Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions

December 2021

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

Cover Photo: iStockphoto.com/metamorworks

December 2021

Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of the Security Council resolutions

DECEMBER 2021

Table of Contents

I. Background and methodology

With reference to Security Council resolution 2395 (2017), Security Council resolution 2462 (2019), paragraph 35, requests the Counter-Terrorism Committee Executive Directorate (CTED) to strengthen its assessment process relating to countering the financing of terrorism (CFT), including through targeted and focused follow-up visits as complements to its comprehensive assessments and to provide, annually, on the basis of its reporting and in consultation with the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and the Taliban and associated individuals and entities, to the United Nations Office on Counter Terrorism (UNOCT), through the Counter-Terrorism Committee, a thematic summary assessment of gaps identified and areas requiring more action to implement key CFT provisions of relevant Security Council resolutions for the purpose of designing targeted technical assistance and capacity-building efforts and taking into account, as appropriate, mutual evaluation reports of the Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs).

Pursuant to paragraph 37 of resolution 2462 (2019), CTED and the Monitoring Team prepared a joint report on actions taken by Member States to disrupt terrorism financing, which was issued in June 2020.[1]

Considering that a second report drafted in the same year, pursuant to paragraph 35 of resolution 2462 (2019), would not be able to provide sufficient updated information, and in view of the challenges posed by the COVID-19 pandemic, the Chair of the Counter-Terrorism Committee informed the President of the Security Council on 31 December 2020, following consultations with Committee Members, that CTED would prepare the first annual thematic summary assessment required pursuant to the aforementioned paragraph during 2021.[2]

Because of the ongoing restrictions relating to the COVID-19 pandemic, CTED was unable to conduct, on the Committee's behalf, targeted and focused follow-up visits on CFT. However, it ensured that CFT-related matters were addressed with sufficient detail and expertise within the framework of the virtual components of the visits conducted in accordance with the Committee's decision to conduct hybrid visits to some Member States *pro tempore*. During 2021, CTED conducted 13 virtual components of hybrid visits, of which 12 contained dedicated CFT sessions. Because the physical components of those visits have not yet been conducted, including to discuss in further detail the operational aspects of the CFT measures

1 S/2020/493

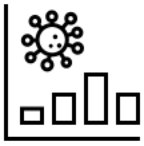
2 S/AC.40/2020/OC.137.

in place, the gaps listed in the present report are based on preliminary findings and are not attributed to specific States. However, additional country-specific elements of CTED's preliminary analysis can be made available to UNOCT, upon request, to substantiate the findings relating to any particular gap.

The present summary assessment builds upon the information gathered during the above-mentioned visits, ongoing analysis of terrorism-financing trends and threats, CFT-related events organized or attended by CTED throughout the year (including its participation in the relevant analytical projects of FATF), as well as inputs provided by the Monitoring Team and gathered from available FATF/FSRB mutual evaluation reports, as appropriate.

As requested by the Council in its resolution 2462 (2019), the present summary assessment focuses on priority gaps and areas requiring further action in which Member States would benefit from technical assistance or specialized expertise. Furthermore, given the need to adjust the work programmes for the hybrid visits to the country-specific context and priorities, not all sub-topics were discussed with all 12 States concerned in equal detail. Consequently, the list of identified shortcomings is not exhaustive.

II. Gaps in understanding terrorism-financing risks



Security Council resolution 2462 (2019) introduces new requirements with respect to regular assessments of terrorism-financing risk to which Member States are exposed. It specifically calls on Member States to identify economic sectors most vulnerable to the financing of terrorism, including non-financial services (such as, for example, the construction, commodities, and pharmaceutical sectors). States should also consider and assess risks associated with specific products and payment methods, including the use and cross-border transportation of cash and bearer negotiable instruments (BNI), as well as other financial products, including value stored and prepaid cards and informal value transfer system providers (e.g., hawala), virtual assets and new financial instruments (including crowdfunding platforms). Member States are also called upon to continue to conduct research and collect information to enhance knowledge of, and better understand, the nature and scope of the linkages that may exist between terrorism and organized crime, whether domestic or transnational.

