THE UNITED REPUBLIC OF TANZANIA

FINANCIAL INTELLIGENCE UNIT

TERRORIST FINANCING RISK ASSESSMENT REPORT, 2022

MAY, 2022

(Revised in June, 2023)

Table of Contents

ACRONYM

ADF	-	Alliance Democratic Force
AML	-	Anti-Money Laundering
AMLA	-	Anti-Money Laundering Act (For Tanzania Mainland)
AML/CFT	-	Anti-Money Laundering/Combating Financing of Terrorism
AMLPOCA	-	Anti-Money Laundering and Proceeds of Crime Act (For Zanzibar)
ASWJ	-	Ansar al-Sunnah wal –Jama'ah
CBDC	-	Cross Border Declaration of Currency
CDD	-	Customer Due Diligence
CTF	-	Counter Terrorism Financing
DNFBPs	-	Designated Non-Financial Services Businesses and Professions
DCEA	-	Drugs Control and Enforcement Agency
DPMS	-	Dealers in Precious Metals and Stones
DRC	-	Democratic Republic of Congo
EAC	-	East Africa Community
EU	-	European Union
ESAAMLG	-	Eastern and Southern Africa Anti-Money Laundering Group
FATF	-	Financial Action Task Force
FIU	-	Financial Intelligence Unit
FSRBs	-	Financial Styles Regional Bodies
FTFs	-	Foreign Terrorist Fighters
GBP	-	Great Britain Pound
GN	-	Government Notice
ISIL	-	Islamic State of Iraq and the Levant
ISIS	-	Islamic State of Iraq and Syria
KYC	-	Know Your Customer
LEAs	-	Law Enforcement Agencies
MVTs	-	Mobile Value Transfer Services
NPOs/NGOs	-	Non-Profit Organizations/ Non-Governmental Organizations
NPPS	-	New Payments, Products and Services
NPS	-	National Prosecution Services
NRA	-	National Risk Assessment
ODPP	-	Office of Director of Public Prosecution of Zanzibar
PCCB	-	Prevention and Combating of Corruption Bureau

RITA	-	Registration, Insolvency and Trusteeship Agency
SADC	-	Southern African Development Cooperation
TF	-	Terrorist Financing
TFS	-	Targeted Financial Sanctions
TIRA	-	Tanzania Insurance Regulatory Authority
UAE	-	United Arab Emirates
UK	-	United Kingdom
USA	-	United States of America
UNODC	-	United Nations Office and Drug Crimes
UNCTOC	-	United Nations Convention on Transnational Organized Crime
VEO	-	Violent Extremist Organization

EXECUTIVE SUMMARY

Background on the TF Assessment

Terrorist financing is the financing of terrorist acts, terrorists, and terrorist organizations. This involves the generation and movement of funds for the sole purpose of committing terrorist acts or sustaining a terrorist network and organization. The definition of funds for the purpose of terrorist financing means assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal document or instruments in any form, including electronic or digital, evidencing title to, or interest in, such asset and for the purpose of this risk assessment will include instrumentalities provided and used for the purpose of terrorist activity.

Terrorism financing typically involves four stages - the first being raising of funds, through donations, self-funding (micro-loans or wages), or criminal activity; the second stage involves transferring funds to a terrorist, terror network, organization, or cell and third stage storage and fourth stage is using the funds, for instance, to purchase weapons to make payments to terrorists or insurgents, or to fund expenses of terror networks. Where the terrorist is a lone actor, the second stage may not occur.

In the United Republic of Tanzania, Terrorist Financing Risk Assessment was first conducted in 2016 during the general National AML/CFT Risk Assessment. The exercise was defined as a comprehensive process of identifying and analyzing the main threats, vulnerabilities of TF in the country and determining the risk levels as a result of identified threat and vulnerabilities. The 2016 NRA did not take into consideration key aspects of NPOs vulnerability to TF or the vulnerability of legal persons and legal arrangements. These deficiencies are intended to be addressed in this current TF Assessment.

The objectives of conducting a Risk Assessment on Terrorist Financing are to identify the overall Threats and Vulnerabilities of the country to terrorist financing; to review the adequacy of measures in URT to prevent terrorism and terrorist

financing and to prioritize actions that will improve the country's ability to combat terrorist financing in order to develop risk-based Counter Terrorist Financing (CTF) actions. By implementing rolling CFT Action Plan, with strict governance, URT will embed sustained reform to dynamically address the TF risk which will facilitate the allocation of available resources in the most effective way.

The assessment was conducted on the basis of a self-assessment by Tanzanian authorities, using the expert's opinion and World Bank methodology tool with customization of the following steps:

- development of a specific questionnaire;
- formulation of working groups; and
- identifying threat and vulnerability and assigning risk rating after the assessment of the threats and vulnerabilities.

FIU on behalf of the National Committee coordinated the exercise and worked in close collaboration with the CFT key stakeholders. The exercise involved 50 participants from key government and private sector institutions from Tanzania mainland and Zanzibar. The Assessment process included the following activities:

- Preparation of methodology;
- Consultative meeting with stakeholders;
- Collecting statistics and Report writing;
- Validation and adoption.

The customized methodology tool defines **Terrorist Financing Risk** at the national level as a function of **National TF Threat** and **National TF Vulnerability**.

The Overall Terrorist Financing risk at the national level is assessed to be **MEDIUM LOW** whereby **TF Threat is Medium-Low**, while **TF Vulnerability is Medium-Low**.

Terrorism and terrorist financing – the URT context

Generally, Tanzania faces TF threat from Ansar al-Sunnah wa –Jama'ah (ASWJ),

ADF, Al-Qaeda and Al-Shabaab. In 2012, Al- Shabaab became an affiliate of Al-Qaida and adopted a more regional strategy involving increased clear-cut terrorist tactics such as attacking civilian's targets in neighboring countries resulting into a major transnational threat. In the case of the US Embassy bombing in Dar es Salaam in 1998, Al-Qaeda had managed to recruit some Tanzanians to perpetrate the attack.

URT has observed that globally, terrorist, terrorist organizations and terrorist groups engage into criminal activities to raise funds to fund their organizations and operations. In 2020 the terrorist Group affiliated to Islamic State of Iraq and the Levant (ISIL) in Mozambique crossed the border and attacked Kitaya, Michenjela and Maulanga villages on the side of URT. In line with the CT initiated to confront that attack, parallel TF investigation was also conducted to identify those engaged to facilitate or accommodate the killing of innocent people. The investigation did not establish or link any person with TF but proved that terrorist had shot of food and drugs and decided to cross the border for that purpose.

Experience shows that terrorist organizations and terrorist groups continue to develop international networks and establish alliances of convenience with criminals as the means to raise funds. To the extent that trafficking in wildlife and poaching, drugs trafficking, illegal smuggling of precious stones and metals, trafficking in counterfeit goods and smuggling of immigrants occurs in URT, it is imperative for the Government to be vigilant and take appropriate action including proportionate and dissuasive sanctions against these vices.

Generally, the sectors and services that are vulnerable to TF include **cross border transportation of cash**, **money transfer services**, **non-profit organizations**, **informal value transfer (hawala) services, and electronic money services**. The present assessment recommends that capacity building to all stakeholders should be strengthened to ensure TF offences are detected, investigated, prosecuted and the funds and assets owned or belonging to terrorists are accordingly targeted for financial sanctions. TF awareness initiatives should be conducted and sanction list dissemination and updates be made on timely manner and should be applied without delay.

URT has established Economic Crimes Centre (ECC) comprising of all Law

Enforcement Agencies (LEAs) to fast-track the investigation (parallel investigation) of all suspicious transaction reports (STR's) concerning money laundering, terrorist financing, and the financing of weapons of mass destruction. The center will provide practical training and accreditation of the staff of the center on detection, investigation, prosecution, forfeiture, seizure and other related issues. The trained staff will be accredited by international accreditation institution. This is expected to boost, strengthen and reinforce Tanzania's response to complex terrorist financing cases through stronger coordination across all law enforcement agencies. It is also expected to facilitate CFT partnership on the use of financial intelligence, investigating TF offences and enhance training and expertise on TF investigation, prosecution and adjudications of cases.

This Terrorist Financing Risk Assessment will be used as a guide to the understanding of TF typologies and effective implementation of TF counter measures in URT. The recommended actions to be taken will be implemented by stakeholders to alleviate the threats and vulnerabilities to TF, thus mitigating the overall risk and managing the residual risk. This Assessment also recommends for a National TF Strategy that among others, sets out appropriate actions to be taken to ensure there are mechanism for coordination, monitoring and evaluation of CFT measures in URT for better effectiveness of the law and international standards.

This assessment updates the National Risk Assessment Report of 2016 and will continue to be updated to keep up with the evolving nature of the crimes of terrorist financing and terrorism. The law requires that at a minimum, the risk assessment at the national, sectoral, institutional and individual level be updated at least once a year for the high risk and for the low risk. Further, the updates will be documented indicating the dates at which the updates are made.

PART I
INTRODUCTION

1.1 The Rationale for the risk Assessment

The Terrorist Financing Risk Assessment is the commitment of URT to implement recommendation 1 of the Financial Action Task Force (FATF) and the Mutual Evaluation recommendations which was conducted in 2019/20. The FATF is an intergovernmental body set up by the G7 in 1989 that focuses on the global prevention and suppression of money laundering, terrorist financing, and other related threats to the integrity of the international financial system. Members of FATF including URT through the regional body ESAAMLG are bound by recommendations stipulating that financial institutions must take appropriate TF preventive and suppressive measures for improving national legal systems and international cooperation. In addition, the FATF monitors the correct functioning and effectiveness of these measures.

FATF Recommendation 1 requires members state to implement a risk-based approach for money laundering, terrorist financing and proliferation financing and to conduct national risk assessments. In 2016 URT conducted a National AML/CFT Risk Assessment. This was reviewed in 2019 by ESAAMLG during the Mutual Evaluation process and was found to have not sufficiently addressed the key issues in preventive and suppression of TF as did not adequately assess sectors such as NPOs, legal arrangements and the terrorist financing threat and vulnerabilities. It was recommended that the NRA be reviewed to address the deficiencies.

1.2 Terrorist Financing Definition

Terrorist financing is the financing of terrorist acts, terrorists, and terrorist organizations. This involves the generation and movement of funds for the sole purpose of committing terrorist acts or sustaining a terrorist network and organization.

Pursuant to section 3 of Anti Money Laundering Act (Cap.423) and section 2 of the Anti-Money Laundering and Proceed of Crime Act (No.10 of 2009) Terrorist Financing (TF) is-

(a) the provision of finance or economic resources or making available financial or related services to a terrorist, terrorist group, terrorist entity, terrorist cause,

a terrorist act, an individual, a group, or entity that is concerned with a terrorist, terrorist group, terrorist entity, terrorist cause, or a terrorist act;

(b) conducting a financial transaction or facilitating a financial transaction directly or indirectly, in order to deal with property that is owned or controlled by a terrorist, terrorist group, or terrorist entity;

(c) Conducting financial transactions or facilitating a financial transaction directly or indirectly, in order to deal with property on behalf of a terrorist, terrorist group, or terrorist entity;

(d) financing or facilitating the travel of any individual or a group of individuals to a country other than their country of residence or nationality in order to participate in a terrorist cause, terrorist training, or terrorist act, or in order to directly or indirectly conduct, perpetrate, plan or prepare terrorist acts;

(e) Organizing or directing others to commit any of these acts or participating in any of those acts as an accomplice, or an attempt to commit any of those acts.

1.3 Objectives

The objective of conducting the Risk Assessment on Terrorist Financing is:

(a) to identify the overall Threat and Vulnerability of the country to Terrorist financing;

(b) to Review the adequacy of measures in URT to Prevent Terrorism and Terrorist Financing;

(c) to prioritize actions that will improve the country's ability to combat Terrorist financing;

(d) to have a periodical review of the NRA to have an up to date of the Risks and vulnerabilities associated with terrorist financing and put in place appropriate measures to alleviate the Risks.

1.4 Participants

The exercise involved 50 participants from 38 Government and private sector institutions. Participants were selected from the institutions listed in **Appendix 1**.

1.5 Methodology

The TF Risk Assessment was carried out using expert opinion and World Bank's TF Assessment Methodology that was customized by FIU. The methodology tool defines

National TF Risk as a function of national TF threat and National TF vulnerability.

As part of the methodology, a third-party independent review based on long experience in countering Terrorism and TF, was sought and obtained by URT from UK's His Majesty's Treasury - Technical Assistance Unit. Their advice was instrumental in improving the risk Assessment Report and the ensuing TF Strategy.

PART II
OVERVIEW OF TERRORIST FINANCING METHODS, VULNERABILITIES AND SOURCES

2.1 BACKGROUND

As is experienced worldwide, the detection of funds and other forms of facilitation to support terrorists or terrorist acts in Tanzania is usually a complex undertaking since the size and nature of the transactions involved are not easy to detect because planning and committing terrorist acts or providing financial support does not require substantial amount of money. In most cases the planning is carried out clandestinely. Where financial institutions such as banks are used for TF, the transaction may normally involve small amount originated/raised from legal or illegal ways as illustrated in sub-section 2.2 and an uncomplicated layering of funds. A good example is the 1998 US embassy bombings in Dar es salaam and Nairobi which was estimated to have amounted to an overall cost of less than US $ 10,000.[1]

URT is mindful of TF threats and vulnerabilities and has taken these into account considering its geographical position in the region and the size and accessibility of its financial sector as well as the DNFBPs and informal financial sector.

The global and transnational nature and reach of financial institutions and DNFBPs, the greater role of intermediaries, and the uneven development, even divergence, of the world's economic systems magnify the challenges of combating terrorist financing as well as increase the opportunities for the terrorist financier.

Informal economic sectors account for many financial and business transactions in Tanzania and are far more economically active than the formal sectors. Also known as the 'parallel market', 'unrecorded trade', or the 'cash economy', these sectors provide for the livelihood of millions of Tanzanians, although their magnitude is undetermined. Direct interaction between the informal sector and formal financial institutions is insignificant. Tanzania has a vibrant informal economy. According to World Bank Index Report, 23.3% of the population in Tanzania use banks for

[1] Annette Hubschale. "Terrorist financing in Southern Africa" ISS Paper (Institute for Security Studies) 132 of January 2007

depository purposes.[2] Businesses and DNFBPs however will use formal financial systems.

2.2 SOURCES OF TERRORIST FINANCING

An examination of trends on sources of terrorist financing reveals that some terrorist organizations have legitimate business operations that generate profits that can be used as fronts for financing terrorist activities.[3] The proceeds from criminal activities such as bank robberies, kidnapping for ransom, extortion, smuggling, and drug trafficking are widely used to finance terrorism. This broad range of detailed sources of terrorist financing have been included in this Assessment in order to help members of the public in Tanzania to understand and be aware of various sources of terrorist financing identified globally as well as assisting devising suitable measures to entities that may be exposed to such risks.

2.2.1 The Illicit Drug Trade

The illicit drug trade has been identified as the largest source of terrorist income Afghanistan's poppy crops are responsible for as much as 86% of the word's opium supply and is widely believed to be a major contributor to terrorist coffers. The cocaine trade is also used to finance terrorist operations. [4]

Terrorist organizations may be related to drug trafficking either by direct involvement in illicit drugs trading or indirectly taxing the drug traffickers and farmers particularly in terrorists control areas where illicit drugs are grown. Terrorists will place a tariff on drug traffickers and thereby benefit by receiving cash to fund their organization. Under these circumstances, drug traffickers benefit from the terrorists' military skills, weapons supply, and access to other clandestine organizations and therefore gain freedom of movement and protection when they operate together with terrorists who control large amounts of territory.

