted a bomb plot in Birmingham in 2011 wherein the attack was partly financed by terrorist cell members posing as Muslim Aid volunteers[xi].
2) NPOs can be created as a front to support terrorist activities[xii]. Terrorist groups, like legitimate entities, are constantly seeking to adapt to developments in the technological arena.

Lastly, the rapid expansion of **social media**, particularly encrypted messaging platforms, are being increasingly exploited by terrorist entities to raise funds from sympathetic individuals globally[xiii].

PROMINENT RISKS AND THREATS

In the 21st century, globalization and technological advancements have created an interconnected financial and supply chain network in which it is relatively easy to transfer funds or goods around the globe. This, in turn, has enabled NPOs to expand their fundraising and outreach capacity, drawing NPOs into unstable high-risk regions where the integrity of their operations is at risk.

Emergency response situations, such as pandemics or natural disasters, have increased the risk of NPO-related TF. Such situations prompt an uptick in fundraising activity by NPOs (legitimate and sham) to provide the necessary resources to aid urgent public health and rescue efforts. Terrorist entities can exploit emergency response situations to raise funds through sham NPOs or abuse legitimate NPOs to divert resources toward their terror activities[xiv].

The use of cash couriers[xv] also poses a significant risk for NPOs as this is recognized as a method used to move funds for terrorist purposes. The movement of cash disguised as legitimate transactions under the name of a NPO and charitable cause could make transportation less likely to be questioned or challenged, which increases the risk of terrorist assets being moved. In some cases, where financial infrastructure is limited or not functioning, cash becomes one of the few options available to NPOs for moving funds to beneficiaries. De-risking and financial institutions restricting wire transfers are reasons some NPOs resort to cash couriering.

Lastly, it is important to note that political considerations, especially during periods of election campaigning, may influence the monitoring of elements affiliated with or sympathetic to extremists causes. This threat should be monitored closely in the coming years due to the ever-increasing rise in popularity of the far-right[xvi].

PROMINENT VULNERABILITIES

Regions which are plagued by war, weak governance (including financial controls, risk management policies and procedures, and appropriate due diligence), corruption, poor infrastructure, are where terrorist organizations pose a higher risk to NPOs[xvii]. Areas of the world where genuine humanitarian relief is most urgently needed are often the same areas of the world where the risk of terrorism is greatest. This is because terrorist networks and NPOs often rely on similar logistical capabilities that are consistent through domestic or foreign operations. With more individuals, wider ranges of activities, and possibly substantial geographic distances involved, it can be difficult for NPOs to maintain adequate control of resources, scrutinize staff actions, perform due diligence and beneficiary verifications, and identify suspicious activity[xviii]. This can make it challenging to distinguish charitable activity from terrorist support.

Current legislation and reporting requirements mean that relevant authorities are addressing misuse after it has already occurred. Awareness of TF risk among NPOs varies, limiting their ability to identify and protect themselves from financial misuse. Limited visibility of the funding cycle[xix] (fundraising through to sending or spending domestically then abroad), compounds the vulnerabilities associated with the cash-intensive nature of most NPOs.

Overall, the key vulnerabilities of NPOs relate to their social purpose, cash-intensive nature, generally minimal regulatory oversight applied to their operations, and the social role and inherent trust[xx] associated with NPOs in the larger community. Embedding TF operations into the regular activities of a trusted organization is the ideal cover for criminal activities[xxi].

ISSUES CONCERNING SPECIFIC NPO TYPES/CATEGORIES

NPOs that are engaged in providing humanitarian services and/or operating in unstable high-risk environments are the most vulnerable to abuse[xxii]. NPOs operating in foreign jurisdictions are at risk of having their funds or goods abused at the point of distribution by the charity or partner organizations. Similarly, NPOs that operate domestically, within a population that is actively targeted by a terrorist movement for support and cover, are also exposed to TF risks. This is because resources generated locally may be transferred internationally to support terrorism if the organization does not exercise direction and control over the end-use of its resources. Unregistered NPOs are highly vulnerable to TF activity as they are subject to minimal to no oversight and very little is known about their operations.

There is a heightened ML/TF risk associated with religious organizations, particularly religious NPOs operating in environments or within populations that terrorist entities actively target. For example, Sunni terrorist groups, such as al Qaeda and ISIS, exploit the Islamic principle of Zakat to raise finance from Islamic communities around the globe. According to the principle, a person is required to give 2.5% of their annual excess wealth to charity.

UNINTENDED CONSEQUENCES

De-risking, described by the FATF as the "phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage risk[xxiii]" may push NPOs to use high-risk, unsupervised informal value transfer systems (IVTS). Such a shift would create visibility gaps. There is also a danger that undue targeting of NPOs may prevent the delivery of genuine relief aid, curtail human rights, and result in wrongful financial exclusion.

The need to implement measures to mitigate the risk of NPO exploitation to finance terrorism should be balanced against the continued ability for NPOs to undertake legitimate activities, such as assisting those in need of humanitarian aid. Given the potential for inadvertent harm to the sector and to legitimate beneficiaries, a risk-based approach should be implemented.

PROMINENT INDICATORS

Overall, the prominent indicators 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 capacity and intent to exploit NPOs[xxiv]. Specifically, 'service NPOs' primarily involved in the delivery of humanitarian services are the most desirable targets for terrorist entities due to the types of resources involved in their operations, the geographic scope of their operations (supply chain and logistics networks available), and their access to vulnerable populations. NPOs operating in locations or among populations that terrorist entities also actively target are at a higher risk of abuse. Notably, this does not always relate to geographic areas of conflict or poor governance. On the other hand, populations within relatively stable environments may still be actively targeted by terrorist entities for support due to their affiliation to a particular conflict, ideology, religous or enthnical group.

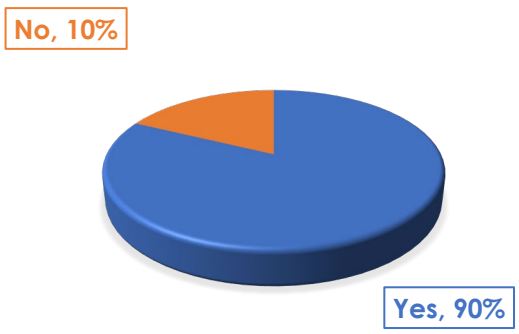
SECTION I – THE NPO SECTOR

The NPO sector plays a vital societal role by providing essential financial assistance and services to vulnerable populations locally and around the globe. 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. Through understanding the above FIUs can update and develop new knowledge on typologies involving the abuse of the NPO sector for TF purposes and improve the detection and prevention of such abuse.