The following priority gaps were identified during the reporting period:

- *No anti-money-laundering/countering the financing of terrorism (AML/CFT) national risk assessment (NRA)* conducted. Member States that have not yet conducted or completed an AML/CFT NRA have insufficient understanding of the risks to be addressed in order to detect and prevent terrorism financing. Even though assistance (including methodologies) is available from several partners (including the International Monetary Fund (IMF), the World Bank, and the United Nations Office on Drugs and Crime (UNODC)), States are not sufficiently proactive in managing these processes and/or lack the requisite resources and coordination mechanisms to conduct an NRA. In cases where the NRA takes several years, the conclusions reached may be outdated by the time of their adoption and dissemination, and even more so by the time that they are reflected in strategies or action plans developed to mitigate the risks.
- *Insufficient scope of analysed threats, risks and vulnerabilities.* Recently completed or updated AML/CFT NRAs often lack analysis of the following elements:
- Risks and vulnerabilities related to financing of terrorism based on xenophobia, racism, and other forms of intolerance.
- Risks and vulnerabilities of specific sectors or payment modes (e.g., misuse of alternative remittance systems (ARS), risks deriving from limited control of cross border cash couriers, or risks deriving from the use of new financial instruments, including virtual assets and crowdfunding platforms.

- Vulnerabilities of economic sectors beyond those represented by AML/CFT reporting entities, including but not limited to non-financial services such as, inter alia, the construction, commodities, and pharmaceutical sectors.
- Terrorism-financing risks linked with the proceeds of transnational organized crime.
- Gender-specific considerations and implications with respect to terrorism-financing risks and CFT measures.

The following are examples of technical assistance recommended during the reporting period:

- Provide support for the conducting/completion of an AML/CFT NRA, including the necessary tools.

III. Gaps in the criminalization of terrorism financing

Security Council resolutions 1373 (2001), 2178 (2014), 2253 (2015), 2368 (2017), 2396 (2017) and 2462 (2019) call upon States to criminalize the financing of terrorism for any reason, including, but not limited to, recruitment, training or travel, even if there is no link to a specific terrorist act. Council resolution 2341 (2017) contains additional provisions on the financing of terrorist attacks aimed at destroying critical infrastructure or rendering it unusable.

In this regard, the following priority gaps were identified during the reporting period:

- *Financing of terrorism "for any purposes" is not adequately covered*. In some States, the definition of the terrorism-financing offence does not extend to wilful financing of terrorist organizations and/or individual terrorists for any purpose.
- *Financing of foreign terrorist fighter (FTF) travel is not explicitly criminalized*. A number of States do not define the terrorism-financing offence to explicitly cover the financing of travel for the purpose of committing, organizing, preparing or preparing terrorist acts, or for the purpose of participating in them or providing or receiving training in terrorism.
- *Collection of funds is not sufficiently covered*. A number of terrorism-financing offences reviewed during the reporting period either do not cover or do not sufficiently cover the collection of funds, including indirect collection.
- Definition of funds is not sufficiently broad. Some States have not specified in their legislation that the terrorism-financing offence should cover economic

resources of any kind and not be limited to financial assets. This shortcoming is of particular concern with respect to cases of terrorism financing through exploitation of oil and other natural resources.

The following are examples of technical assistance recommended during the reporting period:

- Provide expert support for the revision of legal and regulatory framework on AML/CFT.

IV. Gaps in the use of financial intelligence to support terrorism-financing investigations and prosecutions

Council resolutions 2462 (2019) and 2482 (2019) highlight the value of financial intelligence and financial investigations in counter-terrorism and include new and focused requirements in this regard. Council resolution 2462 (2019) also calls for strengthening frameworks allowing competent national authorities, in particular financial intelligence units (FIUs), intelligence services, law enforcement agencies, prosecutorial and/or judicial authorities, to gather and share information on the financing of terrorism; as well as to accelerate the timely exchange of relevant operational information and financial intelligence of terrorist networks, including FTFs and FTF returnees and relocators. The resolution further requires Member States to ensure that designated law enforcement authorities have responsibility for terrorism-financing investigations within their national CFT framework. In accordance with resolution 2462 (2019), there should be a proactive financial-investigation component in all terrorism-related investigations and when conducting investigations into the financing of terrorism.