The Fuerzas Armadas Revolucionarias de Colombia (FARC) a Columbian terrorist group aimed to overthrow the established order in Colombia and replace it with a

---

[2] The Global findex Database 2021 "https://www.worldbank.org/en/publication/globalfindex/Report"

[3] Annette Hubschale. "Terrorist financing in Southern Africa" ISS Paper (Institute for Security Studies) 132 of January 2007

[4] Kaplan, E. 2006. Tracking down terrorist financing. Council on Foreign Relations,4 April. [Online]. Available: http://www.cfr.org/ publication/10356/tracking down _terrorist_financing.html [6 December 2006]

socialist dictatorship, employed terrorist methods such as bombings, extortions, selective assassinations, kidnappings, and armed confrontations with Colombian police and military forces. In order to finance their political agenda, FARC used drug trafficking profits as their principal source of funding and protecting and exploiting drug trafficking operations in Colombia and the region. This is the world's major example of how terrorism and drug trafficking go hand in hand.[5]

The connection between drug trafficking and terrorist financing is also shown by Hezbollah a Lebanese Shia Islamist political party and militant group that was conceived in 1982 and was funded by Iran primarily to harass the Israel invasion of Lebanon. Its forces were trained and organized by Iran with permission from the Syrian government that occupied Lebanon's eastern highlands at the time. Hezbollah is reputed to have been among the first Islamic resistance groups in the Middle East to use the tactics of suicide bombing, assassination, and capturing foreign soldiers, as well as murders and hijackings. It is also described as a "state within a state" and has grown into an organization with seats in the Lebanese government, a radio and a satellite TV station, social services and large-scale military deployment of fighters beyond Lebanon's borders. Either the entire organization or only its military wing has been designated a terrorist organization by several countries, including the European Union, member states of the Arab League, with exception of Lebanon, and Iraq. Hezbollah ventured in global narcotics in 2012 and was estimated by the United Nations Office on Drugs and Crime (UNODC) to have an overall market value of USD 320 billion per year and was significantly expanding and institutionalized to the point where it was raising more money from narcotics than all its other funding streams combined. Hezbollah took advantage of the presence in the tri-border area (TBA) in South America and hundreds of clandestine airstrips and lax border security in Brazil, Paraguay, and Argentina to gained from drug trafficking and laundered the proceeds in Iran and Lebanon. Both Iran and Hezbollah smuggled drugs, laundered money and recruited sympathetic operatives and took advantage of a Tri-Border Area in Chile, Peru, and Bolivia that provided a greater opportunity to Iranian and Lebanon.[6]

---

[5] International Drug Trafficking and Terrorism ,https://archives.fbi.gov/archives/news/testimony/international-drug-trafficking-and-terrorism, Steven C. McCraw Assistant Director , FBIFederal Bureau of Investigation Before the Senate Judiciary Committee.Washington DC May 20, 2003

[6] Hezbollah - Wikipedia, https://en.wikipedia.org/wiki/Hezbollah.

Taliban used profits from the opium trade to buy weapons, food, and other necessary items to support their insurgency in Afghanistan.

An interesting aspect connecting the worlds of drugs and terrorism is the use of the cultivated or manufactured drug by the terrorists themselves as exemplified by US forces after Iraqi security forces reclaimed the city of Mosul in 2014, that there was evidence of amphetamine use among ISIS soldiers as track marks were found on ISIS soldiers indicating intravenous amphetamine use that allowed soldiers to stay alert during battle.[7]

Tanzania is located along major heroin trafficking routes from Southwest Asia. Tanzania's location, porous borders and corruption present challenges to drug interdictions. Between June 2019 to December 2021, Tanzania experienced a surge on drug trafficking, and illegal trafficking of precursor chemicals and UNODC and other international partners have been at the forefront working with Tanzania to combat the surge. A total of 1100kg of heroin and 452 kg of Methamphetamine were seized by DCEA through the illicit drug trafficking of Southern Route from South East Asia. Drugs are trafficked using dhows of Iranians and Pakistanis which are high TF risk jurisdictions. This present risk that proceeds from drug trade could be diverted to support terrorist and other criminal activities.

In view of the possibility of illicit drug trading to fund terrorism, Tanzania has been working closely with other world partners and is a key partner of an integral member of both eastern and southern African regional organizations in support of Tanzanian law enforcement to enhance drug interdiction capacity, improve maritime security, and enacting relevant laws and regulations to combat TF.

2.2.2 Donations from local and foreign supporters

Donations from local and foreign supporters including emigrants and charitable organizations, and cash infusions from wealthy individuals, philanthropists, donors direct funding, conditional funding, project administrative cost or organizations are

[7] The Link Between Terrorism and Drug Trafficking | S.J. Quinney College of Law (utah.edu) , https://www.law.utah.edu/the-link-between-terrorism-and-drug-trafficking/#_ftnref21,*Trajan Evans (2017)*

also source that have been used in various parts of the world to finance terrorism. Donations originating from charities, NGOs, and wealthy individuals have been identified as the largest source of terrorist financing.[8]

Charitable organizations have wittingly and unwittingly been involved in the financing and operation of terrorist grouping. Religious charities have come under increasing scrutiny and severe restriction since the 9/11 US terrorist attacks. Some charities, and charities with religious or ideological aims and beliefs have been identified to have been used to finance or support terrorist activity in various parts of the world.

The Al-Haramain branches in Kenya, Tanzania, Pakistan, Afghanistan, Albania, Bangladesh, Ethiopia, the Netherlands, and the Union of the Comoros are believed to have provided financial, material and/or technological support to the Al-Qaida network. The Al-Haramain organization network is believed to have received funding from Al-Haramain and used Al-Haramain as a front for fundraising and operational activities in Kenya and Tanzania that provided support, or acted for or on behalf of Arabian based Al-Haramain Islamic Foundation and Al-Qaida. [9]

Al-Haramain Foundation (Tanzania) was listed on 26 January 2004 pursuant to paragraphs 1 and 4 of Resolution 1455 (2003) as being associated with Al-Qaida, Usama bin Laden or the Taliban for "participating in the financing, planning, facilitating, preparing or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf or in support of" Al-Qaida and Al-Itihaad al-Islamiya.

The Al-Haramain Islamic Foundation, a Tanzanian entity was shut down in 2004 following receipt of intelligence information on terrorism involvement. Subsequently, the Law Enforcement in Tanzania conducted investigation to trace properties left by the entity, principal officers and affiliated individuals, whereas, the findings revealed that the entity had no ownership or controlling interest in any assets in Tanzania. All properties supported by the entity were in the names of local entities, which unwittingly received the support from the entity.

---

[8] Napoleoni, L. 2005. Terror incorporated: tracing the dollars behind the terror networks. New York: Seven Stories Press

[9] Resolution No 2170/2014 Security Council of the United Nations addressing the acute and growing threat posed by foreign terrorist fighters - dated 24 September 2014

The Government of URT continues to monitor the civil society space to ensure that it is not used for TF purposes and the Government has taken measures to include community-based awareness campaign, putting in place the laws putting in place GN 609 of 2018 and GN 687 of 2019 that empower registrars of NPOs to monitor the funding sources of the NPOs and the use of Assistant Registrars under local government authorities to identify and report suspicious transactions and conduct awareness campaigns to targeted NPOs.

Other measure by the Government includes developing a National NGOs Sustainability Strategy 2022/23- 26/27 with the main objective of enhancing domestic funding for long term sustainability of the NGOs in Tanzania. The strategy has provided enhanced and diversified financing models of NGOs to meet their funding needs by 2026/27 through increasing diversification of fund in the local content.

2.2.3 Exploitation, Trade, and Trafficking of Natural Resources

The exploitation, trade, and trafficking of natural resources including precious metals and minerals such as gold, silver, copper and diamonds, as well as timber, charcoal, and wildlife, present a significant source of profit for criminals and are sometimes used as opportunities to finance terrorist activities and groups, particularly in high-risk locations and jurisdictions.

Terrorist engagement in legitimate businesses related to natural resources is important for these groups, both to generate regular income and to further diversify the sources of funding. In July 2021, FATF noted in its report on money laundering threats and environmental crime that "there is evidence that armed groups and terrorist organizations do, to varying extents, rely on certain environmental crimes to support and finance their operations[10]. FATF also noted that environmental crime, particularly mining, is a profitable tool for insurgent groups in conflict with the central government authorities and for terrorist organizations operating in resource-rich jurisdictions where there is instability. It should be noted that terrorist groups will engage in environmental crime as a means of raising revenue or as a direct

[10] https://www.fatf-gafi.org/media/fatf/documents/reports/Money-Laundering-from-Environmental-Crime.pdf , p. 8. F

means of value transfer/payment for goods (e.g., guns and drugs).

An assessment on the scale and scope of the linkage between the exploitation of natural resources and terrorism financing across the various types of illicit flows has not so far been made in Tanzania and the TF Strategy include this research as part of the activity to be carried out.

It is clear from experiences and typology studies conducted by FATF and FSRBs that terrorist groups are able to strategically diversify their funding streams into a variety of both illicit and licit activities relating to, inter alia, oil and natural gas, resources used for agriculture and fishing, wildlife, or minerals and precious metals. Recommended actions in Part III seek to mitigate threats and risks in this area, focusing on Real Estate Agents, Dealers in Precious Stones and Metals, financial service providers, border controls and other DNFBPs.

In the Syrian Arab Republic and Iraq, ISIL was able to generate considerable income from the production of, and trade in oil and natural gas in areas that it controlled predominantly in 2014 and 2015. As proof of this in May 2022, the Paris Court of Appeal confirmed the indictment of a French multinational company for complicity in crimes against humanity committed by ISIL after it had previously confirmed the charges of financing a terrorist organization for making payments and trading raw materials, including oil, to ISIL and other local armed groups. Despite ISIL's loss of control over territories in this region and the consequent drastic reduction in its access to oil and natural gas fields, FATF has noted funds being generated through extortion of oil networks in eastern Syrian Arab Republic as late as 2021 and that Cash reserves accumulated through the earlier exploitation and trade may still be available to the terrorist group[11].

According to the Twenty-ninth report of the Analytical Support and Sanctions Monitoring Team pursuant to Resolutions 1526 (2004) and 2253 (2015), Al-Qaida in the Arabian Peninsula (AQAP) continues to attempt to establish control over ports along the Gulf of Aden, and oil and gas infrastructure facilities. There are no cases in Tanzania that are linked to terrorist groups attempt to establish control over ports

[11] Lafarge pleaded guilty to TF in New York .ttps://www.justice.gov/opa/video/lafarge-pleads-guilty-conspiring-provide-material-support-foreign-terrorist-organizations

in Tanzania. The Government will continue to monitor ports and harbors in Tanzania to ensure they are not used for TF.

In 2021 report to the President of the Security Council, the members of the Panel of Experts on Yemen noted that the Houthi terrorist group were closer to taking control over important oil and gas wells.

In the Lake Chad Basin region, where the economy is largely based on agriculture and fishing, further examples of the linkages include cattle rustling and livestock raids which have represented a source of financing for Boko Haram.[12] Recurring cases of livestock theft by Boko Haram and increased risks of illegal trafficking of fish products in the Lake Chad Basin is linked to the active terrorism in the Lake Chad Basin region. Boko Haram has been reported to profit from trade in smoked fish and red pepper or to extort communities involved in farming and fishing activities[13.]

There is also growing evidence that the Islamic State West Africa Province (ISWAP) has been able to impose taxation and extorsion of businesses relating to fisheries.[14] There are no cases in Tanzania that are linked to terrorist groups generating funds through imposition of taxation and extorsion of businesses relating to fisheries.

In its 2021 report to the Chair of the Security Council (S/2021/849), the United Nations Panel of Experts on Somalia noted that Al-Shabaab was generating funds through a range of illicit taxation on agriculture, farms and farming produce and livestock (cattle, camels and goats).

Revenue from timber, cocoa and coffee has also been linked to terrorism financing in the Democratic Republic of the Congo where some cultivation, harvest, sale and smuggling of cocoa is linked to the Allied Democratic Forces (ADF).[15] The ADF, is

[12] Petrich, Katherine "Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa" (2022), The Linkages between Organized Crime and Terrorism, Studies in Conflict & Terrorism.
[13] Samuel, Malik "Economics of terrorism in Lake Chad Basin" (2019), Institute for Security Studies.
[14] Tabi Mbang, Etienne, "Raising funds for terrorist purposes through exploitation of natural resources" (2021), Joint special meeting of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da'esh) and Al-Qaida Sanctions Committee on the latest terrorismfinancing trends and threats, as well as the implementation of Security Council resolution 2462 (2019).
[15] 2020, the United Nations Group of Experts on the Democratic Republic of the Congo, Midterm report of the Group of Experts on the Democratic Republic of the Congo, (S/2020/1283), see Summary.

affiliated to ISIL and has been reportedly generating profit from taxation on illegal timber production in Eringeti. ADF is also reported to force Congolese farmers to pay monthly taxes of $10 to $25 per acre per farmer, or part of their harvest.

Indonesian authorities reported in 2012 that Jemaah Islamiyah, which carried out the 2002 Bali bombings and other terrorist attacks in the country, was involved in establishing palm oil plantations and other enterprises as funding sources for its operations.

There are no cases in Tanzania that are linked to terrorist groups generating funds through a range of illicit taxation on agriculture, farms and farming produce and livestock, and also exploiting revenues from major cash crops such as coffee, cashew nuts or any other agricultural crops.
In Iraq and the Syrian Arab Republic, for example, ISIL has exploited water shortages and taken control of water infrastructure to impose its will on communities. Cases showing terrorist exploitation of water shortages or taking control of water infrastructure in Tanzania is nonexistent.

Access to coastal facilities, can also be strategic for terrorist groups seeking opportunities to take control of maritime assets. Evidence linking restrictions to access to coastal facilities in Tanzania to financing terrorists is nonexistent.

Illegal wildlife smuggling/trafficking is among the most lucrative criminal activity worldwide and has been reported as a source of funding for terrorist organizations such as Boko Haram, Al-Shabaab, the Lord's Resistance Army.[16] Evidence linking illegal wildlife trade in Tanzania to financing terrorist is nonexistent.

During the Twenty-ninth report of the Analytical Support and Sanctions Monitoring Team pursuant to Resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), the mining of gold and other precious metals was reported as an important source of terrorism financing for global affiliates of ISIL and Al-Qaida in Africa. It was also noted that rare earth metals were also being excavated to support regional

[16] https://www.usip.org/events/wildlife-poaching-and-trafficking combating-source-terrorist-funding; National Geographic, "How Killing Elephants Finances Terror in Africa" (2015): https://www.nationalgeographic.com/tracking-ivory/article.html.

terrorist groups and that there are linkages between gold mining and terrorism financing including Al Qaida using rough diamonds from West Africa to finance its activities since the 1990s. Research has also established that gold is more attractive to terrorist groups owing to its stable value and relative portability, combined with inherent industry vulnerabilities relating to the cash-intensive nature of the gold trade and limited AML/CFT oversight.

In Colombia and Peru, it has been established by the relevant FSRB that terrorist groups were able to take control of territories where gold mines were located by extorting and coercing the owners to transfer the ownership titles of the land. Part of the gold produced illegally by the terrorist group was sold to legal businesses through cash transactions with a view to concealing its origin. The profits were then used to buy equipment, munitions, medicines, and other supplies needed to continue with the group's terrorist activities.[17]

ISIL affiliates with an established presence in Africa is reported to have exploited the gold mining business not only by extorting gold miners working in unregistered mines but also by engaging smugglers to move the gold from remote mining sites to trade points, and even using existing smuggling routes to sell gold at international trading hubs[18] such as the case in Burkina Faso, Mali, and Niger, which were considered by the terrorist as easily accessible, and gold is available at the lowest risks of detection and disruption.

The Islamic State in the Greater Sahara (ISGS) and Jama'at Nusrat al Islam wal Muslimeen (JNIM) are reportedly fighting in the Gourma sector of Mali, in part for control of gold extraction areas where the groups impose illegal taxation on small-scale gold miners for protection or to collect a form of wealth tax for observant Muslims.

In the Democratic Republic of the Congo, there have been reports that the ADF has been involved in the illegal exploitation of gold mines such that it accelerated its expansion into the gold rich Irumu territory of Ituri Province, and benefitted from

[17] Peru (2017). "Sectorial Assessment of the ML/TF risks of the Mining sector"
[18] Lackey, Chania, "Remarks" (2022) Joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da'esh) and Al-Qaida Sanctions Committee on "ISIL in Africa: Nature of Threat and Responses".

exporting other minerals such as wolframite, coltan and cassiterite.[19]

In late 2020 in the Sahel, it was noted that a terrorism financing trend was prevalent following the seizure of more than 40,000 sticks of dynamite and detonator cords, which were believed to be intended for illegal gold mining for armed terrorist groups in the Sahel.

In Mozambique, Cabo Delgado Islamic State Central Africa Province (ISCAP) which is associated to ISIL is considered as growing risk for illicit activities in the area, including the trade in gold and other precious metals or stones despite lack of direct cases linking precious stone mining and terrorism financing.