THE REGULATION AND SCALE OF NPO SECTORS

In order to examine the extent of the threat of NPO abuse for TF purposes, a baseline regarding the size and regulation of the NPO sector needed to be established. Information was thus collected on the number of NPOs operating in each jurisdiction as well as the registration requirements and types of supervision or monitoring applied to NPOs. Based on the respondents' feedback, no significant correlation was found between the number of supervision measures and the risk perception of NPO abuse for TF purposes.

Figure 1: The percentage of respondents that require the registration of NPOs



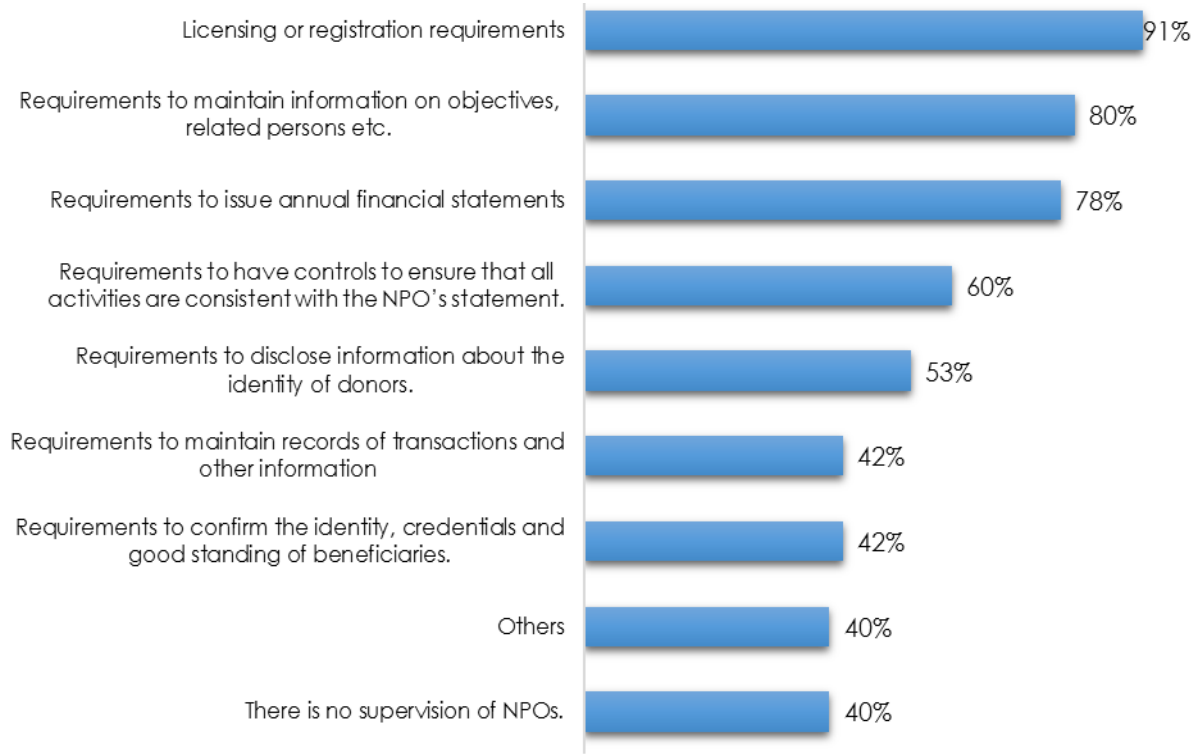
As illustrated in the above graph, NPOs have a registration or licensing requirement in the majority of the jurisdictions. Beyond registration requirements, it transpires that in most jurisdictions NPOs are also required to keep information over time and submit financial statements. The number of NPOs registered in jurisdictions is generally high, with some jurisdictions having over 100,000 registered NPOs. This reflects the large size of the NPO sector generally, noting 40% of jurisdictions that do not register NPOs, report sectors with over 100,000 known entities.

NPO sectors are also economically significant, with an annual turnover of almost USD50 to USD196 billion in jurisdictions that collect and report this data. **Lack of understanding of the NPOs landscape creates vulnerabilities and makes NPOs susceptible to abuse by criminals for terrorist financing, as well as the limited visibility and transparency of the volume of NPO funds.**

Some jurisdictions that do not register or license NPOs use other regulatory tools for monitoring. Examples include taxation systems where NPOs must enrol to receive tax concessions, or where legal entities or bank accounts are mandatory for receiving other government benefits. Nonetheless, these measures are not equivalent to an effective registration regime.

A significant number of jurisdictions also use a range of regulatory methods to monitor and supervise NPOs. Less commonly used tools include requirements to confirm the identity, credentials and good standing of beneficiaries and requirements to disclose information about the identity of donors. This could result from factors like strict data protection laws and a lack of a proper database management systems in place. It likely also creates vulnerabilities that TF actors can use to exploit NPOs.

Figure 2: Use of different types of supervision/monitoring tools applied to NPOs



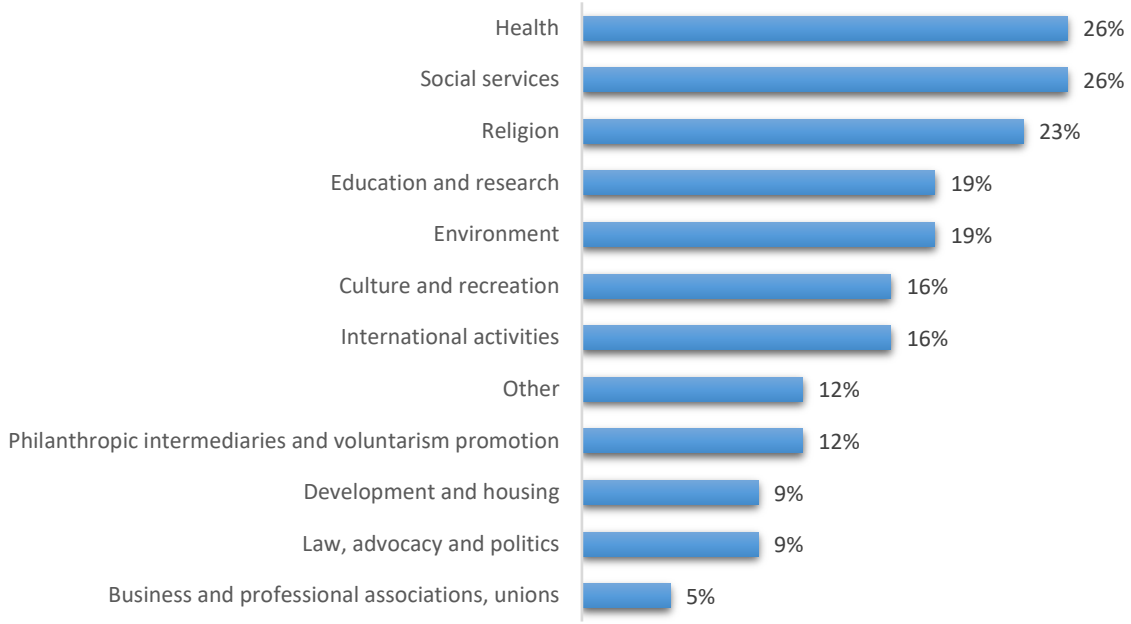
The above histogram illustrates the different types of monitoring/supervision tools that the jurisdiction of responding FIUs apply to NPOs. In certain countries, FIUs indicated that they use a variety of supervision tools, thereby resulting in the percentage total exceeding 100%. While NPO registration and licensing are common, they are not without problems.