In this regard, the following priority gaps were identified during the reporting period:

- *Low number of successful prosecutions on terrorism financing charges.* Although most Member States have the required elements in their legislation, many of them choose not to investigate or prosecute terrorism-financing charges, especially where there is no apparent link to a specific terrorist act. In this regard, they have referred to, in particular, challenges in proving the required knowledge or intent and would opt for alternative charges. Strategic choices not to prosecute instances of terrorism financing that does not represent a serious imminent threat (e.g., a one-off transfer of funds to family members for basic needs) do not

necessarily constitute gaps as such, provided that other effective measures are in place to monitor and prevent any further abuses. However, in several States, the number and nature of prosecuted terrorism-financing cases do not appear to commensurate with their respective risk profiles, which point to more frequent and diverse terrorism-financing occurrences.

- *No legal basis or practice for financial investigations to be systematically conducted in parallel to terrorism cases*. Several States have not ensured that there is a proactive financial investigation component in all terrorism-related investigations. Addressing this gap also involves enhancing the use of special investigative techniques and, where appropriate, mutual legal assistance (MLA) channels.
- *Insufficient powers of FIUs*. In one Member State, the FIU does not have direct access to the financial information of its nationals and is not mandated to request additional information from reporting entities. There are also significant limitations on the information that this FIU can disclose to other national authorities.
- *Insufficient operational and/or analytical capacity of FIUs*. Several FIUs lack the required software to analyse transactions and other information provided by reporting entities. A number of States need to complete the automatization of communication and reporting channels between entities subject to financial monitoring, supervisory authorities, and the FIU. States should provide more capacity-building and training opportunities on the investigation and prosecution of terrorism financing for relevant law-enforcement, prosecutorial and judicial authorities, as well as the relevant FIU experts.
- *Gaps in inter-agency cooperation*. Based on the available statistics, very few terrorism financing related reports submitted by FIUs to relevant law enforcement authorities trigger further action, including criminal investigations. Some States do not have mechanisms or practices in place allowing the authorities in receipt of such reports to provide feedback to the FIU with respect to any shortcomings in their report. Feedback on the information provided by each agency and other similar mechanisms to debrief the relevant authorities on outcomes of the conducted investigations would also serve to enhance the relevant authorities' overall understanding of terrorism-financing trends and enhance the quality of information they provide to each other.
- *Absence of, or insufficient, safeguards to allow for financial intelligence to be effectively converted into evidence that can be used to secure terrorism-financing convictions*. Many States' FIUs do not have any particular measures in place to ensure that the information that they disseminate to law enforcement agencies is collected, processed and communicated with the necessary safeguards (including, e.g., with respect to privacy and data protection that would not impede its subsequent conversion and use as evidence in criminal cases). There is often insufficient information regarding the measures in place to enable law enforcement to generate admissible evidence based on the financial intelligence.
- *Insufficient channels for effective cooperation with foreign counterparts*. Some FIUs engage in a low level of international cooperation with foreign counterparts in the absence of formal bilateral memorandums of understanding, especially if they are not members of international or regional cooperation networks.

The following are examples of technical assistance recommended during the reporting period:

- Provide training to relevant judiciary, prosecutorial and investigative authorities on money-laundering/terrorism financing investigations and prosecutions, including through joint programmes that would include the FIU experts, and strengthen inter-agency cooperation, including with reference to the FATF 2021 Guidance on Investigating and Prosecuting Terrorism Financing.
- Facilitate the exchange of experiences with other Member States on enhancing cooperation between the FIU, law enforcement agencies, and prosecutorial and judicial authorities on CFT.
- Provide training for the relevant authorities on how to perform data forensics with respect to digital terrorism-financing methods.
- Strengthen the capacities of all relevant authorities involved in CFT (including law enforcement and customs authorities), in particular with respect to enhancing the use and integration of financial intelligence in terrorism-related investigations.
- Support the provision of software and other relevant tools to automate transactions analysis reporting for all entities subject to financial monitoring, including designated non-financial businesses and professions (DNFBPs), and provide training aimed at strengthening the relevant capacities of the FIU, law enforcement agencies and reporting entities to identify and process suspicions of terrorism financing.
- Provide assistance in developing a system for processing operational financial information and intelligence, including relevant software to analyse transactions in the FIU.

V. Gaps relating to AML/CFT supervision

Insufficient tools and knowledge available to reporting entities. Most States need to make additional efforts to support and equip their reporting entities outside the formal financial sector (including DNFBPs), including with respect to their awareness of prevalent terrorism-financing risks, trends and mitigation measures (notably through communication of updates on terrorism-financing risk indicators); reporting requirements; and tools available for effective communication, searches and checks. Several States would benefit from technical assistance in this regard.