Cases of the production, taxation and extorsion of charcoal represent a further instance of the use of natural resources as revenue by terrorist organizations, particularly Al Shabaab in Somalia. The existence of the TF through charcoal in Tanzania is not known and there is no evidence of its existence. It is established by various researches that other terrorist and armed groups in Africa including in Central African Republic, Democratic Republic of the Congo, Mali, and Sudan have generated revenue from the illegal or unregulated charcoal trade. [20]

The investigation of crimes associated with the natural resources sector, including TF-related investigations, are often complex and requires extensive financial analysis. It is often difficult to identify the entire criminal network and specific actors (including facilitators) who are committing these crimes. This leads to challenges in the prosecution of these crimes.

Some countries bordering URT suffer from terrorist activity. Accordingly, there is a threat of TF to the formal and informal financial sector, as well as the threat of TF by the movement of and related proceeds/instrumentalities across land borders. The National TF Strategy seeks to address this area of threat to alleviate the level of this risk.

[19] Daghar, Mohamed; Chelin Richard; Haji Mohamed, "Expansion of the Allied Democratic Forces should worry East Africa" (2022), Institute for Security Studies.
[20] RHIPTO, INTERPOL, and Global Initiative Against Transnational Organized Crime, "World Atlas of Illicit Flows" (2018).

It is important for the government to remain vigilant to all the operators in the natural resources sectors, both legal and illegal, to always ensure that stern measures are taken against the illegal operators. Additionally, targeting smugglers and smuggling networks, which often extend beyond the source country of the natural resources in addition to the area in the immediate control of TF group, assist in combating the available method of raising funds. It is also necessary for the government to ensure the public and private sectors collaborate including actors outside of the traditional scope of the CFT regime.

The measures taken by the Government of URT include strengthening of the legislative and regulatory frameworks within natural resource sectors including enacting Natural Wealth and Resources Permanent Sovereignty Act (Cap 449 of the Laws of Tanzania which is implemented through the established Natural Wealth and resources Observatory Unit under the Ministry of Constitutional and legal Affairs. This Unit is mandated to ensure national wealth is preserved for sustainable utilization for economic development. These means that the exploitation of natural resources for TF purposes is unacceptable and is a crime.

Last but not least, the Government takes cognizance that adequately tackle TF from natural resources, the public and private sectors need to be aware of the threats and vulnerabilities of this sector as well as the link of the sector to TF, corruption and organized crime. In this regard awareness campaigns are given priority in the National TF Strategy.

2.2.4 Assistance from Foreign Sympathetic States

Research has proved that a number of countries in the developing world have provided support to terrorist organizations for political and military reasons. When terrorist organizations have the full range of state-controlled financial services at their disposal, large sums of money can be integrated into the international financial system whether the state or some other legal or illicit source is the funding agency.[21] Analysis of information obtained from the participants of this risk assessment suggests there is no evidence that links Tanzania with this type of terrorist financing

[21] Navias, M.S. 2002. Finance warfare as a response to international terrorism. The Political Quarterly, 73(s1):57–79

activity.

2.2.5 Revenues from Legitimate Business Operations

Some terrorist organizations operate legitimate business operations which generate their own profits and can also be used as a front for financing terrorism. Ties to terrorism have been identified in the livestock, fish, and leather trades, as well as industrial operations.

Cash intensive businesses and the use of retail and service businesses such as restaurants, pubs and convenience stores have long been used by criminals to facilitate the laundering of illicit cash. These legitimate businesses are sometimes referred to as "front companies" if they are set up to provide plausible cover for illegal activities. With respect to TF, the proceeds from a legitimate cash-intensive business can be used as a source of funds to support terrorist activities. A wide range of types of businesses have been noted including those in the construction industry, used motor vehicles traders, travel agencies, gold and jewelry trade, currency exchange offices, clothing stores, butchers, sandwich bars and other businesses. These businesses can direct funds to terrorist organizations/activities if the relation between sales reported and actual sales are found to be hard to verify. [22]

There have been a number of cases identified by FATF and FSRBs typology studies of terrorists buying out or controlling cash-intensive businesses including, in some cases, money services businesses to move funds. Casinos are by their nature considered cash-intensive businesses, as the majority of transactions are cash-based. In March 2009, the FATF published a report on ML vulnerabilities in the casino and gaming sector. The report showed that there was significant global casino activity which is cash-intensive, competitive in its growth and vulnerable to criminal exploitation.

There are a number of specific harms resulting from the use of legal businesses by criminals and terrorists including competitive advantage being given to complicit businesses and placement of criminal cash that allows a profit from crime to be

[22] FATF Report, Global Money Laundering & Terrorist Financing Threat Assessment, July 2010

laundered and be realized. Through the use of businesses, criminals may corrupt, wittingly or through coercion, others employed in these businesses.

Criminals and terrorists try to achieve a number of objectives through the use of legal businesses. Mainly, they want to conceal the source of illicit funds by mingling them with legitimate funds or they want to provide value for money by creating economies of scale (i.e. legal businesses are an easier way to get large amounts laundered than through personal accounts). Ownership of legal business permits the acquisition of community standing and influence, which provides additional cover for illicit activities. In addition, proceeds of legitimate business can easily be used as a source of funds to support terrorism.

In Tanzania any person can establish a company as long as they are able to meet the requirements under the Companies Act and pay the necessary registration fees and other charges. Since 2020 it is a legal requirement that the legal persons and other legal arrangements registries register Beneficial Ownership which supports mitigation to the identification of persons or entities under the TFS.

Further, the awareness of the processes of licensing for business and scrutiny of legitimate businesses by the authorities is minimal. It is also difficult to monitor the accounts held by businesses.

A good example of TF through legitimate business is exemplified in the Lafarge case in which between 2013 and 2014 a French cement maker Lafarge made payment through intermediaries, to groups designated as terrorists by the United States, including Islamic State, so the company could keep operating in Syria. The facts of this case were that Lafarge S.A. ("**Lafarge**"), incorporated and based in France, was the parent of a Syrian company (the "**Subsidiary**") which operated a cement plant in Syria, in close proximity to the border with Turkey, between 2011 and 2015. At this time, Syria was in a state of civil war, which had precipitated the rise of jihadist groups including the Al-Nusra Front and the Islamic State of Iraq and the Levant ("**ISIL**" or "**ISIS**"). At the time the Al-Nusra Front and ISIS controlled

large parts of the region, and by 2014 both organizations were designated as Foreign Terrorist Organizations under United States Law. [23]

The difficulties of operating in Syria during the conflict led to many multi-national organizations ending their operations in the region. The Subsidiary, however, decided to remain, and entered into an arrangement with ISIS and other terrorist groups which resulted to the Lafarge paying large amounts of money in return for the safety of its property and employees. This arrangement evolved over time into one of revenue sharing, allowing ISIS to receive money from Lafarge that was proportionate to the amount of cement sold. In essence, ISIS was receiving "taxes" from Lafarge. This was done with the knowledge and approval of senior executives of Lafarge, including its Executive Vice President of Operations and a member of its Security Committee (a citizen of the United States), who were party to the arrangement. A Lafarge in-house lawyer, the Regional Senior Counsel for Africa and Middle East, were also aware of this arrangement. All of these individuals were based in Paris, but several senior executives of the Subsidiary were also involved.

The arrangement was made despite the knowledge that it contravened US and EU laws against the funding and support of terrorist organizations. With this knowledge, the executives involved went to great lengths to conceal the arrangement and anything linking it to Lafarge. The senior company employees concerned in the deal did not use their company email addresses, instead resorting to the use of personal internet-based email accounts. In return for the payments, ISIS issued the drivers of Lafarge trucks with permits providing them with safe passage through ISIS-controlled areas, and Lafarge was at pains to ensure that these permits did not mention the company by name. At one point, it had to specifically raise this issue with ISIS when permits were issued which identified the company. Lafarge also designed a system of invoices that was designed to hide from its external auditors the nature of the payments to the intermediaries.

Lafarge faced competition in the region from another company which imported cement into Syria from Turkey. Not content with securing the safety of its employees and property, Lafarge sought to obtain a competitive advantage through its

[23] https://www.whitecase.com/insight-alert/corporate-liability-terrorist-financing Corporate Liability for Terrorist Financing 07 November 2022 Jonah Anderson | and Daniel Levin

arrangement with ISIS and similar organizations. In return for the sums paid to the terrorist groups, Lafarge encouraged them to hinder the importation of cement from Turkey by extracting from the other supplier sums larger than those voluntarily paid by Lafarge.

It is estimated that from August 2013 to October 2014, Lafarge paid approximately USD 5.92 million to ISIS. At around this time, the United Nations Security Council had issued a resolution condemning ISIS and other such organizations.

In a further measure to distance itself from the arrangement, Lafarge required its key intermediary in the deal to sign a back-dated agreement which purported to terminate his services prior to this period. At the same time, Lafarge encouraged this intermediary to set up a new account. It then wired USD 210,000 from its Paris bank, via a New York-based financial institution, to the intermediary's new bank account.

Around 2015, a competitor of Lafarge entered into negotiations to buy the latter. The purchaser did not make any due diligence enquiries into Lafarge's Syrian activities, which had by now ceased. At a meeting to discuss with Lafarge any ongoing public litigation or antitrust issues, the purchaser did ask if there was anything it should know about. Lafarge did not disclose its activities in Syria. It should be noted that at a time when other businesses had been forced to terminate their operations in the region, the subsidiary had enjoyed sales revenues of USD 70 million. All in all, the cover-up could only last long as subsequent to the successful purchase of Lafarge, an article linking Lafarge to payments to ISIS appeared on the internet and the new owners of the company engaged lawyers to conduct an investigation. The results led to the investigation and subsequent prosecution of Lafarge and the Subsidiary by the US Department of Justice. Upon entering guilty pleas, Lafarge and the Subsidiary were ordered to pay a criminal penalty of USD 90.78 million and forfeiture of USD 687 million. Lafarge was also required to report annually to the US Department of Justice on remediation efforts and the implementation of agreed compliance measures at the company.

This case is reported in detail to assist the reader in fully understanding the mechanisms of a current and relevant terrorist financing offence.

2.3 EMERGING TERRORIST FINANCING RISKS

In accordance with the FATF report of the *Emerging Terrorist Financing* of October, 2015, this TF risk assessments takes cognizance of the fact that foreign terrorist fighters (FTFs), social media, new payment products and services, and the exploitation of natural resources are trends to be considered for an in-depth TF risk Assessment. The aim of this section is to provide a broad overview of the situation in URT regarding the emerging issues on TF and identify whether there is an information in that regard to better understand the country TF risks.

2.3.1 Foreign Terrorist Fighters (FTFs)

FTFs require financing to enable their activities as they aim to join and form part of terrorist groups in other jurisdictions. Self-funding by individuals and funding by recruitment/facilitation networks are the two common methods used to raise funds for FTFs. The funding needs of FTFs are generally modest and include transportation, accommodation while in route, outdoor clothing, camping goods, mobile phone/plans, food and other general living expenses.

FTFs incur expenses prior to commission of terrorist act or participating to a war zone. Their expenses include the purchase of weapons.

In Saudi Arabia, authorities undertook an analysis of the account information of 1,150 individuals who travelled to the Syrian/Iraq conflict zone and found that three out of four of these individuals were between the ages of 20 and 30 and their sources of income included payments from friends and relatives, loans, salary and government social support payments. For the most part there was normal account activity in comparison to the level of their income. This proves that FTF do not involve large amounts of funds to participate in acts of Terrorism.

In some cases, it has been revealed that small businesses were intentionally established and used to generate revenue that supported FTF travel.

In another case, a sudden sale of assets including personal belongings and assets purchased on credit just prior to the FTFs planned travel have been observed. In this

respect, there are similarities between FTFs and small terrorist cells as some extremists who have plotted attacks in Western Europe most commonly relied on funding from the cell members' own salaries and savings. The vast majority of the cells studied (90%) were involved in income-generating activities, and half of them were entirely self-financed. Only one in four received economic support from international terrorist organizations.

Cases have been reported about FTFs continuing to receive social security or other government paid benefits from their home countries after travelling to a conflict zone. This practice is attributed to varying circumstances in different jurisdictions, including relevant authorities being unaware of the involved person's status or unable to process such information timely.

In 2015, Rashid Charles Mberesero, a Tanzanian was arraigned for participation in Kenya's Garissa University College attack, which caused the death of at least 148 people, most of them being students and close to 100 were injured. Rashid Charles Mberesero was found guilty of conspiracy to commit a terrorist attack and belonging to al-Shabab, which is linked to al-Qaeda. He died in prison in 2020. Mberesero and his two accomplices, Mohamed Abdi Abikar and Hassan Aden Hassan were found by investigations to have contact with the attackers and that his call data revealed that the suspect was in constant communication with contacts in Somalia suspected Al-Shabaab operatives. The phone records and handwritings linked him to the attack. The incident ranks amongst the deadliest attacks in East Africa.[24]

Although FTFs have in some incidences been found to bring additional funds with them when joining terrorist groups, in most cases they are more valuable as human resources than as fund providers. There are claims that some terrorist groups provide for FTFs and family members once they reach the conflict zone.

2.3.2 Vishing fraud Courier and vishing frauds

This is a type of telephone scam that has been identified as a TF method. The funds were used to finance travel to Syria and Iraq and also to sustain individuals who have

[24] https://www.thecitizen.co.tz/tanzania/news/international/-tanzanian-convicted-for-garissa-terror-attack-dies-in-kenyan-prison-3213998

travelled to these areas to fight with ISIL. UK based extremists adopted the organized crime group tactic of targeting vulnerable individuals with phones calls purporting to be either police or banking officials. They were informed that their account(s) have been compromised in some way and are persuaded to either transfer money into accounts controlled by the suspects or to physically withdraw the cash. A courier from the criminal network is then dispatched to the victims' home address and picks up the cash. London-based networks were known to have targeted individuals through this method which it is not clear how the victims were selected. Normally it is as simple as online telephone directories. Such networks defrauded victims out of hundreds of thousands of pounds and some money was transferred overseas using Money Service Businesses (MSBs) to the Middle East by suspects, although the final destination of these funds was not established in most cases. The amounts sent were in the low thousands for each transaction or below the GBP 500 limit so suspects did not have to provide further identification. Evidence linking vishing fraud in Tanzania to Financing terrorist is nonexistent.

2.3.3 Material support involving returning FTF

In one case the flat of a Syrian national was searched for suspected preparation of a serious act of violence endangering state security. During the search, police seized computers, several data carriers as well as mobile phones. On this occasion, the individual who was the subject of the investigation received an order prohibiting him to leave the country because it was considered probable that he would participate in combat activities in Syria. Information obtained indicated that he had left Germany for Syria via Turkey and had handed over EUR 9,500 of donated funds there. Subsequently, he joined the extremists and participated in combat activities and returned to Germany following a gunshot injury.[25]

Information about the funding sources for returning FTFs is limited. It has been generally observed that some of the funding techniques to travel to the conflict zone have also been used when FTF return to their home country including fund transfers via MVTS to countries adjacent to conflict zones and returning FTFs requesting their respective embassies assistance to travel back to their home country due to a lack of documentation.[26]

[25] FATF Report "Emerging Terrorist Financing Risk, October 2015
[26] FATF Report "Emerging Terrorist Financing Risk, October 2015

2.3.4 Recruitment/Facilitation Networks

Recruitment networks and individuals facilitate FTFs to travel to conflict zones and join terrorist groups. Family, friends or facilitation networks also provide financial support to FTFs once they depart for the conflict zone. It appears that most TF groups are informal or ad hoc, depending on what assistance is required by the FTF and there are often links between facilitators in the home country and areas bordering the conflict zone. There also appear to be links between facilitation networks and criminal organizations (some facilitation networks are not based on ideology but on profitability). Many facilitation networks will have specific recruiters (who often exploit social media applications) who sometimes include members or sympathizers of extremist groups or individuals who are loosely affiliated with extremist groups.

Some networks include random individuals who send money to each other, thus forming common counter-parties and becoming a de facto facilitation network.

FTFs also get logistical support from these facilitation networks, including arranging transportation and purchasing supplies. Funding for individuals intending to participate in conflicts may also occur through family networks, particularly through funds sent to countries neighboring conflict zones. It is often difficult to determine the real end use of the transfers, particularly within family groups, as the majority of funding from source countries to countries near conflict zones is likely to be for legitimate family support or humanitarian reasons.