NPOS FINANCIAL ACTIVITY

Terrorist organizations exploit NPOs in various ways to raise, move and store funds. In the past, money was distributed by the organizations' high command to various regional branches and cells using the formal banking system. The use of this strategy was fairly easy for law enforcement and security services to identify and stop. The implementation of sanctions and other enforcement measures reduced the ability of terror groups to acquire funding via the formal banking system. This forced terrorist organizations to alter their fundraising strategies and resulted in these organizations decentralizing and diversifying their fundraising activity. The shift from a centralized organizational structure to smaller self-sufficient affiliates means that terrorist operations require less funding now than before. Where terrorist organizations still need to move funds, they will usually use VASPs, MSBs and/or informal *hawala* transfer networks. They use trade-based terrorism financing techniques (TBTF) along with modern and sophisticated methods to raise and transfer funds, such as DeFi, crypto-currency, virtual assets, and FinTech platforms and applications.

NPOS TURNOVER

Figure 3: NPO categories with the highest turnover per jurisdiction



The NPOs were categorized based on the UNSD's ISIC, and information was collated on their yearly turnover, source of funding and changes in financial activity over the last 5 years. The ability to raise and move funds is one of the biggest vulnerabilities abused by terrorist organizations. Therefore, from the above figure, Health, Social Services and Religion are among the top categories of NPOs with the highest turnover within jurisdictions. This implies that FIUs and competent authorities should pay more attention to NPOs within these categories to prevent their potential abuse of Terrorism Financing.

However, the FATF risk-based approach to protecting NPOs from TF misuse requires other factors to be considered, primarily the subset of NPOs (regardless of sector or turnover) that jurisdictions identify as most exposed to misuse. As outlined below in section 3, the presence of domestic and foreign terrorist groups in a jurisdiction or its neighbours and regionally, as well as NPOs operating in or near conflict zones, are the key risks affecting NPOs. That said, the abuse of NPOs for TF purposes can also occur in other jurisdictions such as the UK or USA. For

example, the British charity called the Palestinian Relief and Development Fund[1] (Interpal) was designated by the US government in 2003 for funding and supporting terrorism. **This underlines the fact that TF does not only occur in the physical proximity of terrorist organizations and activities. Collection of funds can also take place in areas less associated with terrorism. This is particularly relevant at present as NPOs and terrorist actors can utilize online payment systems, to gain access to donors situated in different parts of the globe.**

Overall, the financial data, particularly when viewed as standalone figures, is not sufficient to indicate the level of risk or vulnerability posed by each category of NPOs. This is bolstered by the fact that the majority of respondents (60%) stated that the total yearly turnover of the NPO sector in their country was unknown. The small values involved in much TF activity also make (sub)sector turnover a questionable indicator of risk.

NPOS SOURCES OF FUNDING

Government funding and domestic donations are the most popular sources of funding for NPOs, according to the FIUs' responses. These sources of funding also appear to be channelled into the categories with the highest NPO turnover previously mentioned (Health, Social Services and Religion).

In theory, government funding of NPOs can reduce the risk of TF as governments are expected to conduct sufficient due diligence to ensure their funding does not reach nefarious actors such as terrorist organizations. However, in practice, governments often employ the services of private companies to examine NPOs. Audits are often performed by parties with limited knowledge and understanding of terrorism/terrorist financing. These companies are not properly certified and are not exposed to government or intelligence information that could help them understand and address the TF risks associated with NPOs.

To prevent TF, it is necessary for NPOs to conduct a more thorough examination of their sources of funding, with an emphasis on donations. To ensure this, there is a need for increased NPO

[1] *OFAC. (2023). Sanctions list search. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=7917. Accessed August 3, 2023.*

engagement and training as well as the implementation of appropriate supervisory measures on NPOs.

CHANGES IN FINANCIAL ACTIVITY VOLUME OVER THE LAST 5 YEARS

Most of the responding FIUs have indicated that the financial activity volume of the NPO sectors in their jurisdictions has increased or remained unchanged over the last 5 years. That said, the number of respondents to this question was particularly low (only 27%), therefore, this data cannot be used to draw any definitive conclusions.

Overall, the lack of data is concerning and may be due to the non-implementation of supervisory measures, a lack of knowledge or cooperation on the part of the NPO sector, or simply insufficient expertise to collect the relevant information**. The inability to gather sufficient data also casts doubt on the understanding of how the sector operates and of the risks pertaining to the NPO sector.** Consequently, **the lack of information can lead to the implementation of incorrect or ineffective supervisory and preventive measures**.

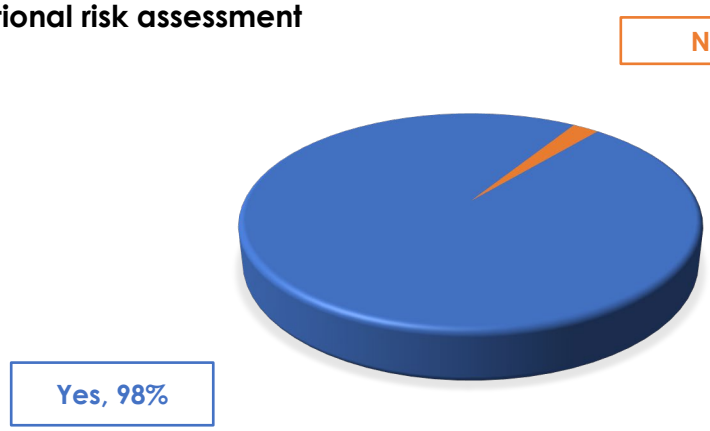
SECTION II – THE NPO SECTOR RISKS, THREATS AND VULNERABILITIES

TF RISKS AND THREATS EMANATING FROM THE NPO SECTOR

The risks arising from the NPO sector are diverse and can be linked to the activities of terrorist organizations abroad or in the jurisdiction itself. At the international level, the primary risk is the exploitation of NPOs in the region or neighboring countries (the activities of foreign terrorist groups in the region or in neighboring jurisdiction) and, in particular, in high-risk areas or conflict zones. In addition, there are local risks arising from the activities of domestic terrorist groups in their jurisdiction. At a domestic level, there are also risks related to the activities of radicals and lone wolves.