VI. Gaps relating to asset-freezing mechanisms

Council resolution 2462 (2019) stresses the need for effective implementation of asset-freezing mechanisms pursuant to Council resolution 1373 (2001), including considering third-party requests from other States. The resolution also calls on States to invest resources in the implementation of sanctions regimes pursuant to resolutions 1373 (2001), 1267 (1999), 1989 (2011) and 2253 (2015), and in seizure of funds in the course of investigations.

In this regard, the following gaps were identified during the reporting period:

- *Inadequate legislative framework for implementing asset-freezing measures pursuant to resolution 1373 (2001)*. Several States do not have clear legislation establishing a national mechanism to identify targets for national designations or defining the competent authority responsible for making, compiling and maintaining the designation of individuals or entities involved in terrorist activity. At least one State has no explicit procedures to identify targets and determine whether to designate.
- *National designation and freezing mechanisms exist but are underused or not sufficiently operationalized*. Several States rely exclusively on the supranational designation process and do not have any national designation process and have not submitted proposals for listings at the supranational level. Other States have not made any national designations at all in the past three years, despite having investigated and prosecuted terrorism and terrorism-financing cases. Some, but not all of these gaps are explained by the use of other post-conviction mechanisms (forfeiture) or by strategic choices with reference to low threat (e.g., where the convicted individuals had low incomes). In most States with deficient freezing mechanisms, there is no mechanism for communicating delisting and guidance on the obligation to comply with unfreezing measures.
- *Gaps in reviewing national designations and/or in de-listing procedures*. Several States do not periodically review their designation lists to ensure that they are up to date (including as new investigations into terrorism cases are conducted) and contain the names of persons or entities whose designation is no longer justified. At least one State that has a national freezing mechanism in place does not have publicly known review request or de-listing procedures. Delays in periodic reviews also occur in States that have legislative provisions providing for such reviews at least on a biannual basis.
- *Insufficient information is provided to the designated entities or persons*. Reasonable efforts should be made to inform the designated person or entity as soon as possible after the designation or freezing has taken effect. The contents of notice should include the fact of designation and its implications; review procedure and information on de-listing processes, including the contacts of

the competent authorities; summary of reasons for designation (unclassified); and procedures for requesting access to funds for basic needs, work payment authorization, etc.

- *Gaps in implementing freezing requests from third States or making such requests*. In some States, there no formal procedures in place with regard to direct foreign request to take freezing action pursuant to resolution 1373 (2001). Some States rely exclusively on supranational channels of communication. At least one State has no legal provision to request other States to freeze assets at its request.
- *Gaps in operational capacities of the relevant authorities and reporting entities (especially outside the formal banking sector) to implement freezing measures effectively and without delay*. Several States lack any mechanism for automating relevant searches and processes (especially for reporting entities outside the formal banking sector) and do not provide sufficient training or guidance to the private sector.
- *Challenges in freezing virtual assets*. In those States where the legal framework contains provisions on both national freezing mechanisms and AML/CFT requirements for virtual assets and service providers, there are no impediments in principle for virtual assets to be frozen. However, very few have practical experience or a clear understanding of how to implement such measures in practice.

The following are examples of technical assistance recommended during the reporting period:

- Support the development of a regulatory framework and help operationalize the national asset-freezing mechanism pursuant to resolution 1373 (2001).
- Support the provision of software and other relevant tools to automate checks against sanctions lists used for asset-freezing for all entities subject to financial monitoring, including DNFBPs.

VII. Gaps in preventing the terrorist abuse of money value transfer services (MVTS) or informal financial networks

Council resolution 2462 (2019) explicitly mentions abuse of legitimate businesses (including emerging payment methods, such as prepaid cards and mobile payments or virtual assets, and innovative financial technologies) for terrorism-financing purposes (*see also section VIII, below*).

In its Twenty-eighth report submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities,[3] the Monitoring Team notes that MVTS and hawala channels remain among the primary methods for sending and receiving funds for terrorist groups in several regions, as well as for ISIL fighters and their families in Syrian detention facilities or camps. At least three Member States with advanced AML/CFT frameworks visited by the Committee during the reporting period highlighted the challenges that they faced with respect to detecting terrorism-financing abuse of MVTS and hawala-like systems. The economies of several other States visited during the reporting period rely heavily on cash and thus face even higher risks relating to ARS and physical transportation of money by cash couriers. Those States' economies are characterized by the prevalence of informal sectors that often operate outside the regulatory framework in place.