Using networks of contacts, returnees are likewise involved in facilitating aspiring FTFs transit to conflict areas and in raising money to assist in financing the travel or to support fighting groups. There are incidences involving family members paying facilitation networks to returning FTFs.

One example of the use of network contacts is one European network occurring between 2006 and 2013 with facilitators of four individuals that carried out 28 funds remittances through seven different entities located in Germany and France. These transactions had 17 different beneficiaries who withdrew the funds in 16 distinct business entities, located in Egypt, Germany, Greece, Morocco, Portugal and Tunisia. The beneficiary in Portugal withdrew the funds in January 2009, in three different entities. He did not have any income or property in Portugal. In 2014, the

beneficiary in Portugal allegedly travelled to Syria, via Turkey, suspected of joining ISIL. He was later arrested when returning to Europe.

In another incidence, the police in Turkey were informed that families of FTFs attempted to buy the freedom of their children who had earlier travelled illegally to Syria through facilitators' networks. There had been a number of FTFs, in particular young adults with single women or women with children, who were assisted by the families or other individuals to exit from ISIL and were deported from Turkey to their source countries.

FTFs have used some of the traditional methods and techniques to move and get access to funds. These primarily include the physical movement of cash, use of ATMs to access funds from bank accounts and use of MVTS. One such cased that has been reported as a typology in the studies by FSRBs is the use of MVTS from Middle-Eastern countries to finance fighters to join ISIL. This case involved young Spanish recruits joining to fight with ISIL as FTFs. It was difficult for young Spanish recruits in Ceuta and Melilla to purchase plane tickets due to the high long-term unemployment rate in their districts and therefore, from an analysis conducted on 249 transfers that took place from 1 January 2014 to 31 May 2015 via three MVTS totaling EUR 117,000 sent from Syria, Iraq, Turkey and Lebanon to Ceuta and Melilla, was found or considered suspicious because of a lack of information regarding their purpose, and there were no apparent relationship between senders and receivers. In addition, some of the receivers were associated with previously filed suspicious transaction reports associated with TF.[27]

2.3.5 Fundraising Through social media

The widespread access to and anonymity of the Internet and especially the rapid expansion of social media, have been exploited by terrorist groups to raise funds from sympathetic individuals globally and represents a growing TF vulnerability. Social networks are widely used by terrorist organizations to spread their terrorist propaganda and reach out globally to sympathizers. [24]

Many FTFs are actively using social media to document their experience in the

[27] FATF Report "Emerging Terrorist Financing Risk, October 2015

conflict zone in real time. Rather than relying on official accounts provided by terrorist groups, most of these FTFs look to and receive information about the conflict from so-called disseminators. These disseminators are officially unaffiliated with a terrorist organization but are sympathetic to the ideology and significantly invested in the conflict. This has reduced the ability of terrorist groups to control information, giving private individuals greater influence over how the conflict is perceived by those involved in it.[28]

Social networks are being also used to coordinate fundraising campaigns/ schemes aimed at several thousand 'sponsors' and may raise significant amounts of cash. Some terrorist organizations have been able to conduct outreach to a large audience through a peer-to-peer horizontal communication, that starts on chats and forums, goes on through social networks (such as Facebook, Twitter and Instagram) and sometimes keeps on going through mobile application for communication (such as WhatsApp and Viber) or more secure communications networks. In addition to targeting would-be FTFs on social media networks, donors are also a priority target group. Explicit calls for funds on social networks in a Facebook for example in reported cases in the typology study involved a group on recipes for women where one of the users placed a call for funds. A call was made for a fighter in Syria who urgently needed "equipment, food and pharmaceuticals". There was time to collect funds in order to "dispatch" the requested material. The user also provided the details of an account held with a specific bank where the funds were to be sent. It was not known if the author of the Facebook call for funds was also the person responsible for this initiative. The owner of the account was a convert, who was suspected of coordinating this advertising campaign.

The use of organized crowdfunding techniques also represents an emerging TF risk. Crowdfunding is an internet-enabled way for businesses, organizations, or individuals to raise money, from donations or investments, from multiple individuals. Crowdfunding websites allow people to easily set up a fundraising page and collect donations. Yet, crowdfunding is vulnerable to exploitation for illicit purposes, including instances where the true purpose of the funding campaign is

[28] Carter, J.A., Maher, S. and Neumann, P.R. (2014), #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks, International Centre for the Study of Radicalisation and Political Violence (ICSR), London, United Kingdom"

masked. Individuals and organizations seeking to fundraise for terrorism and extremism support may claim to be engaging in legitimate charitable or humanitarian activities and may establish NPOs for these purposes. Several cases indicate that the end-use of funds collected through crowdfunding and social networks was not known to donors.

Crowdfunding techniques can also be used to transfer funds abroad by avoiding regulated financial entities. In case an individual under investigation for terrorism-related offences, including attempts to leave the country for terrorist purposes, used crowdfunding websites prior to leaving and/or attempting to leave his country of birth.

In another case, a reporting entity received information from law enforcement that an individual left a country, which prompted his account review that indicated details with regard to a crowdfunding website showing the account was used for four transactions with a known crowdfunding website. This person was categorized by its bank as "Professional Services". The company's website described itself as an international crowdfunding site, allowing people to easily set up a fundraising webpage and collect donations. Most of the donation options were related to conflict relief to terrorist dominated countries.

Legitimate charities have set up viral campaigns on social networks to gain followers, and encourage donations. This approach is also being used by bogus NPOs. Funds can be raised overtly or under the guise of humanitarian aid. Funds can be raised via social media, or via more formal crowdfunding platforms. Collected funds will pay for material support for FTFs (payment for mobile communication, air tickets, as well as different goods and services ordered via the Internet), or serve as operational funds to undertake a terrorist attack. The Government in URT is working on putting measures to control fundraising activities where the NPOs legislation have provisions that entitle NPOs to engage only into legally accepted fundraising activities.

Fundraising advertisements are usually placed in social networks and thematic websites, as well as in specialized media, closed online forums and sent in private messages. In order to conceal the real purposes of fundraising and avoid blocking,

such advertisements often do not contain direct references to fundraising for TF but use ambiguous language or the pretext of collecting funds for charitable and humanitarian purposes. Fundraising advertisements and financial details may be placed in different formats rather than in a text (for example, as an image or video), which makes it impossible to detect them through the standard search engines and makes it difficult to identify sites that contain these advertisements, as well as to explore advertisements using known financial details. The majority of social networks used by terrorists inadvertently provide terrorist groups and their adherents a platform for TF. The companies providing these social networks themselves are not participants of such criminal activities, and in many cases cooperate with the competent authorities on providing information, and the closing or blocking of such accounts.

In order to attract more people, the organizers of online fundraising campaigns may use multiple payment systems and instruments to receive funds, which are popular among different groups of potential 'sponsors. Fundraising campaigns may use social networks as a medium for facilitating financial transfers, facilitating the exchange of credit card numbers, prepaid card details and account ID information.

The most venerable payment systems that are subject to TF abuse are those which suggest a high level of confidentiality and an opportunity for distant account management. Members of terrorist networks may get access to the regulated financial system by registering payment instruments in the name of third parties. They frequently use online payment systems due to this straightforward registration process and the relatively high level of anonymity. To avoid detection, the organizers and facilitators of the scheme ensure 'rotation' of payment requisites (e-wallets, credit cards, mobile phone numbers, etc.), posting the relevant changes in information on the Internet. New payment methods such as e-wallets are used in such a scheme.

Example, a group of individuals led by Mr. A (Group A) organized a scheme to raise funds via social networks and the internet. This group registered numerous e-wallets, credit cards and mobile phone numbers. The financial requisites were placed on the internet/ social networks under the pretext of collecting donations for Syrian refugees, people in need of medical and financial aid, and for the construction of

mosques, schools and kindergartens. The wording contained some indirect indications that the money was intended as financial support for terrorist activities. Indeed, the funds were sent as an aid for terrorists and their families and to support terrorist activities. The money was sent either to credit card accounts or to e-wallets. Collected funds were moved through a chain of transfers and were withdrawn in cash to be further transported by couriers. The payment instruments were managed via the internet (using mobile devices as well).

Some cases show that the money is being moved in several stages: collected funds are moved through a chain of electronic transfers and then withdrawn in cash to be further transported by couriers. In some cases, the cash is being re-deposited in other accounts. Those schemes aim to break the operational chain and conceal the source of the funds and the final beneficiaries.

Funds are also shuttled through multiple jurisdictions or sent through conduit neighboring countries to reduce suspicion. Crowdfunding platforms and payment processors can provide valuable information to an investigation when misconduct is suspected. In most cases, responses to legal processes have included personal identification information, transaction details, IP addresses, and account information.

In one jurisdiction, a charity was prosecuted for terrorist financing. That charity was created to raise funds for humanitarian projects in Palestinian territories and Syria. After a donation campaign, the charity sent two ambulances to Syria with medical material to build a hospital. Pictures were posted on Facebook to attest to the reality of the project and communicated to the donors. A month later, the charity made a new call for funds on social networks, indicating that three members of the association planned to enter with funds into the jurisdiction. A customs control in another country's airport revealed that each of them carried EUR 9,900, below the declaration threshold, but only EUR 6,000 were to be used for the humanitarian project. The remaining funds were to be given to FTFs. An administrative order froze the assets of the charity and four of its members. The association was dissolved, and two members were arrested for TF and criminal conspiracy in connection with a terrorist enterprise. Law enforcement authorities used Facebook

public messages and pictures as evidence. [29]

The challenges associated with the use of the social media to raise funds is that often, it is not possible to distinguish between the sympathizers, supporters and actual terrorists. The identification of persons contributing money, either intentionally or unwittingly, is another serious challenge to competent authorities. It is often difficult to get evidence of the use of funds when transferred via the internet. [30]

Social networks are used to show the relationships but finding proof of TF is still difficult. Consideration should be taken on possibilities to monitor, block or remove websites to prevent their use for TF and possibilities of referring crowdfunding platforms and other companies as reporting entities and adapting legislation and regulations on new payment methods.

More work should also be done to better leverage social media information for investigative purposes and including it as admissible evidence.

Competent authorities should strengthen information sharing particularly with reporting entities through clear legal channels and should consider collaboration with the private sector to get access to more data and analysis, including adapting fields in reporting requirements for online information.

Generally, methods of TF continue to evolve in response to changes in technology or deliberate attempts to circumvent law enforcement CFT efforts. Electronic, online and new payment methods pose a vulnerability which may increase over the short term as overall use of these systems grows. Many of these systems can be accessed globally and used to transfer funds quickly. A number of online payment systems and digital currencies are also anonymous by design, making them attractive for TF, particularly when the payment system is based in a jurisdiction with a comparatively weaker AML/CTF regime.

Between 2006 and 2010, the FATF issued typologies reports focusing on the

[29] FATF Report "Emerging Terrorist Financing Risk, October 2015
[30] Ibid.,

potential for NPPS to be misused by criminals; the identification of risk factors significantly differs from one new payment product or service to another, depending on functionality; and risk mitigates which can be tailored to a particular new payment product or service to address its specific risk profile. In 2013 the FATF issued guidance on taking a risk-based approach to prepaid cards, mobile payments and internet payment systems.

2.3.6 Virtual Assets/Currencies

For the purpose of applying the FATF Recommendations, countries are required to consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value" and apply the relevant measures to virtual assets and virtual asset service providers (VASPs).

Virtual currencies emergence has attracted investment in payment infrastructure built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. At the same time, virtual currency payment products and services (VCPPS) present TF risks. The FATF made a preliminary assessment of these ML/TF risks in the report Virtual Currencies Key Definitions and Potential AML/CFT Risks. [31]As part of a staged approach, the FATF developed guidance focusing on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers.

Virtual currencies such as bitcoin, while representing a great opportunity for financial innovation, have attracted the attention of many and pose risk for TF because the technology allows for anonymous transfer of funds internationally. While the original purchase of the currency may be visible, all following transfers of the virtual currency are difficult to detect or trace.

Promotion of virtual currency to fund terrorism can be exemplified by one case in which one accused person was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL. The accused person pleaded guilty admitted to using Twitter to provide advice and encouragement to ISIL and

[31] FATF (2015), Emerging Terrorist Financing Risks

its supporters. He used the Twitter handle and provided instructions on how to use bitcoin, a virtual currency, to mask the provision of funds to ISIL, as well as facilitation to ISIL supporters seeking to travel to Syria to fight with ISIL. He also admitted that he facilitated travel of one teenager, who travelled to Syria to join ISIL. The teenager, was charged with conspiring to provide material support to terrorists, conspiring to provide material support to ISIL and conspiring to kill and injure people abroad. The accused person account boasted over 4,000 followers and was used as a pro-ISIL platform during the course of over 7,000 tweets. The accused tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilize this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which kept the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin to other people.[32]

2.3.7 Prepaid Cards

Prepaid cards are cards with data encoded directly in the card, or stored remotely, that are preloaded with a fixed amount of electronic currency or value. While there are a wide variety of prepaid cards, the category of card of most concern is open-loop cards where funds can be withdrawn at Automatic Teller Machines (ATMs) worldwide. These are network-branded payment cards that allow transactions with any merchant or service provider participating in the payment network (e.g., Visa or Master card). General Purpose Reload (GPRs) cards are financial products that consumers can apply for online or pick-up from the prepaid section at various retailers. These cards are activated later by the consumer by phone or online. These products function like any other bank-issued debit card. [33]

Prepaid cards are replacing travelers' cheques as a method of moving money offshore. In terms of TF risk, these cards can be loaded domestically via cash or non-reportable electronic methods and carried offshore inconspicuously with no requirement to declare their movement across the border. On arrival in a high-risk country or transit country for TF, the funds are then converted back to cash through

[32] FATF Report "Emerging Terrorist Financing Risk, October 2015
[33] Ibid,.

multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Once a loaded card has been carried offshore, funds are accessible with minimal chance of detection. [34]

Prepaid cards providers that fall below AML/CTF regime thresholds are not subject to customer due diligence requirements. This can make it difficult to link a card back to an individual. Further, some of the systems allow multiple cards to be linked to common funds, allowing a third party to load funds using one card, while overseas beneficiaries access funds using a separate linked card. Additionally, any person can access the value stored on these cards with the accompanying PIN allowing for the cards to be sent to third parties more easily and securely than cash.

Some prepaid cards provide the possibility of person-to-person transfers. Many of the large, reputable companies will capture relevant data and have records similar to credit cards or debit records. In such cases, the companies can provide this data to competent authorities via compulsory measures such as a court order. This can include information about the card itself including: activation date, card holder information such as phone and e-mail address, transaction activity, transaction time and location and IP addresses used when logging in.

2.3.8 Internet-Based Payment Services

Internet-based payment services provide mechanisms for customers to access, via the internet, prefunded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider. Pre-funded accounts that consumers use for online auction payments are among the most dominant internet-based payment services. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Some TF cases involving low-value transactions via online payment systems such as PayPal have also been linked to a number of terrorism suspects. The extent to which these transactions have been used to finance terrorism is not established. Terrorism suspects have been observed using multiple online payment accounts, combining both verified and guest accounts. [35]

[34] FATF Report "Emerging Terrorist Financing Risk, October 2015
[35] FATF Report "Emerging Terrorist Financing Risk, October 2015

Payments appear to be linked to online purchases of equipment and clothing prior to the departure of individuals travelling to conflict zones rather than direct payments to associates to fund terrorist activities.

The use of an online payment system to assist in financing terrorism is more a reflection of the prevalence of this payment system in the wider financial system rather than any indication that online payment systems are more vulnerable to terrorism financing.

One case exemplifies a PayPal account used for fundraising in which a charity was set up in whose chairman was specialized in e-marketing. The charity offered on its website several options to make donations by credit card, PayPal, cash transfers, checks. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. EUR 2 million was collected out of which, EUR 600,000 came from a few PayPal transactions from another country. Personal PayPal accounts were also used to collects funds, then to be withdrawn by cash, or transferred to other accounts. [36]

In another case, law enforcement identified the use of CashU accounts to anonymously engage in transactions for illicit purposes. CashU is a prepaid online and mobile payment method available in the Middle East and North Africa, a region with a large and young population with very limited access to credit cards. Because of this, CashU was one of the most popular alternative payment options for young Arabic online gamers and e-commerce buyers. CashU uses courier companies in the UAE to collect cash from customers and is mainly used for paying for online games, Voice over Internet Protocol (VoIP), matrimonial, Information Technology services, foreign exchange trading and download of music and software.