In this section, the project team examines the types, level of risk, and vulnerabilities of the NPO sector as perceived by the FIUs and seeks to raise awareness of NPO characteristics.

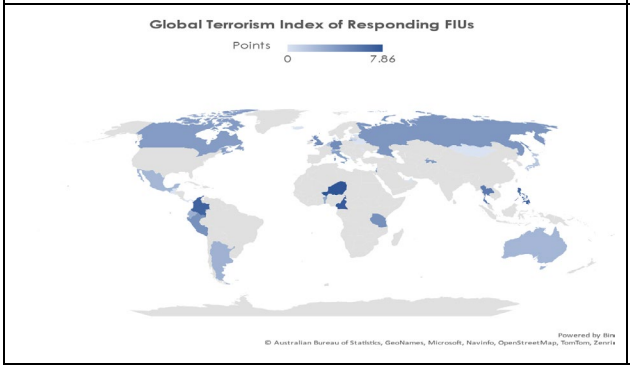
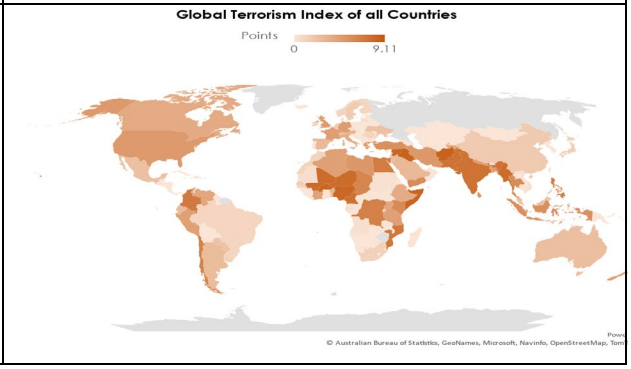
Figure 4: The percentage of FIUs that considered NPO sector-related TF risks in their national risk assessment



98% of FIU respondents indicated that TF risks emanating from the NPO sector were taken into consideration in their recent National Risk Assessments.

In their respective NRAs, nearly all participants assessed TF risks relating to NPOs as low to medium level, with only 16% rating it high. This outcome can be explained by the population of the responding FIUs comprising jurisdictions with a low global terrorism financing index (see below).

According to the 2023 Global Terrorism Index[xxv], the FIUs in jurisdictions mostly affected by Terrorism and Terrorism Financing activities did not respond to the questionnaire. While this gap may not overly alter broad findings, further examination of the threat of TF abuse, directly or indirectly, for NPOs operating in or near conflict zones is needed in order to build a holistic picture of the risk.

Global Terrorism Index of Responding Jurisdictions	**Global Terrorism Index of all Countries**
	

Additionally, the abuse of NPOs for TF purposes may be a less prominent source of funding for terrorist groups than other typologies such as kidnapping for ransom, looting, extortion, and drug trafficking. Limited usage of NPO-related TF has likely played a role in the formulation of the respondents' low to medium threat perception.

On the other hand, as seen in some mutual evaluation reports, there are jurisdictions where the risk of TF is viewed too narrowly and linked to only the presence of terrorist risks and terror acts committed in that jurisdiction. This can lead to incomplete and inaccurate risk assessments. TF can be a significant risk for jurisdictions otherwise relatively immune to terrorism groups or threats, due to financial and trade factors, migrant communities and geopolitical locations, among other things. Terrorist organizations exploit the high trust that NPOs have in the country and lax governmental supervision (which is determined according to the NRA) to operate in areas considered low terrorism risk areas. FIUs may fail to locate suspicious transactions and information that fall outside their designated focus areas and strategic activity. Furthermore, as previously stated, there is not enough information available regarding the financial activity of NPOs, which limits the state's ability to assess risks.

In order to gauge the overall risk perception of NPO related TF, all FIU responses were summarized and normalized to formulate a uniform measure. Analysis of the data shows that the risk perception of jurisdictions where mandatory registration of NPOs is required is lower than the risk perception in jurisdictions where this obligation does not apply. FIU respondents exhibited a higher risk perception when FIUs sent a higher number of information requests involving NPO and TF to other FIUs. Similarly, a higher risk perception was shown by countries where FIUs disseminated a higher number of reports involving NPOs and TF. In contrast, countries displayed a lower risk perception towards the threat of NPO abuse for TF purposes when they employed more stringent regulatory requirements and when FIUs had higher levels of collaboration with DNFBs.

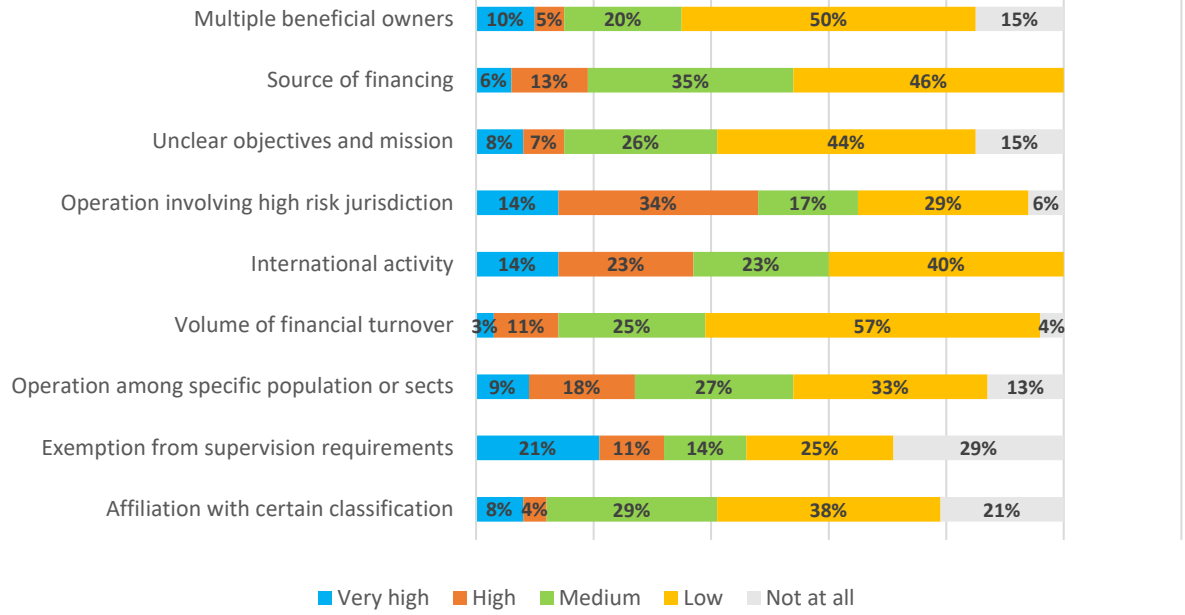
For the majority of FIUs, the activities of terrorist groups, either in their jurisdiction or based in their neighbouring countries or region, pose key threats to NPOs. Other areas of concern to FIUs are the establishment of sham NPOs following natural disasters or epidemics, the exploitation of charities operating in or near conflict zones, the ease of establishing and closing NPOs, and the use of online platforms to solicit funds.