In this regard, the following gaps were identified during the reporting period:

- *No risk assessment or insufficient risk assessment conducted with respect to new payment methods and financial instruments.* Several States located in regions where the use of new payment methods (prepaid cards, mobile phone payments, "mobile money", etc.) has rapidly increased in recent years, including to respond to challenges related to the financial exclusion and certain COVID-19 impact, lag behind in conducting adequate risk assessments relating to possible terrorism-financing abuse and vulnerabilities, and as such have significant gaps in legislative and operational responses to such risks.
- *Low compliance with preventative AML/CFT measures.* Some States experience low levels of compliance with preventative measures, including for example in the case of transfers via mobile phones by clients without a banking account) and do not impose a threshold amount of electronic assets for certain categories of users. One State, where "electronic money" is allowed and can be registered, does not extend AML/CFT reporting obligations to such services relying primarily on corresponding banking institutions used at the time of cashing out.
- *Insufficient operational measures and/or capacity to effectively detect and prevent the use of hawala-like systems for terrorism financing purposes.* Several States noted the challenges they face to identify cases of abuse of hawala systems to transfer funds intended for terrorist purposes and requested technical assistance in this regard.

The following are examples of technical assistance recommended during the reporting period:

- Support the identification and evaluation of ML/TF risks that can emanate from the development of new payment products and the use of new technologies.
- Provide training for the relevant authorities on how to identify, trace and counter the use of digital terrorism-financing methods.

3 S/2021/655, paras, 55, 67, 69.

- Enhance the capacity of relevant authorities to detect and prevent the use of informal MVTS, including hawala-type systems, for terrorism-financing purposes.

VIII. Gaps in addressing terrorism financing risks related to virtual assets and crowdfunding platforms

In its above-mentioned report,[4] the Monitoring Team highlights concerns about growth in the use of cryptocurrencies by terrorists and an evolution in tactics, which now include training in how to send funds using certain privacy-enhancing methods. It also notes concerns regarding suspicious transactions involving so-called neobanks (banks that operate exclusively online) used for transferring large sums in support of ISIL and Al-Qaida supporters in Europe and abroad. These financial institutions reportedly lack effective sanctions-screening capabilities and are used by malign actors who seek to evade counter-terrorism sanctions listings that may differ across jurisdictions.

Crowdfunding has become particularly popular over the past decade and is often associated with social media networks and other online communication methods. Although it is an entirely legitimate way of obtaining funding from masses of donors, various terrorist groups have used it widely as a fundraising model.[5] This method may receive further prominence with an increasing use of virtual assets, which in many cases enable the financier to maintain pseudonymity.

Council resolution 2462 (2019) calls on States to enhance the traceability and transparency of financial transactions, including through assessing and addressing potential risks associated with virtual assets and new financial instruments, including crowdfunding platforms, that may be abused for terrorism-financing purposes, ensuring that they are subject to AML/CFT obligations. It further encourages all States to apply risk-based AML/CFT regulations to virtual asset service providers (VASPs) and to identify effective systems to conduct risk-based monitoring or supervision of VASPs.

4 S/2021/655, paras. 70-71.

5 See *e.g.,* S/2021/655, para. 66, which notes the use of social media, including crowdfunding websites, to reach audiences beyond the region and collect donations from sympathizers, family members and friends of ISIL supporters in camps.

In this regard, the following gaps were identified during the reporting period:

- *No risk assessment or insufficient risk assessment*. Although several States have taken steps to evaluate the risks associated with virtual assets and VASPs, many are still at the preliminary stages of such assessments. Most States have not assessed potential terrorism-financing risks associated with crowdfunding platforms.
- *Virtual assets are neither regulated nor effectively prohibited*. In the absence of national or supranational provisions explicitly prohibiting the use of virtual assets, some States rely on statements of relevant officials to suggest that the circulation of such assets is not allowed in the State or region. One State has no regulations in place with respect to virtual currencies and considers operations in such currencies to be prohibited, even though several instances of their use by national entrepreneurs have been reported. One State only allows and regulates non-resident VASPs, while prohibiting them for residents. As clarified in the above-mentioned FATF Guidance, jurisdictions that do not consider that they can effectively regulate VASPs should consider prohibiting VASPs through law and effectively enforce the prohibition while they develop the required expertise to regulate and monitor them, so that they do not become a safe haven for unregulated VASPs.
- *Inadequate regulatory frameworks*. Several States are only developing or have only partially developed regulatory frameworks for virtual assets and VASPs. Having recently introduced AML/CFT regulatory framework for VASPs, one State has observed an ongoing shrinking of the sector, in contrast to global and regional trends, which may be an indication of over-regulation or gaps in the implementation of a risk-based approach. Although relatively advanced in regulation and supervision, some States need to address gaps relating to their current definitions of virtual assets and VASPs, particularly in light of the recent revision of the related FATF Standards.
- *Crowdfunding platforms are not subject to AML/CFT regulation*. Several States have not extended their AML/CFT frameworks to crowdfunding platforms, although some have taken steps to introduce licensing or registration requirements and/or designated competent authorities to monitor these services for criminal abuse more broadly.
- *Insufficient guidance to reporting entities, including registered VASPs*. Several States have taken few or no measures to equip their reporting entities with the knowledge and tools required to prevent terrorism-financing abuse. Such measures should include guidance on "red flag" indicators with respect to virtual assets, on documentation required for registration of VASPs and reporting requirements, as well as on platforms for related public-private discussions.

The following are examples of technical assistance recommended during the reporting period:

- Assistance with drafting and enacting an AML/CFT regulatory framework with respect to virtual assets and VASPs and with the implementation of risk-based monitoring and supervision.

- Facilitate the exchange of experiences with other jurisdictions on how to successfully assess, regulate, and supervise new and emerging payment services for AML/CFT purposes, including virtual assets and VASPs, as well as crowdfunding platforms.

IX. Gaps in preventing the use of cash couriers for terrorism-financing purposes

Council resolution 2462 (2019) calls upon Member States to assess the risks associated with the use of cash and BNI, including the risk of illicit cross-border transportation of cash, as well as to strengthen cross-border cooperation between customs and tax administrations and improve the coordination of international police and customs operations. In its above-mentioned report, the Monitoring Team also notes the use of FTF returnees as cash couriers to fund ISIL cells in Africa, as well as to send funds to ISIL fighters and their families in Syrian detention facilities or camps.[6]

Although in the case of most hybrid visits conducted by the Committee in 2021 it was decided to address this topic during the visits' physical, rather than virtual, components, the following gaps were identified during the reporting period in this regard:

- *No risk assessment*. Some States have not assessed the terrorism-financing risks associated with the use of cash and BNI.
- *Insufficient inter-agency cooperation*. Most States have legal and operational measures in place requiring the customs authorities to submit the relevant information to the FIU (in particular, declarations of cash and BNI) or, in case of suspicion of terrorism financing, the competent law enforcement authorities for further analysis and, if appropriate, investigation. However, there are rarely any mechanisms in place for customs to receive feedback on actions taken based on the information they provide.
- *No sanctions for false declarations*. At least one State lacks any legal provisions imposing sanctions for false declaration or false communication in relation to the physical transportation of case or BNI.

6 S/2021/655, paras. 9, 69.

The following are examples of technical assistance recommended during the reporting period:

- Enhance the capacity of the relevant authorities to detect and prevent the use of informal MVTS, including hawala-type systems, for terrorism-financing purposes.

X. Gaps relating to preventing abuse of the non-profit organization (NPO) sector for terrorism-financing purposes

Council resolution 2462 (2019) explicitly recognizes the vital role played by NPOs in national economies and social systems and encourages Member States to work cooperatively with the NPO sector to prevent the abuse of such organizations by terrorists and their supporters, while recalling that States must respect human rights and fundamental freedoms. The resolution also calls on Member States to periodically conduct a risk assessment of their NPO sectors or update existing assessments to determine the organizations particularly vulnerable to terrorism financing and to inform the implementation of a risk-based approach.