The development, increased functionality, and growing use of new payment products and services (NPPS) globally have created challenges for countries and private sector. Notwithstanding their known vulnerabilities, the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear in Tanzania given the very few TF incidences.

[36] Ibid,.

2.4 HISTORICAL EVIDENCE OF TERRORIST FINANCING IN TANZANIA

Most financial experts agree that the financing of terrorism can occur in any country in the world, whether or not it has complex financial systems. Since complex international transaction can be abused to facilitate terrorist financing it may occur in a host of different countries. Despite the country's apparent vulnerability to terrorist financing, evidence obtained from law enforcement agencies during this risk assessment process shows that terrorist funding within or from URT is scant and mostly subjective hearsay and unreliable.

2.4.1 Precious Stones and Metals Dealings

Tanzania is very rich in mineral resources, such as gold, diamonds, uranium, and gemstone. There were allegations at some point in time that gemstone and gold smuggled outside Tanzania to Dubai and other destinations may be used to support terrorist networks. There is however no direct evidence of a link between the gemstone and gold trade or illicit gold and gemstone smuggling and terrorist networks or other terrorist groups although clandestine arrangements involving the gemstones and gold trade create suspicion to the use of this trade to finance terrorists in other parts of the world.

The tanzanite scandal in 2001 exposed by two Wall Street Journal reporters suggested that al-Qaeda controlled a sizeable trade in tanzanite from Tanzania. No evidence however was found of such a connection although the publication led major US retailers to drop tanzanite from their sale offering in February 2002. [37]Tanzania had to assure dealers at a major gem trade show in Tucson, Arizona, that no terrorist group was involved in tanzanite trade. As a result of this scandal, a system of warranties guaranteeing the gems were mined and exported legally was established.[38] The United Republic of Tanzania to date has declared the mining site of Mererani a controlled area where all controls are set in accordance with Mererani Controlled Area regulations (The Mining (Mirerani Controlled area) Regulations 2019) where no visitors are allowed without a dealer's license and other identification. Such control measures include due diligence process by registration

[37] Elvin, J. 2002. Gem dealers face war-on-terror backlash. Insight on the News, 18(25).
[38] Annette Hubschale. "Terrorist financing in Southern Africa" ISS Paper (Institute for Security Studies) 132 of January 2007.

of all buyers and sellers of tanzanite and reporting system of buying and selling of tanzanite.

2.4.2 Abuse of Charities

The detailed analysis of abuse of charities for TF is contained in risk assessment for NPO. Except for the case of Al-Haramain Islamic Foundation cited in paragraph 2.2.2 above, there is no information or investigation on abuse of charities in Tanzania for the purposes of terrorist financing or evidence that the funds are being channeled to terrorist networks. The NPOs TFRA has identified as having high TF risks NPOs that receive donations from abroad directly without using financial institutions and having the ability to operate in the proximity of conflict zones such as DRC and Mozambique.

2.4.3 Cross Border Currency Transportation

The FATF Recommendation 32 and the associated interpretive note, defines physical cross-border transportation as '… any in-bound or out-bound physical transportation of currency or BNIs from one country to another country and includes physical transportation by a natural person, or in that person's accompanying luggage or vehicle; shipment of currency or BNIs through containerized cargo or the mailing of currency or BNIs by a natural or legal person.

Tanzania's long, porous and unpatrolled borders may be vulnerable to terrorist financing, this is due to close relationship of societies between the neighboring countries. Police Force has encountered, and at times arrested, suspects attempting to export huge amounts of US dollars from Tanzania. However, it has been proved that all cases that involve the illegal smuggling of currency across national borders are attempts to bypass or flout tough foreign exchange and currency regulations.
Despite the increasing prevalence of non-cash payment methods in Tanzania, cash remains an important means of settlement with millions of cash evidenced by the STR received by FIU showing cross border cash transportation involvement.

Cash is still widely used in the criminal economy and there is a possibility that terrorist financing may occur as a result of cross border currency transportation in the western regions of Tanzania which could be linked with financing insurgencies in DRC. Similarly, cross border cash transportation in the southern regions could

be linked with financing of the Mozambique insurgents.

The physical transportation of cash across Tanzania's borders is widespread while there are no fully reliable records of the amount of cash transported in this way. Cash smuggling is an increasing problem and physical transportation of cash as a method is not restricted to a particular type of crime.

Cross border cash transportation is preferred by drug trafficking organizations, it is also linked to the illegal trafficking of other commodities, such as alcohol and tobacco, it is also used widely by criminals involved in other activity including tax crimes, weapons and arms smuggling, organized immigration crimes and the financing of terrorism. There are no cash smuggling methods more associated to one form of crime than another, and no guarantee that criminals committing the same type of crime will move their proceeds in the same way and by the same route. Instead, the methods used to physically transport illegally obtained cash are dependent on a decision-making process undertaken by the criminal. This process begins with the criminal deciding what the purpose of the cash movement is (for example, to break the audit trail, to pay a supplier, to bank it in another jurisdiction etc.). This will dictate the ultimate destination, which will in turn inform the method used, and ultimately the route chosen.

Once the cash has been moved to its destination and used for its intended purpose it will eventually enter the legitimate financial system and will be recycled by banks and other financial institutions.

In Tanzania the cross-border currency transportation is done in huge quantities on a daily basis across remote borders, by natural persons (carrying cash on their person, in their personal effects, or in a vehicle). The statistics on this from 2020 to 2023 is as indicated in the table below:

Table No. 1: Cross-border currency transportation statistics

SN	YEAR	STATISTICS
1	2020/21	1,885
2	2021/22	2,705
3	2022/23	2,457

Having adequate measures in place to detect and prevent illicit cross-border transportation of cash and bearer negotiable instruments (BNIs) is required to be strengthened.

2.4.4 Informal Remittance Systems/Hawala

Alternative/informal remittance systems take the form of non-bank institutions that transfer funds on behalf of clients through their own networks. Many of these transactions are paperless. Unregistered operators move money across borders with no written record. Part of the attraction of this system lies in the fact that there is no trail to the source or destination of the funds. It has been alleged that al-Qaeda has exploited the global hawala network by using it to transfer funds around the world.[39]

Hawala in Tanzania particularly in 1980s was not "underground" and operated openly in the street markets such as Kariakoo and was common among Asians and Somalis in the largest market area in Kariakoo in Dar es Salaam. The remittances were undertaken by legitimate businesses, such as travel agencies, clearing and forwarding companies, local grocery and many other business establishments. Many operators operated openly and people knew where to go when they needed the services. It is widely believed that informal remittances arose in Tanzania when people were seeking ways to evade trade and foreign exchange controls. There is no evidence linking informal remittance that was common in Tanzania with violence or gangs and crime syndicates. On the contrary, they were operating free of bribery and corruption and were preferred by many. They were benign, and were the result of people seeking a workable, efficient, cheap and secure means of transferring money and settling accounts with one another in a more expeditious way of transferring money from one location to another.

[39] https://www.investopedia.com/terms/h/hawala.asp, Julia kagan 2023

Given fewer or limited case linking financial flows to or from Tanzania to terrorist networks, it only remains highly probable that hawala is a vulnerability through which funds can be transferred to terrorist. Hawala operations are said to have prevailed in Tanzania and was common for diaspora communities to collect money in the developed world and send it to their brothers and sisters in Tanzania.

In October 2013 a story appeared in one newspaper known as Citizen that informal money transfers, especially internationally, was a big business not only in Tanzania but the rest of East Africa giving criminals a leeway to transfer their ill-gotten monies to the destination of their choice. The report referred to an incidence of a person named Ahmed; a Dar es Salaam-based businessman who wanted to transfer $50,000 (then about TZS 80 million) in January 2013 without involving the banking system. He was directed to see a merchant from Pemba, who was running an import-export business in Dar es Salaam. A friend, who is an importer of used Japanese vehicles, advised him to use the 'Pemba merchant courier', as the service was fast and reliable and that there was no room the money could be traced by authorities. Upon meeting the Pemba merchant, and explaining that he wanted to transfer $50,000 to his brother in London, he was instructed to give the exact name and mobile number of the recipient. He was then instructed to pay cash in Tanzanian currencies based on day's prevailing exchange rates. He paid TZS 81 million at the exchange rate of Sh1,620 plus the service fee of $500 (TZS 810,000). An hour later his brother called him from London to confirm receipt of the money. The recipient received it via a man of Somali origin. Had the trader used the bank, the exchange rate would have been Sh1,650 per dollar and he would have paid Sh84 million including bank charges and the transfer would have taken a minimum of 72 hours. He saved a whopping TZS 2.99 million and it took only an hour to transfer the money. He was assured that even if he wanted to transfer $1 million, arrangements for the transfer would have been made, provided he notified Pemba merchant at least a day in advance.

Tanzanian economy is heavily cash-based and financial infrastructures or services have not been able to reach the remote rural area. Access barriers to financial services such as high fees or minimum account balances, are a barrier to unserved rural areas as fees for the typically small amounts individuals need to send often amount to 20 to 30% of the transfer value (e.g. $10 fee for a transfer of $50). In this

regard, even today with the advent of mobile money networks, money transfers in Tanzania still by-pass formal financial and mobile money services and use niche services that fill the gaps. Domestic and intra-regional transfers are still transacted by informal means or nonfinancial services such as busses or individual couriers such as motorbike riders who serve as commuters nationwide. These alternative remittance forms are well known but operate clandestinely and are significantly cheaper as well as faster. Even some international transfers/remittances of migrants are still transacted through informal channels. The major problem that arises with this form of remittances is that the volumes are unreported in official statistics and provide no audit trail and therefore increases their vulnerability for terrorist financing particularly financing of FTF or financing individual for committing terrorist acts.

Exporters of crops often need to transport cash directly to the buying areas to pay producers at the farm gate or local trading centers. Given this context, various market research studies.[40] looked at how low-income individuals and small or microentrepreneurs transfer money and make payments in Tanzania and identifies gaps and weaknesses in the existing money transfer services. As a result, the studies in 1990s noted that these weaknesses offered an opportunity for different remittance services, including hawala system through services by bus companies and courier companies in Tanzania. The findings also showed that money transfer is a service almost everyone needs for purchase of new stock in the case of small traders, or the parents or migrants, who need to send home a supporting remittance or pay fees to school for children. Typical amounts sent for personal purposes range from $5 to 500 and for small traders up to $-50,000 per transaction.

Many migrants remit money home primarily to support their families, but also to purchase land or to build a homestead. Of recent the URT has given special attention to diaspora by introducing special status to the diaspora and also Bank of Tanzania has approved remittance agencies as products with a view to enhance contribution of diaspora remittances.

Internal or domestic migration is very common as well as intra-regional migration

[40] Sander, Cerstin and Samuel M. Maimbo, "Migrant Labour Remittances in Africa: Reducing Obstacles to Developmental Contributions", Financial Sector Vice-Presidency, Africa, World Bank, Washington, D.C., 2003a(www.worldbank.org/afr/wps/wp64.htm)

to neighboring or other countries overseas. Internal or domestic migrants tend to move from rural areas to either rural or urban centers for employment. These migrants usually use both formal and informal remittances to their relatives in their place of origin. Generally, domestic remittances are estimated to be lower in cumulative value than international remittances. The Bank of Tanzania does not track informal remittances.

International remittances in Tanzania tends to flow to and from neighboring countries for business purposes by small and big traders especially given that Tanzania serves as an exit by almost five landlocked countries (Zambia, Malawi, DRC, Rwanda and Burundi). Many of the overseas migrants from Tanzania are found in the United Kingdom, Germany, or the United States. Informal overseas remittance flows are not tracked and reported as part of the balance of payment statistics and Tanzania has no reported data. Remittance flows via informal channels or non-financial services, such as overland busses, are known to happen. The extent of this has not been estimated. In fact, informal money remittance in Tanzania were prevalent before mobile phones and mobile money service and were preferred fast and cost-effective method for worldwide remittance of money, particularly for people who were outside the reach of the formal financial sector or who transferred relatively small sums to avoid high minimum charges at conventional institutions. The development and widespread of retail banking branches and mobile telecom networks as major providers of financial services rendered hawala demand ineffective.

2.4.5 Radicalization and Violent Extremism

The Radicalization and Violent extremism are two important stages for an individual or group of people in the society or country towards joining the violent extremism organization (VEO) and committing violent acts. The individuals who join the VEO are either self-radicalized through social media or through VEO recruits agents in a face-to-face environment. The process of radicalization and recruitment are done in clandestine environment and sometimes it is difficult to be noticed by society and government security organs.

The presence of active VEO such as Al-Shabaab, Ansar al-Sunnah wa –Jama'ah (ASWJ) and ADF in countries neighboring URT, the porous border and the

proximity to the countries where VEO operate, pose direct radicalization and violent extremism (VE) threat in URT. Al-Qaida and ISIS are known VEO but they do not provide direct or indirect VE in Tanzania.

There is no single reason for an individual or group of people to be recruited and join the VEO but they range from individual push and pull factors to social, economic and political factors. The youth is the most vulnerable group to be radicalized and recruited into VEO to fight as foreign fighters where there are active VEO. It is from this process of recruitment and travelling to join VEO, they need financial support to sustain their travel, accommodation, meals and attaining weapons. The provision of financial support provided by individuals, VEO or other entities to facilitate their movement is TF.

URT takes cognizance of the prevalence of Radicalization, VE threat and Terrorism financing in the country. In response and to ensure this problem is addressed, the government has taken some legal measures including the enactment of Prevention of Terrorism Act and the Anti-money laundering legislations (AMLA and AMLPOCA) which prohibit acts of terrorism, financing of terrorists and other forms of assistance or facilitation of terrorists including VE related to terrorism or terrorists. Through NCTC in collaboration with other stake holders, the government implements, the whole government and Society Soft approach to prevent Radicalization and VE in the country. Apart from these measures, building security service capability to address VE, cooperation in information sharing with Law enforcement agencies and financial institutions in addressing TF threat, the multi-agencies collectively work together to prevent VE and TF. As part of the Government's measures to prevent Radicalization and VE, the implementation of UNSC Resolution 1373 (2001), which among other things emphasize on the domestic designation of terrorists, terrorist organizations and terrorist groups is given priority as an effective way of dealing with radicalization and VE. The URT as a member of both EAC and SADC, through regional cooperation in defense and security, works together with all member states of these two blocks to prevent not only Radicalization and VE but also TF in the region.

Table No. 2: - The incidents related to VE threat which may have TF connection:

s/no	Year	Incident	TF
1	Oct 2013	Arrest of suspected Violent extremists of Al-Shabaab ideology supporters undergoing Military training in their camp in Makoliongo mountains, in Mtwara region.	Self-financed
2	Oct 2013	The arrest by Kenyan Defense Forces (KDF) of three Tanzanians travelling to Somalia to join Al-Shabaab.	Self-financed
3	Nov 2013	The arrest of 69 people running child indoctrination camp, who were aged between 4-13 years old in Kilindi district, in Tanga region.	Unknown financier
4	2015	The arrest of Tanzanian youth in Garissa University terror attack in Kenya.	Self-financed

PART III
RISK ASSESSMENT OF TERRORIST FINANCING IN TANZANIA.

Taking into consideration Parts I and II of this report, this section will focus on analyzing the data collected and identifying the threats, vulnerabilities and likelihood of TF in specific sectors in the Tanzanian context. The relevant aspects of concern will be addressed with recommendations to mitigate the risk. Each sector will be looked in terms of an overview of the sector, the threat, the vulnerability, threat and vulnerability assessment, and recommended action. This part is concluded by identifying the most vulnerable areas for TF with a view to guide the public in general as where more resources should be allocated and where close supervision is needed.

3.1 Data Analysis

From 14th -18th March, 2022 a workshop was conducted and a questionnaire was circulated to over 50 participants presented at the workshop that include 10 Law Enforcement Agencies (FIU, Tanzania Police Force, Immigration Department of Tanzania, National Prosecution Services, ODPP-Zanzibar, NCTC, Drugs Control Enforcement Authority, Tanzania Revenue Authority, TISS and Zanzibar Revenue Authority) 7 Government Ministries (Ministry of Home Affairs, Ministry of Works, Ministry of Foreign Affairs and East Africa Cooperation, Ministry of Constitution and Legal Affairs, Ministry of Land and Human Settlement, Ministry of finance and Planning and the President Office) 9 regulatory authorities (BOT, CMSA, TIRA, Gaming Board of Tanzania, RITA, Zanzibar Investments Promotion Authority, Tanzania Investment Center, Tanzania Communications Regulatory Authority and the Mining Commission), 3 Registrars of NPOs (Registrar of NGOs-Mainland, Registrar of Societies-Mainland and Registrar of NGOs- Zanzibar).