NPOS VULNERABILITIES TO TERRORISM FINANCING ABUSE

The NPO sector operates in a unique way and enjoys a high level of trust from governments and the public. However, certain sector characteristics expose NPOs to abuse by terrorist organizations for TF purposes. These characteristics can be related to the NPOs' field of activity, operation among certain populations, geographic area of activity, source of financing, and more.

The following graph illustrates the level of vulnerability assigned by FIUs to nine specific NPO characteristics with regard to their susceptibility to TF abuse. The majority of FIU respondents perceived all the NPO characteristics to be of a low to medium vulnerability to TF abuse. This result aligns with the fact that virtually every FIU respondent perceived TF risks relating to NPOs as low to medium level. Based on the responses, an operation involving a high-risk jurisdiction is the most vulnerable to TF abuse, followed by international activity and exemption from supervision requirements.

Figure 5: NPO characteristics and their perceived TF risk



NPOs, particularly those providing humanitarian services in economic and geopolitically unstable jurisdictions, are vulnerable to exploitation by terrorist organizations for TF purposes. This is because the target population/s for NPOs and terror organizations in such jurisdictions are typically intertwined, thus making it difficult to differentiate terrorist support from charitable endeavours. In addition, limited regulation of the NPO sector in both low and high-risk jurisdictions

increase the risk of abuse of non-profits for TF. The lack of adequate oversight procedures enables nefarious actors, such as terrorist groups, to set up sham NPOs or infiltrate legitimate non-profits with the aim of siphoning off funds to support terrorist activity. The absence of supervision also enables NPOs to obscure their sources of funding, thus providing donors with relative anonymity. Radicalized individuals or persons supportive of radical ideologies can exploit the lack of transparency to donate funds to terrorist organizations.

SECTION III – MEASURES

The project is limited to the FIU participant perspective and does not account for perspectives from other government bodies that might render regulatory oversight of NPOs in certain jurisdictions. Statistically speaking, FIU participants rated mechanisms for international cooperation as the element most contributing to the effectiveness of dealing with the risks and vulnerabilities relating to the abuse of NPOs for TF. Other elements include investigation and information gathering, supervision or monitoring and sustained outreach. These findings correspond with the tools, means, and methods perceived by FIUs to ensure that NPOs are not being misused for TF purposes. In addition, the responding FIUs listed educating NPOs and other sectors about TF risks, typologies and mitigating factors as the main measure to ensure that NPOs are not being misused for TF purposes. This was followed by regular monitoring and supervision, conducting risk assessments on a consistent basis, NPO-related legislation, and collaboration with other FIUs.

Collaboration with the financial institutions was most effective in mitigating the risks relating to the abuse of NPOs for TF in the views of the responding FIUs. This was followed by collaboration with domestic LEAs, security agencies, and prosecution authorities.

In order to mitigate the risks relating to the abuse of NPOs for TF, it is recommended that jurisdictions mandate NPO registration and appoint a supervising authority to oversee the NPO sector. While this measure does not fall within the area of responsibility of most FIUs, they can collaborate with the relevant authorities to raise awareness of the risks pertaining to NPO abuse for TF purposes.

SECTION IV – FIU'S ROLE IN IDENTIFICATION AND DETECTION

STRS – GENERAL TRENDS

Many project participants reported general increases in overall suspicious transaction reports during the period under review, 2019-2021. There was a substantial increase in the number of

STRs concerning suspicions of money laundering (an increase of 350%). There was also a considerable increase in the number of reports concerning suspicions of TF activity (an increase of 82.6%).

There was a jump in STRs between 2020 and 2021. Increased awareness among reporting entities of ML/TF risk and associated indicators is one likely reason for the rise. Another potential contributing factor was the COVID-19 pandemic[xxvi] which brought changes in financial behaviours and patterns. The public and criminal actors found alternative methods to move funds, such as online financial services and virtual assets. The concern that terrorist groups would use these methods to raise and move funds may be the cause for the substantial increase in STRs.

STRS - SUSPICION OF TF INVOLVING NPOS

Similarly, there was a substantial increase in the number of STRs linking NPOs and terror financing, with a relative increase of about 310% identified.

The responses indicated an increase in the number of STRs involving NPOs linked to terrorist financing in 2021 which is more than double the figures for 2019.

The consistent increase in the number of received STRs related to TF involving NPOs might be explained by several factors. These factors include changes in the terrorism landscape and loss of some revenue source have seen terrorist groups and their financiers turning to alternative methods of raising/moving funds, including the misuse of NPOs.

Despite the consistent increase in the number of received STRs related to TF involving NPOs, the absolute numbers of STRs are low. The low number of STRs may be due to the fact that more than half of the participant's jurisdictions do not require NPOs to disclose information about the identity of donors. The lack of awareness of reporting entities, inadequate training and resources can result in suspicious transactions going unnoticed and thus not be reported.

Secondly, there are discrepancies in terms of which entities and/or individuals are listed in the various terrorism designation lists i.e. OFAC and UNSC lists. For example, Hezbollah in its entirety is listed by OFAC as a terrorist entity while the group is not included in the UNSC list. Reporting entities often do not consider the actions of undesignated entities to be suspicious and therefore do not report. Due to high societal trust in NPOs, reporting entities may attribute suspicious financial activity to another entity rather than to an NPO, or they may not report such

activity at all. To potentially rectify these issues, red flags and risk indicators should be sent to NPOs.