All participants responded to the questionnaire, resulting in a response rate of 100%. The questionnaire was divided into ten (10) sections, being: general questions in relation to incidences of TF encountered by each entity, number of STR related to TF, LEAs requests from FIU on TF related issues, ongoing investigations on TF, seizures made in relation to TF cases, prosecutions on TF, pending cases on TF,

court decision and forfeiture and confiscation made in relation to TF cases.
Responses from the questionnaire were collated, analyzed and the findings were as set out below:

- Overall, the majority of the participants 80% except the LEAs were not aware of the various methods of TF. The respondents indicated that they have not been trained on TF related issues confirming NRA findings that awareness levels were low.

- Most (90%) participants except FIU, NCTC and the Police had not handled transactions TF. The majority indicated a low level of determining TF suspicious transactions/activities.

- A sizeable 100% of participants have not made any request to FIU for TF related information including LEAs;

- 20% participants mostly LEAs keep records of TF information. Effectively this means 80% do not keep TF records which is a problem as almost all participants have no TF related information in their records.

- On TF STR from FIU the responses indicated 20 STR were received from reporting persons for consecutive three years representing only about 0.8% of all STR received which is very low. The summary of TF related STR received is as shown below:

Table No.3: TF related STRs

Year	**No. of TF related STR**
2020	3
2021	9
2022	8

- On the TF Intelligence Reported disseminate to LEAS from FIU, it was indicated that eight (8) TF related Intelligence report was disseminated to various LEAs constituting 0.92% of all intelligence packages disseminated. The details of intelligence disseminated is as shown below:

Table No. 4: TF Intelligence Disseminations

YEAR	Recipient LEA	No. Of Intelligence disseminate	rcentage to total number of intelligences
2020	NCTC	1	0.99%
2021	NCTC	1	1.79%
2022	NCTC	6	1.83%

- On Prosecution, the NPS and ODPP of Zanzibar reported that there were eight (8**)** T/TF cases prosecuted between 2020 – 2022.

- On the decided cases and forfeitures /confiscation made, NPS and ODPP Zanzibar reported that between 2020 – 2022 there were 6 TF cases ongoing cases in various courts of law and two (2) completed cases. However, there was no property in connection with pending/completed cases which was forfeited or confiscated.

- A whopping 100% of shareholders had not reported TF suspicious activity/ transaction or any matter to financial institutions.

- All participants do not have TF policy and also do not carry out TF risk assessments in their organizations and 40% particularly the regulators have a designated Compliance Officer responsible for TF and ML issues.

- On the pending investigation it was reported by LEAs that there were four (4) TF cases pending investigation at the TPF, there was no TF related corruption cases at PCCB and no TF related Drug cases at the DCEA.

- From observation, even though the results seem to be of concern, it has to be noted that 100% of the respondents were from the Government which have enforcement role in the whole TF spectrum and supervision role for the implementation of TF counter measures. In addition, all of the respondents are not reporting persons in terms of Money laundering legislation. The private sector involvement will be considered in the sector and institutional Risk Assessment. The National level TF Risk Assessment focusing on

identifying the national TF risks to ensure the better understanding of its ramifications and guide or form the basis for other stakeholders' risk assessments (that is sectoral and institutional risk Assessments).

3.2 Assessment of abuse of Non-profit organization (NPO) for Terrorist Financing.

3.2.1 Overview

In a publication entitled "Combating the abuse of NPO – Recommendation 8 of June 2015, FATF defines NPO by referring it to legal person or legal 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". For the purpose of this report the term Non-Governmental Organization (NGO) may refers as to Non- Profit Organization (NPO).

NPOs play a vital role in society and in a URT's economy because they complement the government's efforts to provide services and assistance to communities. In cases where government support is minimum, NPOs usually fill in the gap. As such, NPOs enjoy the confidence of governments and the public, with both governments, donor and Private sector funneling funds into NPOs for their "good works" and programs. However, recently most NGOs potential donors have changed some funding modalities and agree only to fund NGOs directly through call for funding as opposed to previous general practice of foreign donation that requested all funding to be channeled through Treasury according to the Government Loans, Guarantees and Grants (Amendment) Act.

In the United Republic of Tanzania, the legal system identifies NPOs as NGOs and Societies. The laws governing NPOs (Act No 24 of 2002 of Tanzania Mainland and Act No 6 of 1995 of Zanzibar) define NGO to mean a voluntary grouping of individuals or organization which is autonomous, non-partisan, nonprofit making which is organized locally at the grassroots, national or international levels for the purpose of enhancing or promoting economic, environmental, social or cultural development or protecting environment, lobbying or advocating on issues of public interest of a group of individuals or organization, and includes a Non-Governmental

Organization, established under the auspices of any religious organization or faith propagating organization' trade union, sports club, political party, or community based organization. The Societies Act, Cap 337 define 'Society' as a non – partisan and non – political association of ten or more persons established for professional, social, cultural, religion or economic benefits or welfare of its members but does not include Companies, trust, trade union, cooperative societies, agricultural associations, political Party, non – governmental organization Sports association and community microfinance group registered under relevant laws.

In June 2022, URT conducted an assessment of NPO sector with a view to identifying the scale, scope and identifiable characteristics of the NPO sector in Tanzania. It was important to identify precisely the NPO landscape and the regulatory framework that surrounds it and based on international best practice, identify the emerging strategic gaps and risks, culminating in the recommendations to mitigate risk and improve regulatory processes in order to increase trust and confidence within the sector.

During preparation of this report, there a number of changes were going on in the coordination and registration of NGOs in Tanzania, one being rolling out of NGOs online registration system which includes identification of all registered members through National identification (NIDA). Moreover, the Guideline for coordination of NGOs in Tanzania mainland where Government departments, Local government and Private sector roles in coordination of NGOs were issued to ensure all NGOs are coordinated at sectorial levels. The said improvements in the sector sought to identify vulnerability and TF risk to the sector and design relevant mitigation and action plan.

In URT there are three regulators for the NPOs. These are: Registrar of NGOs Mainland, Registrar of Societies Mainland and Registrar of NGOs Zanzibar. The Registrar of NGOs in Mainland was established under Section 3(1) of the Non-Governmental Organizations Act, 2002 (CAP.56) with a view to coordinate and regulate activities of Non-Governmental Organizations (NGOs).

The Registrar of Societies in Tanzania Mainland is established under Section 5 of The Societies Act, Cap 337. Section 2 as amended by Section 39(b) of the Written

Laws (miscellaneous Amendments) (No. 3) Act, 2019 provides for powers to register and regulate civil societies.

The Registrar of NGOs in Zanzibar is established under section 9 of the Societies Act No 6 of 1995 to coordinate and regulates the activities of Non- Governmental Organizations and Civil societies.

Records reveal that in URT there are about 11,197 registered NGOs and 1,685 Religious Societies registered as of April, 2023, as shown in table 5 below:

Table No. 5: Registered NPO in URT

SN	REGISTRAR	TOTAL REGISTERED NGO	TOTAL REGISTERED SOCIETIES	TOTAL REGISTERED FOREIGN NPO
1	REGISTRAR OF NGO ZANZIBAR	2,494	65	41
2	REGISTRAR OF NGO MAINLAND	8,703	NIL	563
3	REGISTRAR OF SOCIETIES	NIL	1,620	147
	TOTAL	**11,197**	**1,685**	**751**

3.2.2 Threats

The Assessment conducted identifies the following threats in the NPO sector:

a. Deliberate activities of bad actors using NPO as cover to raise funds;
b. Misuse of funds;
c. Establishment of NPOs branches to act as TF cells to finance terrorism;
d. Financial fraud;
e. Fund rising abuse; and
f. Legitimate NPOs used as cover for illegal activities.

For the period of 2020-2022, there were neither SRSs nor SAR related to TF linked to the threats identified in paragraph 3.1.2. In addition, from the data base of LEAs and regulators there were no statistics on issues set out in (a) – (f) linked to TF.

The above threats are minimized/mitigated by the registrars of NPOs supervisory process in their legal framework particularly on approvals of any fundraising, submission of quarterly activity and financial statements and sanction power including registration/ license revocation. Terrorist financing threat through abuse of NPO is rated **Medium** on grounds of the possibility of direct access to funding from other sources without using financial institutions.

3.2.3 Vulnerability

The Assessment conducted identifies that NPO sector is vulnerable in the following aspects:

a. Access to receive direct contributions from different sources of funds;
b. Ability to operate in area close to conflict zone, example DRC (Democratic Republic of Congo) and Mozambique;
c. Cash intensiveness;
d. Ability to operate globally networks (Global networks);
e. Transparency and accountability of usage and money movements; and
f. Existence of undisclosed philanthropist.

The above vulnerabilities are minimized/mitigated by the registrars in URT supervision powers of NPOs including power to review the planned activities and funding sources. Terrorist financing vulnerability through abuse of NPO is rated **Medium,** taking into account the above vulnerabilities.

3.2.4 Overall rating

The current TF threat facing the sector is largely due to the presence of foreign NPOs The statistics of foreign registered NPO from 2020 to 2023 is as indicated in the table 3. NPOs located in underdeveloped areas within the country and other service type NPOs including charitable, social development, humanitarian disaster relief and educational which are prone for abuse for TF. There is no data from the Financial Intelligence Unit of STR related to the NPO sector filed on TF.

Based on the Medium rating of the threat together with the Medium TF vulnerabilities the NPO sector likelihood for TF risk occurring is **Medium.**

3.2.5 Specific Recommendation

It is recommended that-

a. Registrars should conduct "sectoral risk assessment" to categorize existing NPOs available in their various registries depending on their risk status (high, medium or low);
b. Registrars should apply risk-based supervision and enhanced due diligence to high-risk NPOs;
c. Registrars should properly allocate resources to mitigate or prevent high TF risk areas;
d. Registrars should ensure NPOs financial transactions are conducted through banks to avoid use of cash transactions;
e. Registrars should ensure compliance by NPOs on submission of audited financial statements on timely basis;
f. Registrars should enhance effective cooperation with regional and global counter-parts institutions in sharing NPOs information.
g. Registrars should ensure effective, proportionate and dissuasive sanctions are imposed to non-compliantly NPOs;
h. Before registering of foreign NPOs registrars should conduct enhanced screening against TFS designated list;
i. Registrars should conduct outreach programs for TF and TFS awareness purposes.

3.3 Assessment of Organized Crime for Terrorist Financing.

3.3.1 Overview

United Nations Convention on Transnational Organized Crime - UNCTOC, adopted by General Assembly in November 2000 through Resolution No 55/25 does not contain a precise definition of Organized Crime nor does it list the kinds of crimes that might constitute it. The lack of definition, according to UNODC, was intended to allow a broader applicability of the UNCTOC to new types of crime that emerge constantly as global, regional and local condition change over time.

The, UNODC (2018) define organized crime as a continuing criminal enterprise that

rationally works to profit from illegal activities that are often in great public demand. Its continuing existence is maintained through corruption of public officials and the use of intimidation, threats, or force to protect its operations.
Article 2(a) of UNCTOC define "Organized criminal group" to mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit. Example of Organized crimes include terrorism, drugs trafficking, trafficking in wildlife, illegal smuggling of mining and trafficking in timber and charcoal.

In URT there is no current declaration made from any terrorist groups or affiliate, or request made to compel or stop the government from doing its activities that indicate criminal organized activities.

3.3.2 Threat

The Assessment conducted identifies the following threats regarding organized crimes:

a. Trafficking in wildlife and poaching;
b. Illegal logging and the trafficking in timber and charcoal;
c. Drugs trafficking;
d. Smuggling of Precious stones and Metals;
e. Trafficking in Counterfeit Goods;
f. Smuggling of Immigrants;
g. Tax Crimes;
h. Trade Based Offences;
i. Small arms proliferation; and
j. Irregular migrants through borders from Rwanda and Burundi.

The risk assessment revealed that there is no evidence that linked the above threat of Organized Crime with Terrorists Financing in URT but with the proximity of URT to conflict jurisdiction, there is a possibility of the risk of Organized Crime to be used for TF. Terrorist financing through Organized Crime is rated **Medium,** given that the risk is mitigated by robust legal, institutional framework, preventive measures and sanction regime.

3.3.3 Vulnerabilities

Organized crime operates beyond the jurisdiction limits in an organized way. URT is among the jurisdictions that are prone to abuse by organized crime and TF, because of, among other things, porous borders with 8 neighboring countries experiencing conflict and instability to certain degree such as Democratic Republic of Congo, Mozambique, Burundi, Rwanda, Uganda and Kenya. This geographical position increases Tanzania's vulnerability of being abused by organized criminals for terrorist financing and terrorism purposes.

In 2015 URT extradited to Uganda Mr. Jamil Mukulu, Mr. Mohamed Matovu and Mr. Omari Abdallah Mtuka who were alleged to commit Murder and TF related offences. In 2017 URT disseminated evidence through mutual legal assistance relating to TF offences committed by the mentioned extradited persons. The above extradition and transfer of evidence from URT was made possible due to extradition and mutual legal assistance mechanism existing in Tanzania to mitigate its vulnerability to international organized crime.

In addition, following security threat incidences by ISIS-Mozambique in Mtwara Region by organized criminals, URT's Inspector General of Police signed an MOU with counterpart Inspector General of Police of Mozambique to share information to strengthen security along the border area.

The above Vulnerabilities is minimized/mitigated in URT through available legal framework and institutional framework such as extradition and mutual legal assistance and MOU with counterpart law enforcement authorities. Terrorist Financing vulnerability through Organized Crime is rated **Medium Low**.

3.3.4 Overall rating

In 2016 threats from organized crime including trafficking in wildlife and poaching, trafficking in timber and charcoal from Mozambique and drugs trafficking were identified, in the National Risk Assessment – NRA, as ***high-risk crimes***. Other crimes identified, in the National Risk Assessment, as high-risk crimes include illegal smuggling of precious stones and metals, trafficking in counterfeit goods and smuggling of Immigrants. Efforts employed by the URT, in between 2016 and 2022,

managed to mitigate the organized crime named above. Basing on mitigation measures employed, the Terrorist Financing risk from organized crime is assessed as **Medium** and therefore the sum total of medium threat and Medium low vulnerability culminates to Medium Risk.

3.3.5 Specific Recommendations

a. Investigation of offences [such as trafficking in wildlife and poaching, trafficking in timber and charcoal, drugs trafficking, illegal smuggling of mining, trafficking in counterfeit goods and smuggling of Immigrants] LEAs should conduct parallel financial investigation with a view to ensuring proceeds emanating from this are confiscated/forfeiture and elevate chances of the use of such proceeds for TF.
b. Patrol on the borders with neighboring countries should be increased in order to mitigate or minimize threats of attack or movements of criminals.
c. Cooperation with neighboring countries to strengthen security at their borders should be given high priority.

3.4 Assessment of Precious Stones and Metals Dealers for Terrorist Financing.

3.4.1 Overview

Precious stones are defined as visually appealing gemstones created from rocks or minerals. Often used for jewelry and fashion accents. This term was created in the mid-1800s to refer to four specific stones; diamonds, rubies, emeralds, and sapphires. All precious stones are translucent and are valued by the richness of their color, except for the diamond, which has a higher value based on being colorless.
Precious stones include diamonds, sapphires, rubies, emeralds, jade, and pearls. Precious metals include gold, silver, and platinum. International and regional typologies studies indicate relatively few instances of terrorist financiers using precious stones and precious metals to move or raise funds for terrorism. However, precious stones and metals have high intrinsic value in a relatively compact form and tend to maintain or increase their value over time.

Precious stones and metals are a good store of value and accepted as an alternative

to money, easily transported and concealed, and easily converted to cash. Criminals may purchase precious stones to hide the illicit sources or purposes of their funds. This exposes dealers to TF risks. There may also be a risk that dealers are actively involved in TF to facilitate their business in high-risk locations.

Tanzania is very rich in mineral resources, namely gold, iron, silver, copper, platinum, nickel and tin all these represents Metallic Minerals. Other minerals found in Tanzania includes diamonds, tanzanite, ruby, garnet, emerald, spinel, alexandrite, tourmaline and sapphire representing Gemstones. While Uranium Coal represents energy minerals Kaolin, Phosphate, Lime, Gypsum, Bentonite, Vermiculite, Salt, Beach sands etc represents Industrial minerals.

However, the common traded minerals across the world includes gold, diamonds, uranium and tanzanite. There is allegation that gemstone and gold smuggled outside Tanzania to Dubai and other destinations may be used to support terrorist networks. There is however no direct evidence of a link between the gemstone and gold trade or illicit gold and gemstone smuggling and terrorist networks or other terrorist groups. However, clandestine arrangements involving the gemstones and gold trade create suspicion to the use of this trade or financing terrorists in other parts of the world.

3.4.2 Threat

The risk assessment reveals that trends of illegal smuggling of precious metals and stones are decreasing as shown in table No. 4 below. There is no evidence to associate the smuggling of precious stones and metals with terrorist financing. Extraction mining operations in high-risk jurisdictions where terrorist groups operate do however pose TF threat. Dealers and brokers of precious metals and stones in Tanzania, and financial service providers may not be aware of the TF risks in their business and they may not apply preventive measures when conducting businesses or submitting suspicious transactions or activities reports to FIU. In this regard, the Terrorist Financing through Precious Metals and Stones is rated **Medium.**

Table No.6: Illegal Smuggling of Precious Metals and Stones Incidences

S/N	YEAR	INCIDENCES	GRAM
1	2019/20	100	15,401,887.37
2	2020/21	87	1,723,274.72
3	2021/22	63	51,560,176.977

Source: Mining Commission Database

3.4.3 Vulnerabilities

The risk assessment of terrorist financing reveals that URT is vulnerable to illegal smuggling of precious stones and metals due to the following facts;

a. Porous borders;
b. Instability of neighboring countries where extraction of mining is active and terrorist groups are operating;
c. Illegal mining and trading in precious stones and metals;
d. Lack of AML/CFT/CPF regulator in the sector; and
e. Corruption.

URT has a legal framework (The Mining Act (Cap:123) for trading of precious stones and metals which requires all small miners to trade the precious stones and metals at the district's mineral markets where proper KYC/CDD and all relevant information of the dealers are kept and maintained. Pursuant the Anti-Money Laundering Act (Cap:423) dealers in precious stones and metals are reporting persons and hence subject to CDD, record keeping, filing STR and other preventive measures. These requirements mitigate the vulnerabilities in this sector.

Since the Terrorist Financing Vulnerabilities are minimized/mitigated in URT through available legal framework and institutional framework, the Terrorist Financing vulnerability through Precious Stones and Metals is rated **Medium Low**.

3.4.4 Overall risk rating

The risk assessment reveal that, there is no evidence to associate the smuggling of precious stones and metals with terrorist financing. In addition, since 2016 to date URT has made substantial reforms in mining sector and therefore the Terrorist Financing threat through precious metals and stones is assessed as **Medium** as a

result of the sum total of Medium Threat and Medium Vulnerability.

3.4.5 Specific Recommendations

a. There is a need to amend AMLA, AMLPOCA and Mining Act to empower the Mining Commission to supervise DPMS for the AML/CFT/CFP purposes.

b. The Mining Commission and FIU should conduct to conduct **"sectoral risk assessment"** to enable categorization of existing DPMS depending on their ML/TF risks levels;

c. ***CFT Risk-based supervision*** should be applied to DPMS and enhanced due diligence should be applied to high-risk DPMS;

d. The Mining Commission should conduct CFT outreach programs to high risk DPMS;

e. The Mining Commission should ensure effective, proportionate and dissuasive sanctions are imposed to any non-compliant DPMS; and

f. The Mining Commission should before licensing DPMS conduct screening of the applicants against TFS designations.

3.5 Assessment of Transportation of Funds for Terrorist Financing

3.5.1 Assessment of Banks

3.5.1.1 Overview

Terrorist financiers are known to use the banking sector to move funds into and out of countries. These typologies are well reported in the region and around the world. Based on investigations and cases prosecuted by law enforcement agencies to date, TF activities through banks in URT have not been experienced. Nevertheless, URT remains vigilant to the risk of the banking system being used as a conduit by terrorists and their financiers, given that URT is bordered with countries faces terror attacks.

The statistics maintained by FIU on TF related STRs from the banking sector are as shown below:

Table No. 7 - TF related STRs from the banking sector

SN	YEAR	No. of STRs
1	2019/20	2
2	2020/21	0
3	2021/22	8
4	2022/23	6

3.5.1.2 Threats

The assessment revealed that the financial sector is at risk of being abused as a conduit by the terrorist and their financers due to being close to the countries facing terror attacks. Terrorist financing threat through Bank is rated **Medium Low** due to availability of effective preventive measures.

3.5.1.3 Vulnerability

The assessment reveals that banking sector in URT remain at risk for being used as a major conduit for transfer of value and funds and remain vulnerable for TF. However due to comprehensiveness legal framework and effectiveness supervision as well as strong and effective control Terrorist Financing Vulnerability through banking sector is rated **Medium Low**.

3.5.1.4 Overall rating

Terrorist financing through banking sector is assessed as **Medium Low**.

3.5.1.5 Specific Recommendations

a. Bank of Tanzania (BOT) should conduct "sectoral risk assessment" to enable categorization of existing licensees depending on their TF risk;
b. BOT should apply ***risk-based supervision*** to its licensees and apply enhanced due diligence to high-risk licensees;
c. BOT should ensure effective, proportionate and dissuasive sanctions are applied for non-compliance; and
d. Before licensing a bank to operate in URT the BOT should conduct enhanced screening against TFS designated list.

3.5.2 Assessment of Money or Value Transfer Services (MVTS)

3.5.2.1 Overview

According to the FATF, "Money or Value Transfer Services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments, or other stores of value and payment of a corresponding sum in cash or other forms to a beneficiary by means of communication, message transfer or through a clearing network to which the relevant financial service provider belongs. Transactions performed by such service may involve one or more intermediary transactions and final payment to a third party and may include any new payment methods. A terrorist financier can abuse MVTS by transporting funds from originator/source to Terrorist group due to its less stringent KYC requirements. Example of MVTS service operates in URT are Western union and MoneyGram.

3.5.2.2 Threats

The Assessment conducted identifies the following threats regarding MVTS:

a. Walk in customer one time or occasional customer;
b. Electronic fund transfer services;
c. Anonymity between parties;
d. Virtual Assets;
e. Internet based payment systems; and
f. Prepaid cards.

Terrorist financing threat through MVTS is rated **Medium** due to involvement of electronic fund transfers.

3.5.2.3 Vulnerability

In URT MVTS uses commercial banks platform or have sub agency contract with commercial banks to render their services and they are obliged to observe reporting person's obligation as other financial service providers; KYC/CDD for both sender and receiver. The use of commercial bank platform reduces the MVTS vulnerability to be abused. Terrorist Financing Vulnerability through MVTS is rated **Medium Low**.

3.5.2.4 Overall rating

Terrorist financing risk through Money or value transfer services is assessed **Medium** because in URT, Money or Value Transfers Services uses commercial banks platform or have sub agency contract with commercial banks to render their services. In addition, MVTS service providers are obliged to observe reporting person's obligation as other financial service providers.

3.5.2.5 Specific Recommendations

a. BOT should conduct "sectoral risk assessment" to enable categorization of existing MVTS licensees depending on their TF risk;
b. BOT should apply ***risk-based supervision*** to MVTS Service providers; and
c. BOT should ensure effective, proportionate and dissuasive sanctions are applied to non-compliant licensees.

3.5.3 Assessment of Cross Border Transportation of Cash

3.5.3.1 Overview

"Cross border transportation" means any physical transportation of currency or bearer negotiable instrument from URT to another country or vice versa and includes: -

(a) Physical transportation by a natural person, or in that person's accompanying luggage or vehicle;
(b) Shipment of currency or bearer negotiable instrument through containerized cargo; or the mailing of currency or bearer negotiable instrument by the natural or legal person;

Cross-border transportation of cash is therefore the movement of hard cash from one jurisdiction to another. Terrorist financers around the world have been known to use hard cash couriers as a means to physically move funds across borders to finance their activities. Unlike transactions in regulated sectors, cash movement transactions do not leave physical or digital footprint.

URT has a legal framework (i.e. The Anti-money laundering - Cross border declaration of Currency and bearer negotiable instruments Regulations of 2016*)* G.N. NO. 38 of 2016 and Anti-money laundering and Proceed of Crime Regulations

of 2022 which deters the transportation of hard cash to or from URT. The law imposes proportionate and dissuasive sanctions for non-compliance and the customs department of the Tanzania Revenue Authority enforce cross-border declaration of currency.

Regulation 4 (1) of Anti-Money Laundering ((Cross Boarder Declaration of Currency and Negotiable Instruments) Regulations of 2016) and Regulations 23(1) of AMLPOC Regulations 2022 require a person entering or departing the territory of the United Republic of Tanzania while in possession of currency or Bearer Negotiable Instrument amounting to Ten Thousand US Dollars (USD 10,000) or its equivalent in Tanzanian shillings or any foreign currency based on the official conversion rate of the Bank of Tanzania which is in effect at the time of transportation of the currency or bearer negotiable instrument across the border, to declare to the customs authority the amount in his possession.

Regulation 7 (1) of the Anti-Money Laundering ((Cross Boarder Declaration of Currency and Negotiable Instruments) Regulations of 2016) and AMLPOC Regulations 27 (2) (c) of 2022 requires customs officers to report to FIU within seven working days from the date of receipt of the declaration, on every declaration made under Regulations. Although the submission of the report to FIU takes longer than seven days**.**

3.5.3.2 Threats

The Assessment conducted identifies the following threats regarding Cross-border transportation of cash:

(i) Porous borders; and
(ii) Cash economy and Bearer Negotiable Instruments transportation use.

Terrorist Financing threat through cross border currency transportation is rated **Medium High**

3.5.3.3 Vulnerability

Assessment reveals that, due to its proximity to eight neighboring countries, URT porous borders seems [to be] vulnerable for being abused by terrorist financers to transport funds to any neighboring jurisdiction targeted for terrorist activity.

Initiatives are underway to automate cross border declarations to ensure effectiveness and reduce vulnerability. Terrorist Financing Vulnerability through cross border currency transportation is rated **Medium Low** given border control measures and surveillances and the legislative requirements on forfeiture/confiscation of undeclared amount

3.5.3.4 Overall rating

Terrorist financing threat through cross border currency transportation is assed as **Medium** given the high porous border areas and the presence of conflict zones in DRC and Mozambique. The 2020 strategic report on Cross Border Transportation of cash indicated high movement of cash through the major border posts in Tanzania to destinations that had deficient AML/CFT measures including UAE as well as from conflict area in DRC. In the case of BNI, they are not much in use due to technological development.

3.5.3.5 Specific Recommendations

a. TRA should ensure that persons do not enter or leave the United Republic while in possession of currency or bearer negotiable instrument of the threshold prescribed by law;

b. TRA should strengthen the customs department to raise its detection capacity so that any person who contravenes the declaration requirements is prosecuted and the undeclared amount forfeited /confiscated as required by the law;

c. LEAs needs to increase patrol of the porous borders;

d. TRA should finalize the automation of CBDC and implement the submissions to FIU accordingly; and

e. LEAs should enhance capacity to investigate source and purpose of non-declared funds and negotiable instruments.

3.5.4 Assessment of Hawala

3.5.4.1 Overview

Hawala is the transfer of money without actually moving it and is based on trust.

Simply stated, hawala is *"money transfer without money movement"*. It is a popular and informal value transfer system based not on the movement of cash, or on telegraph or computer network wire transfers between banks, but instead, it is based on the performance and honor of a huge network of money brokers (known as hawaladars). While hawaladars are spread throughout the world, they are primarily located in the Middle East, North Africa, the Horn of Africa, and the Indian subcontinent. They operate outside of or parallel to, traditional banking, financial channels, and remittance systems.

In the most basic variant of the hawala system, money is transferred via a network of hawala brokers or hawaladars.

Principally hawala practices allow anonymity of sender and receiver of the transaction, and their information cannot be traced so it can be abused easily by terrorist financiers.
All participants responded negatively to the question whether there have been convictions on Hawala operation. The LEAs explicitly stated that they do not have data to support the existence of Hawala and that they base their conclusion that there has been no intelligence report on Hawala based TF. All participants viewed Hawala as vulnerable to TF and all agreed that they should be rated as Medium High risk. All participants also responded that Hawala is not common in Tanzania anymore because of existence of highly efficient and convenient banking and remittance services.

3.5.4.2 Threats

The Assessment conducted identifies the following threats regarding Hawala in URT:

(i) Presence of Hawaladars albeit very few;
(ii) Presence of Foreign immigrant;
(iii) Presence of Tanzania Diasporas in countries that use Hawala;
(iv) Costly formal remittance services; and
(v) Presence of informal cash couriers.

Terrorist Financing threat through Hawala is rated Low given that it is no longer a preferred mode of payment today.

3.5.4.3 Vulnerabilities

The Assessment conducted identifies the following vulnerabilities regarding Hawala:

(i) Lack of supervision;
(ii) Settlement across multiple jurisdictions;
(iii) Settlements through value/net settlement without funds movement;
(iv) Settlement outside the financial system;
(v) Commingling of licit and illicit proceeds; and
(vi) Use of modern IT communication services of international funds transfers.

Terrorist Financing Vulnerability through Hawala is rated **Medium**.

3.5.4.4 Overall rating

Terrorist financing risk through Hawala is rated **Medium Low** because of the high cost of other existence of forms of remittance.

3.5.4.5 Specific Recommendations

a. There is a need for BOT in collaboration with LEAs to conduct research so as to determine the extent, magnitude and threat of Hawala Remittances in URT; and
b. Financial Regulators should enhance financial inclusion efforts to discourage use of Hawala.

3.6 Areas That Are Most Prone For TF

All stakeholders agreed that the following areas are more prone for TF. This categorization is also based on the FIU's monitoring of trends from the STRs received on which the analysis points to the likelihood of the identified areas to be abused for TF. Three most vulnerable areas, in order of priority that all stakeholders agreed to be prone for TF are:

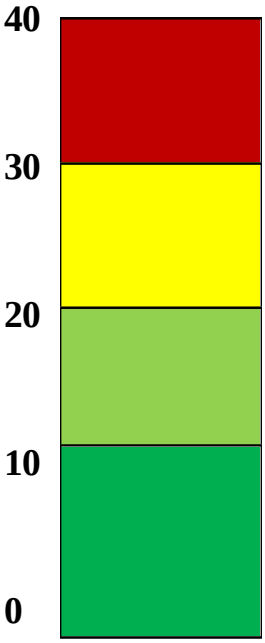
a) Remittance services including both formal and informal funds transfer. The trends from STRs indicate substantial remittances particularly from payment aggregators involving international remittance in some instances conflict or insurgency prone areas of DRC and Burundi. These remittances could be channeled to finance the conflict/ insurgents.

b) Activities taken place in the proximity of border areas near conflict zone or areas experiencing insurgencies. The STRs from border areas shows likelihood of illegal activities particularly illegal foreign exchange businesses, illegal mining and illegal smuggling of farm produces are generating funds that are laundered through the financial institutions.
c) NPO sector is also an area that may be prone to TF given the ability to obtain funds directly without being channeled through financial institutions. Most NPO's donors prefer anonymous methods of channeling funds to NPOs without leaving trail of the financial transactions to the respective NPOs.

It is highly recommended that competent authorities should focus on these three areas in terms of allocating resources to ensure that the operators in those areas are reached out and made aware of their vulnerability to TF. Competent authorities should also conduct inspections of the operators in the three identified areas. LEAs in particular, Tanzania Revenue Authority, Tanzania Immigration Department and the Tanzania Police Force should closely monitor the activities along border areas.

PART IV
TERRORIST FINANCING RISK LEVEL IN URT

4.1 TERRORIST FINANCING THREAT SCALE.

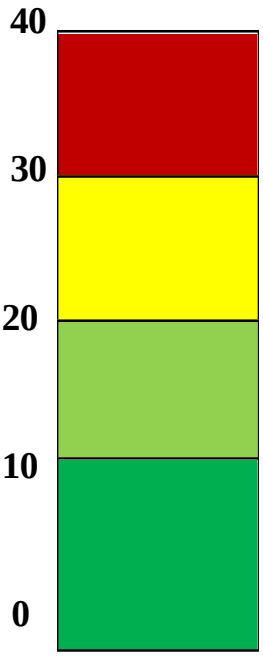


KEY:

HIGH – **40** and above
MEDIUM-HIGH **30 – 39**
MEDIUM **20 – 29**
MEDIUM-LOW **10 – 20**
LOW 0 **-9**

The Threat score is 13 as shown in Appendix 2. Therefore, the Threat is rated **MEDIUM LOW(ML)** based on the key above.