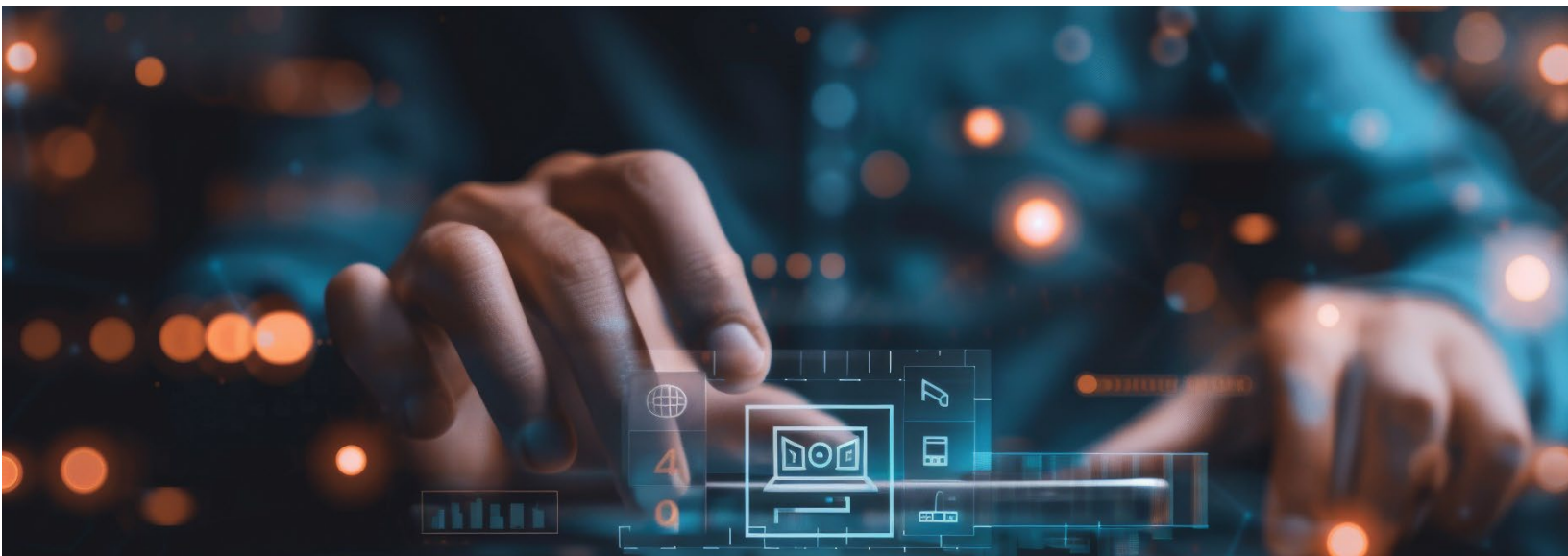
It is common that terrorists and terrorist organizations use cash or informal value transfer systems such as *hawala* and trade-based methods (TBTF) to transfer funds, making the identification and subsequent reporting impossible. In addition, difficulty in detecting potential NPO abuse for TF is compounded by the fact that the sum of money needed to finance small terror cells, lone wolves, and modern-day terrorist attack is usually relatively low. This means terrorist actors can infiltrate or manipulate legitimate NPOs to transfer lawfully acquired funds to terrorist organizations without arising suspicion.

Overall, detecting the abuse of NPOs for TF is a great challenge due to the use of the low amounts of money, informal methods of transferring funds, high public trust in NPOs, and the use of cash by the terrorists and terrorist organizations.

STRS INVOLVING NPOS AND UNSC OR OTHER DESIGNATION LISTS

Obliged entities check persons and entities against a variety of designation lists, including the United Nations Security Council resolution (UNSCR) lists, domestic designation lists and other jurisdictions' designation lists. Such lists contain the names and details of countries, organizations, and individuals that are subject to economic, trade, or diplomatic sanctions due to their criminal or terrorist activity.

The lists most commonly in use by reporting entities according to the project participants are UNSCR 1267 and its successor resolutions', followed by UNSCR 1373 and domestic designation lists. Additionally, other lists in common use include Dow Jones Watch List, UNSCR 1988, the European Union sanction list, OFAC List and more.



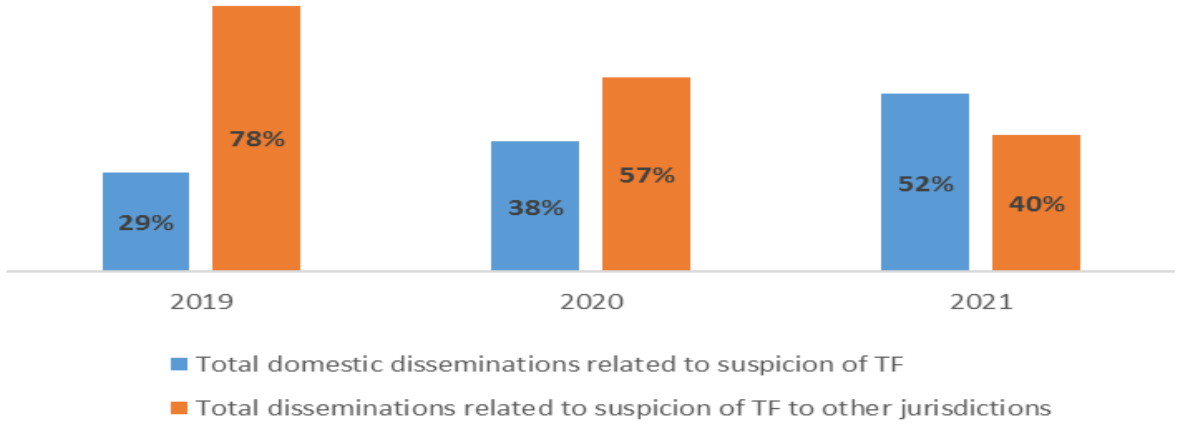
SECTION V – FIU'S ANALYSIS OF FINANCIAL INFORMATION

REPORTS DISSEMINATED BY FIUS CONCERNING NPOS

During the years under review, 2019-2021, project participants reported overall annual increase of about 29% in the total number of disseminated reports concerning both ML and TF domestically and internationally combined. The relative increase in reports concerning TF amounted to only 12% to 14% each year.

During the years 2019 – 2020, there was a noticeable increase in the volume of reports disseminated in which NPOs were involved, both in general (an increase of 310%), and with reference to TF (an increase of 393%). In 2021, the increase continues albeit in lower volumes, including reports in relation to NPOs in general (28% increase) and in relation to NPOs in which terrorist financing is involved (69% increase). Overall, the proportion of NPO disseminations out of the total TF reports rose significantly from 8% in 2019 to 28% in 2020. This increase continued in 2021, albeit at a slower rate, with NPO disseminations accounting for 32% of all TF disseminations that year. These findings seem to be in line with the increased STRs on NPOs.