4.2 TERRORIST FINANCING VULNERABILITIES SCALE.



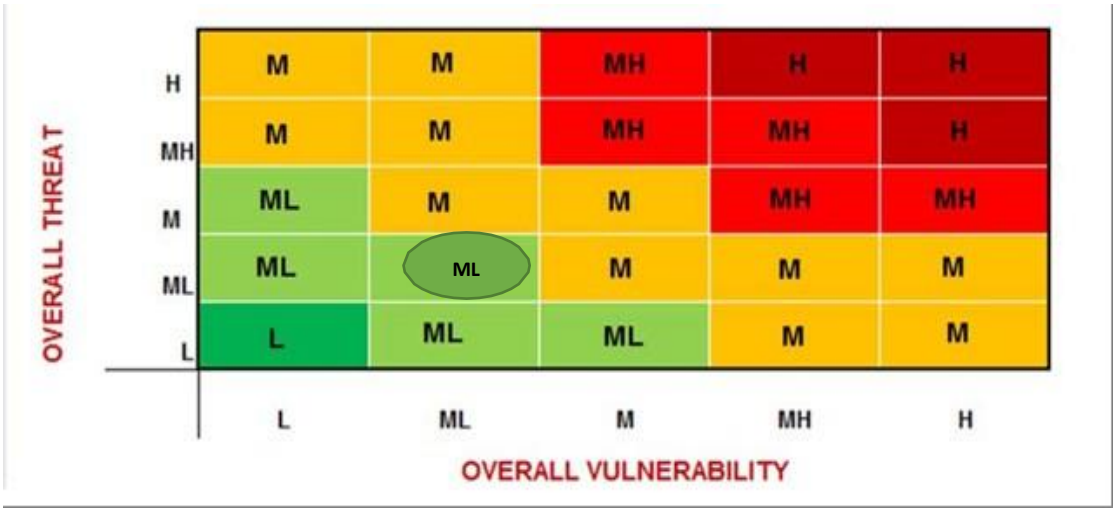
KEY:

HIGH	–	**40** and above
MEDIUM HIGH	-	**30 – 39**
MEDIUM	-	**20 – 29**
MEDIUM-LOW	-	**10 – 19**
LOW	-	**0 - 9**

Vulnerability score is 17 as shown in Appendix 2. Therefore, Vulnerability was rated as **MEDIUM LOW** (ML) based on the key above.

XY PLANE

Overall Assessment of Terrorist Financing Risk is a function of TF threat and TF vulnerability. TF threat was rated as MEDIUM LOW(ML) and TF vulnerability was also rated MEDIUM LOW(ML**). Therefore, the overall TF risk is MEDIUM LOW** (ML). This is illustrated in the diagram below.



4.3 CONCLUSION

The TF Risk Assessment in URT is ML (**Medium-low**). The assessment also noted some deficiencies. These include inadequate AML/CFT knowledge for both supervisory authorities and reporting entities especially for DNFBPs, improper distribution of the UN sanction list to the stakeholders, and competent authorities need to improve inter-agency corporations to increase effectiveness in effort against TF.

The assessment has made various recommendations that will be incorporated on the National Counter Terrorist Financing Strategy. The CTF Strategy is documented separately from this report. There are recommendations at the national level which are applicable universally, and there are recommendations at a sector level, which are applicable to specific sectors to assist both Government and other Stakeholders to prioritize their allocations of resources to mitigate TF risks.

Monitoring and Evaluation will be the responsibility of Ministries responsible for finance both in Tanzania Mainland and Zanzibar and the National Committee.

APPENDIXES

APPENDIX 1

TF risk assessment participating Institutions organizations:

1.	FIU	20.	MVTS (TCB)
2.	Bank of Tanzania (BOT)	21.	Zanzibar Law Society (ZLS)
3.	Tanzania Bankers Association (TBA).	22.	Tanganyika Law Society (TLS)
4.	Tanzania Police Force (TPF)	23.	Tanzania Revenue Authority (TRA)
5.	National Counter Terrorism Centre (NCTC)	24.	Zanzibar Revenue Authority (ZRA)
6.	National Prosecution Services (NPS).	25.	Registrar of NGO's (Mainland)
7.	Director of Public Prosecution (Zanzibar)	26.	Registrar of NGO's (Zanzibar)
8.	Director of Criminal Investigation (DCI)	27.	Registrar of Societies (MOHA)
9.	Interpol	28.	NACONGO
10.	Tanzania Intelligence and Security Services (TISS)	29.	ANGOZA
11.	Immigration Services Department	30.	RITA
12.	Ministry of Foreign Affairs.	31.	PBZ (Peoples Bank of Zanzibar)
13.	Tanzania Mining Commission	32.	Tanzania Gaming Board (TGB)
14.	BRELA	33.	Gaming Operators Representative
15.	BPRA	34.	TIRA
16.	MNO's	35.	Insurance Apex Board/ Representative
17.	Tanzania Investment Centre (TIC)	36.	CMSA
18.	Zanzibar Investment Centre (ZIPA)	37.	Capital and Securities Apex Board/ Representative
19.	Drug Control and Enforcement Authority (DCEA)	38.	Tanzania Communication Regulatory Authority (TCRA)

APPENDIX 2

MARKED QUESTIONNAIRE FOR GROUP A, B AND C
RISK ASSESSMENT ON TERRORIST FINANCING

FOCUS GROUP DISCUSSION – QUESTIONNAIRE (GROUP A)

Table: Threats

ORGANIZATION		THREATS FEATURES	Total Score
1.	FINANCIAL INTELLIGENCE UNIT (FIU)	• Does FIU receive STR with Terrorist or Terrorist Financing clues?	Yes -1
		• Does FIU disseminate Intelligence with Terrorist or Terrorist Financing clues?	Yes – 1
		• Does FIU receive Currency declarations for passengers crossing URT borders?	Yes – 0
		• Does FIU comply with FATF standard regarding sharing of information in TF?	Yes – 0
		• Does FIU have skilled personnel for TF analysis?	Yes – 0
2.	TANZANIA POLICE FORCE (TPF)	• Does TPF have MoU with counterpart institutions within a Regional and Global for exchanging/sharing information in TF/T.	Yes – 0
		• Does URT have an incidence of Organization recruiting Tanzanian Citizens to join Terrorist Groups as Foreign Terrorist fighters.	Yes – 1
		• Does TPF have skilled personnel for TF investigation?	Yes – 0
3.	IMMIGRATION DEPARTMENT OF TANZANIA	• Does URT have foreign residences from high-risk countries	Yes – 1
4.		• Does Immigration have MoU with counterpart institutions within a Regional and Global for exchanging/sharing information in TF/T.	Yes – 0

ORGANIZATION		THREATS FEATURES	Total Score
		• Does Immigration screen the foreigners requesting residence permit against United Nation sanction/Blacklisted list?	Yes – 0
		• Does URT have People who travel to High-Risk Countries?	Yes – 1
		• Does URT have foreign experts with working permit from High-Risk Countries?	Yes – 1
		• Does Immigration department have skilled personnel for TF investigation?	Yes – 0
5.	NATIONAL PROSECUTION SERVICES (NPS)	• Does URT have citizens who were prosecuted abroad for TF/T?	Yes – 1
		• Does NPS have skilled personnel for the Prosecution of TF cases?	Yes – 0
6.	NPS/DPP ZANZIBAR	• Does DPP have skilled personnel for the Prosecution of TF cases?	Yes – 0
7.	NATIONAL COUNTER-TERRORISM CENTER (NCTC)	• Does NCTC have MoU with counterpart NCTC within a regional or global for exchanging of TF information?	Yes - 0
		• Does URT have individuals returned from fighting as a Foreign Terrorist Fighter?	Yes – 1
8.	DRUGS CONTROL ENFORCEMENT AUTHORITY (DCEA)	• Do DCEA MoU with counterpart institutions within a Regional and Global for exchanging/sharing suspects information.?	Yes – 0
		• Do DCEA have an interagency relationship with other Law Enforcement Agencies?	Yes – 0
		• Do DCEA Screen names of Suspects against Blacklisted / Sanction list?	No – 1
9.	MINISTRY OF WORKS	• Does URT monitor foreign experts (from High-risk	Yes – 0

ORGANIZATION		THREATS FEATURES	Total Score
		Countries) after being granted a Work or resident permit?	
10.	MINISTRY OF FOREIGN AFFAIRS	• Do URT have neighbors Countries that have Terrorist Activities?	Yes - 0
		• Does URT have an incidence of Tanzanians Citizen to Terrorist Activities?	Yes – 1
		• Does HAWALA operate in URT	Yes – 0
11.	MINISTRY OF CONSTITUTION AFFAIRS AND LEGAL AFFAIRS	• Does NPS have MoU with counterpart NPS within a regional or global for extradition of TF suspects?	Yes - 0

Table: Vulnerabilities

S/N	ORGANIZATION	VULNERABILITY FEATURES	TOTAL SCORE
1.	NATIONAL PROSECUTION SERVICES (NPS) DPP ZANZIBAR	• Does URT criminalize TF?	Yes - 0
		• Does URT sanctions to TF offense are they proportionate and dissuasive?	Yes - 0
		• Does URT criminalize Foreign Terrorist Fighters?	Yes - 0
		• Does URT has MoU of exchanging TF suspect with Regional and Global counterparty?	Yes - 0
		• Does URT have in place a legal framework for freezing the Terrorist Asset.	Yes – 0
		• Does URT have in place a legal framework for defrizzing the frozen Assets suspected for TF.	Yes - 0
2.	FINANCIAL INTELLIGENCE UNIT (FIU)	• Does URT have law and Regulations which insist on the identification and verification	Yes - 0

S/N	ORGANIZATION	VULNERABILITY FEATURES	TOTAL SCORE
		of customers according to the risk?	
		• Does AMLA/AMLPOCA have a section in place to conduct an inspection to enforce AML/CFT Compliance.	Yes – 0
		• Does URT have Law in place which requires declaration of cash before crossing the border (CBDC).	Yes -0
3.	IMMIGRATION DEPARTMENT OF TANZANIA	• Do you have a Legal framework which allows screening the foreigners requesting residence or work permits against the sanction/Blacklisted list?	Yes - 0
4.	TANZANIA REVENUE AUTHORITY (TRA) ZANZIBAR REVENUE BOARD (ZRB)	• Does TRA submit Cross Border Declaration of Currency within seven days?	Yes - 0
5.	MINISTRY OF WORKS	• Does URT have a legal framework that allows monitoring foreign experts (from High-risk Countries) after being granted a Work or resident permit?	N0 - 0

RISK ASSESSMENT ON TERRORIST FINANCING

FOCUS GROUP DISCUSSION – QUESTIONNAIRE (GROUP B)

Table: threats

S/N	ORGANIZATION	THREAT FEATURES	TOTAL SCORE
1.	BANK OF TANZANIA (BOT)	• Does BOT have MOU with counterpart Bank within Region and Global for exchange of information related to TF.	Yes – 0
2.	GAMING BOARD OF TANZANIA (GBT)	• Does GBT vet Gaming operator CEOs against sanctioned list?	Yes – 0
3.	TANZANIA INSURANCE REGULATORY AUTHORITY (TIRA)	• Does TIRA vet the company names and CEOs against the sanctioned list before issuing a license?	Yes – 0
4.	CAPITAL MARKETS SECURITIES AUTHORITY (CMSA)	• Do CMSA vet the company names and CEOs against the sanctioned list before licensed?	Yes – 0
5.	MINISTRY OF FOREIGN AFFAIRS	• Does URT receive a sanction list from UN	Yes – 0
6.	TANZANIA COMMUNICATION REGULATOLY AUTHORITY (TCRA)	• Does TCRA have Control over registration of Sim Card.	Yes – 0
7.	PEOPLES BANK OF ZANZIBAR (PBZ)	• Does PBZ have a secured EFT services/product	Yes – 0
8.	TANZANIA COMMERCIAL BANK (TCB)	• Does TCB have secured bureau de change services	Yes – 0

Table: vulnerabilities

S/N	ORGANIZATION	VULNERABILITY FEATURES	TOTAL SCORE
1.	BANK OF TANZANIA (BOT)	• Does BOT have law in place which deter his licensee to issue Service / Product which offer anonymity?	No - 1
		• Does BOT have a legal framework to ensure secured EFT services to his licensee?	Yes -0
		• Does BOT have Legal framework which allow to conduct vetting to CEOs of the Bank?	Yes -0
2.	GAMING BOARD OF TANZANIA (GBT)	• Does GBT have law in place which deter his licensee to issue Services / Products which offer anonymity?	Yes -0
		• Does GBT have law in place for conducting vetting of Gaming operator CEO's?	Yes -0
3.	TANZANIA INSURANCE REGULATORY AUTHORITY (TIRA)	• Does TIRA have law in place which deter his licensee to issue Services / Products which offer anonymity?	No - 1
		• Does TIRA has Legal framework which allow to conduct vetting to CEOs of the Insurance Companies?	Yes -0
4.	CAPITAL MARKETS SECURITIES AUTHORITY (CMSA)	• Does CMSA have law in place which deter his licensee to issue Services / Products which offer anonymity?	No - 1
5.		• Does CMSA has Legal framework which allow to conduct vetting to CEOs of the Companies?	Yes -0

RISK ASSESSMENT ON TERRORIST FINANCING

FOCUS GROUP DISCUSSION – QUESTIONNAIRE (GROUP C)

Table Threats

SN	ORGANIZATION	THREAT FEATURES	SCORE
1	REGISTER OF NGO (Mainland)	Does registrar of NGO's screen NGOs against sanction list?	No - 1
		Does registrar of NGO's conduct target /periodic supervision and monitoring to NPO and provide reports?	Yes – 0
2.	REGISTER OF SOCIETIES (Mainland)	Does registrar of civil societies screen the leaders of civil societies against sanctioned list?	Yes – 0
		Does registrar of civil societies conduct targeted supervision and Monitoring to NPO?	No – 1
3.	REGISTER OF NGO (Zanzibar)	Does registrar of NGO's screen NGOs against sanction list?	N0 - 1
		Does registrar of NGO's conduct target /periodic supervision and monitoring to NPO and provide reports?	Yes - 0

Table: Vulnerabilities

SN	ORGANIZATION	VULNERABILIY FEATURES	SCORE
1.	Registrar of NGO Mainland	Does registrar have MoU/ Communication strategy for an interagency relationship?	Yes - 0
		Does registrar have MoU with reginal and global counter party institution?	No -1
		Do sanctions impose by registrar dissuasive and proportionate?	No – 1
		Does URT have a law/regulation that requires NGO to transact via banks?	No - 1
		Does Registrar have a legal framework that allows conducting of targeted supervision and monitoring to NPO's	Yes - 0
2	Registrar of NGO Zanzibar	Does registrar have MoU/ Communication strategy for an interagency relationship?	N0 - 1

SN	ORGANIZATION	VULNERABILIY FEATURES	SCORE
		Does registrar have MoU with reginal and global counterparty institution?	No - 1
		Do sanctions impose by registrar dissuasive and proportionate?	No - 1
		Does URT have a law/regulation that requires NGO to transact via banks?	No - 1
		Does Registrar have a legal framework that allows conducting of targeted supervision and monitoring to NPO's	N0 - 1
3	Registrar of Civil Society Mainland	Does registrar have MoU/ Communication strategy for an interagency relationship?	No – 1
		Does registrar have MoU with regional and global counter party institution?	No - 1
		Do sanctions impose by registrar dissuasive and proportionate?	No – 1
		Does URT have a law/regulation that requires NGO to transact via banks?	No -1
		Does Registrar have a legal framework that allows conducting of targeted supervision and monitoring of NPO's	No - 1
4	Business Registration and Licensing Agency (BRELA)	Does BRELA have the legal framework to access the ultimate beneficiary owners of the company	Yes – 0
5	Business Property Registration Agency (BPRA)	Does BPRA have the legal framework to access the ultimate beneficiary of the Company?	No - 1
6	Registration Insolvency and Trusteeship Agency (RITA)	Does RITA have the legal framework to access the ultimate beneficiary owners of the trustee	Yes - 0