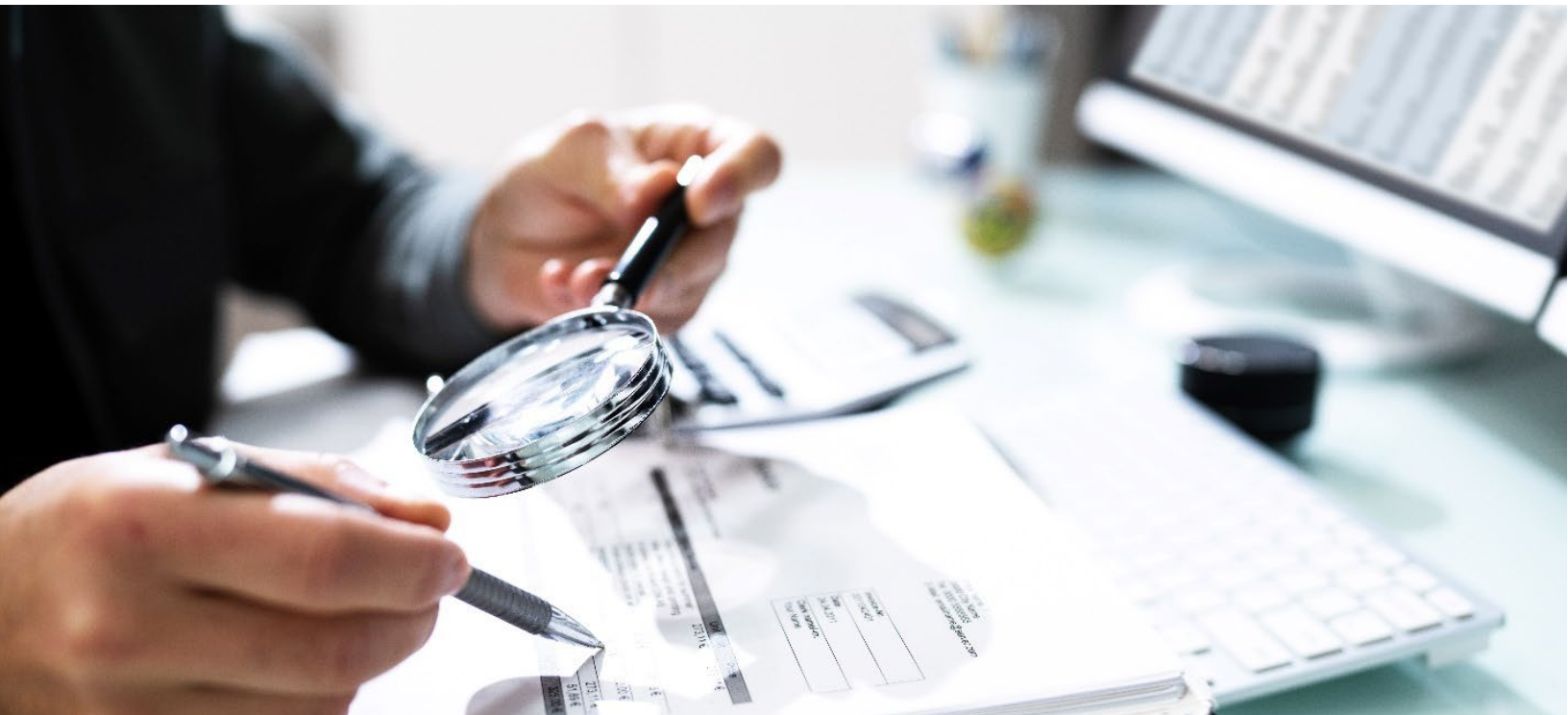
Figure 6: Jurisdictional breakdown of the total NPO-related TF disseminations



These figures are interesting when considered against some of the reasons put forward to explain increased NPO-related STRs mentioned above. Increased domestic disseminations might reflect the general growth in NPO-related STRs, as well as authorities focusing on investigating domestic NPOs to disrupt TF at its source. A decline in terrorist attack planning in some countries may have

also contributed to authorities shifting their focus to domestic TF to support extremist ideology, propaganda, and recruitment.

Another reason for the uptick in domestic disseminations is the shift in terrorist organizations' fundraising strategies in recent years. Groups, such as Al Qaeda and ISIL, have adopted a decentralized organizational structure whereby their various affiliates have been empowered to become more self-sufficient financially and operationally. The shift away from large, centralized organizations to localized affiliates and cells has enabled terrorist groups to operate on a smaller budget.



CONCLUSION

Most questionnaire respondents assess the threat of NPO abuse for TF purposes as low or medium level. The risks arising from the NPO sector are multifaceted and include operating in or near conflict zones, the presence of terrorist organizations in their jurisdiction or region, and religious or humanitarian activities that provide cover for TF. That said, TF risks relating to NPOs are not limited to high-risk war-torn regions and it is incorrect to perceive a lack of terrorism activity as meaning no TF threat. Non-profits also conduct fundraising campaigns in jurisdictions less associated with terrorism.

Over time, terror groups have decentralized and diversified their fundraising strategies due to law enforcement success in thwarting TF activity within the formal banking sector. The adoption of emerging technologies, such as crypto-currency, virtual assets, IVTS, and FinTech, have made it more difficult for FIUs to detect and investigate TF activity, particularly when the payment system is based in a jurisdiction with weak AML or CTF measures. The difficulty in detecting potential NPO abuse for TF is exacerbated by the fact that limited funds are usually required to finance a modern-day terrorist attack. This means nefarious actors can infiltrate or exploit genuine NPOs to siphon off funds towards terrorist groups without arousing suspicion.

While NPO registration and licensing are common, they are not without flaws. Limited regulation of the NPO sector in both low and high-risk jurisdictions increase the risk of abuse of non-profits for TF. There is also a clear lack of sufficient information available regarding the financial activity of NPOs, which limits a nation's ability to evaluate risks and may indicate a misunderstanding of how the sector functions as well as its related risks.

Beyond the detection challenges, investigating information related to the exploitation of NPOs for TF is also challenging for FIUs. This is due to the fact that the parties involved in TF in many cases do not have criminal records or there is no suggestion of previous involvement in TF. Hence, even when financial data is accessible, it is often not considered suspicious unless there is a direct link to terrorist acts and showing that charitable donations are being used to finance terrorist activities can be difficult.

Given nearly all the FIUs considered the risk posed by NPO abuse in their recent NRAs shows there is a general awareness of the threat of NPO abuse for TF. However, the lack of sufficient information available about NPO financial activity is worrisome and may have led to an incorrect assessment of the threat posed by NPO abuse as well as the implementation of incorrect or ineffective supervisory and preventative measures.

Overall, FIUs play a critical role in detecting TF activities due to the NPO sectors' global reach, growth, and risk. Due to their importance in mitigating the risk of NPO abuse for TF, FIUs need to be proactive in their engagement with the NPO sector, regulators, reporting entities, domestic partners and LEAs, and foreign FIUs and LEAs.

RECOMMENDATIONS

Abusing NPOs for terrorism is a global issue and cross-border movement of funds necessitates international collaboration. The following recommendations aim to raise awareness and to mitigate the risk of abusing NPOs for TF and are based on the project's findings. The recommendations are not binding, and jurisdictions may have different models in place that warrant different approaches:

1) Jurisdictions are encouraged to create and promote publicly accessible online databases for NPOs. These databases will allow the general public to search for and access information related to NPOs' status, activities, finances, and trustees. These databases will help promote transparency and maintain public trust in the NPO sector and facilitate international information sharing, enabling partners to find details about NPOs operating beyond their own jurisdiction.
2) FIUs, supervisors and relevant authorities are advised to educate reporting entities about the various designation lists in existence as well as the importance of checking as many of these lists as possible when investigating NPO trustees and activities. Additionally, training sessions with reporting bodies should be arranged to ensure the reporting entities know how to properly check designation lists.
3) Increased engagement with prominent social media companies is advisable. Platform moderators should be educated about the dangers of NPO abuse for TF, the methods used, red flag indicators, as well as the entities to report suspicious activity too. This will help improve platform moderators' ability to identify potentially suspicious NPO fundraising activity and may increase the number of NPO-related TF STRs received by FIUs.
4) It is advisable that NPOs be required to maintain registered bank accounts, create annual financial statements, and utilize regulated channels or systems to conduct financial transactions. This will result in NPO accounts being brought under the relevant controls or regulations of the financial system.
5) The results from strategic analysis should lead to intelligence-based policies to be implemented in order to disrupt and prevent TF through NPOs.

6) The use of multiple designation lists by the relevant stockholders is advisable when examining the activity and investigating the legitimacy of NPOs, their trustees, donors and beneficiaries.

[i] FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html. Accessed on July 12, 2023.

[ii] FATF. (2014). *Risk of terrorist abuse in non-profit organisations*. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Risk-terrorist-abuse-non-profits.html. Accessed on July 12, 2023.

[iii] FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html. Accessed on July 12, 2023

[iv] FATF (2023) Best practice paper on combatting the abuse of non-profit organizations https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html. Accessed December 2023

[v] FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html. Accessed on July 12, 2023.

[vi] Carnegie Mellon University. (n.d) Key differences between Non-Government Organizations (NGO) and Non-Profit Organizations (NPO). https://www.cmu.edu/career/documents/industry-guides/NGOs%20and%20NPOs.pdf. Accessed on August 20, 2023.

[vii] United Nations. (2023). *The UN and civil society*. https://www.un.org/en/get-involved/un-and-civil-society#:~:text=Association%20with%20the%20UN%20Department%20of%20Global%20Communications&text=A%20civil%20society%20organization%20(CSO,local%2C%20national%20or%20international%20level. Accessed on September 12, 2023.

[viii] FATF. (2014). *Risk of terrorist abuse in non-profit organisations*. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Risk-terrorist-abuse-non-profits.html. Accessed on July 12, 2023.

[ix] Federal Ministry Republic of Austria Finance. (2023). *NPOs and prevention of terrorist financing.* https://www.bmf.gv.at/en/topics/financial-sector/money-laundering-and-terrorist-financing/npos-and-prevention-of-terrorist-financing.html. Accessed on July 13, 2023.

[x] ACNC. (2023). *Terrorism financing*. https://www.acnc.gov.au/tools/guides/terrorism-financing. Accessed on July 12, 2023.

[xi] FATF. (2014). *Risk of terrorist abuse in non-profit organisations*. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Risk-terrorist-abuse-non-profits.html. Accessed on August 20, 2023.

[xii] Ministry of Interior of the Czech Republic. (2020). Awareness Raising For The NPO Sector Regarding The Fight Against Terrorism Financing. https://www.mvcr.cz/chh/soubor/awareness-raising-for-the-npo-sector-regarding-the-fight-against-terrorism-financing-eng-final-pdf.aspx. Accessed on July 13, 2023.

[xiii] US Department of Justice. (2020). *Global disruption of three terror finance cyber-enabled campaigns*. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns. Accessed on July 13, 2023.

[xiv] De Willebois, E. (2010). *Nonprofit Organizations and the Combating of Terrorism Financing A Proportionate Response*. The World Bank Working Paper, 208. https://doi.org/10.1596/978-0-8213-8547-0. Accessed on July 13, 2023.

[xv] HM Treasury. (2020). National risk assessment of money laundering and terrorist financing 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf. Accessed on July 13, 2023.

[xvi] Federal Ministry of the Interior and Community. (2020). *Sectoral risk assessment Terrorist financing through (the abuse of) non-profit organisations in Germany*. https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2020/sectoral-risk-assessment.pdf?__blob=publicationFile&v=8. Accessed on July 13, 2023.

[xvii] Singapore Office of the Commissioner of Charities. (2015). *Protecting Your Charity Against Money Laundering and Terrorist Financing.* https://www.charities.gov.sg/_layouts/15/download.aspx?SourceUrl=/PublishingImages/Fund-Raising/Use-of-OFR-and-CFR/Documents/AgainstMoneyLaunderingTerroristFinancing-May-2015.pdf. Accessed on July 13, 2023.

[xviii] FATF. (2014). Risk of terrorist abuse in non-profit organisations. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Risk-terrorist-abuse-non-profits.html. Accessed on July 12, 2023.

[xix] AUSTRAC. (2018). *Non-profit Organizations & Terrorism Financing Red Flag Indicators*. https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf. Accessed on July 13, 2023.

[xx] Charity Commission of England and Wales. (2022). *Guidance Compliance toolkit chapter 1: Charities and Terrorism*. https://www.gov.uk/government/publications/charities-and-terrorism/compliance-toolkit-chapter-1-charities-and-terrorism. Accessed on July 13, 2023.

[xxi] NZ Charity Services. (n.d.) *Charities Operating Overseas: protect your charity against terrorist financing risks.* https://www.charities.govt.nz/assets/CFT-Outreach-Resource-002.pdf. Accessed on July 13, 2023.

[xxii] GAFILAT. (2021). *Report on guidelines and challenges to prevent the misuse of NPOs for terrorist financing in GAFILAT countries*. https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traducciones/4191-report-on-guidelines-and-challenges-to-prevent-the-misuse-of-npos-for-terrorist-financing-in-gafilat-countries/file. Accessed on July 13, 2023.

[xxiii] FATF. (2021). *Mitigating the Unintended Consequences of the FATF Standards*. Available at: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Unintended-consequences-project.html. Accessed on July 13, 2023.

[xxiv] FATF. (2014). Risk of terrorist abuse in non-profit organisations. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Risk-terrorist-abuse-non-profits.html. Accessed on July 12, 2023.

[xxv] Institute for Economics & Peace. Global Terrorism Index 2023: Measuring the Impact of Terrorism, Sydney,

March 2023. Available from: https://www.economicsandpeace.org/wp-content/uploads/2023/03/GTI-2023-web.pdf. Accessed on October 9, 2023.

[xxvi] FATF (2020), COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html. Accessed on August 6, 2023.