In its Twenty-eight report, the Monitoring Team notes concerns regarding abuse of the charitable or non-profit sectors in South-East Asia by ISIL affiliates and their supporters, including through collecting donations under the guise of supporting natural disaster relief. The funds raised were channelled to the Abu Ahmed Foundation, which used them to support an entity in the Syrian Arab Republic known for training FTFs.[7]

In this regard, the following gaps were identified during the reporting period:

- *No risk assessment of the sector.* Some States have not conducted or completed a sectorial risk assessment that would allow them to identify the nature of the terrorism-financing threat faced by NPOs at risk and evaluate whether the legal framework in place adequately and proportionally addresses risks associated with each type of NPO without unduly restricting their work. Such review of the NPO sector should identify which subset of organizations fall within the

7 S/2021/655, para. 63.

FATF definition of NPO[8] and then identify which NPOs in the subset would be considered higher risk for terrorism financing abuse. One State, which has taken commendable measures review the NPO sector risks and develop measures to mitigate identified risks, has not extended its evaluation to religious organizations registered therein.

- *No mechanism in place to ensure the implementation of targeted risk-based monitoring or supervision of the NPO sector.* Proportionate, risk-based supervision or monitoring is an integral part of an effective approach to protecting the NPO sector from terrorism-financing abuse. Yet, several States have not put such measures in place,[9] including but not limited to designating the competent authority for their implementation. Any such mitigation measures should be commensurate (i.e., proportionate) with the risks identified through a domestic review of the NPO sector and the understanding of the risks in the sector, avoiding CFT regulatory measures that disproportionately affect or burden NPOs with little to no terrorism-financing risk.
- *Insufficient outreach to the NPO sector.* Several States need to further enhance their efforts to raise awareness and sensitize the relevant NPOs and donor communities to the potential vulnerabilities of NPOs to terrorism-financing abuse and the measures to be taken to protect themselves from such abuse. States should also enhance their efforts to meaningfully involve their NPO sectors in the conduct of the sectorial risk assessment and the development of risk-based targeted measures to prevent abuse for the purpose of terrorism financing.

The following are examples of technical assistance recommended during the reporting period:

- Provide support (including through facilitation of experiences exchanges with other Member States) for the evaluation of the NPO sector to identify the subsets that fall under the related FATF definition and, due to their activities or characteristics, are potentially vulnerable to terrorism-financing abuse.
- Facilitate the exchange of experiences and provide training to the relevant authorities on the implementation of the risk-based approach to regulating and monitoring the NPO sector.

8 The FATF defines an NPO as "a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"".

9 Non-profit organizations may, for instance, be licensed and registered, issue annual financial statements on their income and expenditure, have appropriate controls in place, and make publicly available relevant information about their objectives, control, and management.

XI. Gaps in taking into account the potential effect of CFT measures on exclusively humanitarian activities

Council resolution 2462 (2019) calls on all Member States, when designing and applying measures to counter the financing of terrorism, to take into account the potential effects of those measures on exclusively humanitarian activities that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law.

Nine of the twelve States did not cite any dedicated measures in place to comply with this requirement. As noted in the Committee's Global survey of the implementation of Security Council resolution 1373 (2001) and other relevant resolutions by Member States (S/2021/972) and the above-mentioned 2020 joint report of CTED and the Monitoring Team, States could consider, inter alia, establishing consultation mechanisms for the Government, financial institutions, NPOs and humanitarian actors to improve their common understanding of terrorism-financing risks and ways to mitigate any potentially negative impact of CFT measures on exclusively humanitarian activity, including through strengthening the transparency of licensing and specific exemption measures.

XII. Gaps in analysing and detecting links between organized crime and terrorism financing

Several Security Council resolutions (including resolutions 2388 (2017), 2462 (2019) and 2482 (2019)) call upon Member States to increase their capacity to conduct proactive financial investigations to identify potential linkages between organized crime, such as human trafficking, and terrorism financing. Council resolution 2482 (2019) acknowledges that the nature and scope of such linkages vary by context and highlights the need to coordinate efforts at the local, national, regional, subregional and international levels to respond to this challenge.

In its above-mentioned report, the Monitoring Team also highlights several relevant examples in this regard, including attacks against artisanal gold sites, exploitation of natural resources (notably oil), cattle rustling, kidnaping for ransom, looting, arson, extortion raids, as well as opportunistic links between terrorist and criminal groups such as supplying with motorcycles and weapons.[10]

Although some States have identified instances of linkages, most do not have legal frameworks, practices or resources in place to seek proactively and systematically to establish them and investigate whether the proceeds of relevant organized crime cases were intended (or used) for terrorism financing. Financial investigations conducted in parallel with investigations into predicate offences, such as human trafficking, migrant smuggling, and trade of illicit weapons would continuously enhance the capacities of the relevant authorities to better understand the nature and scope of the linkages that may exist between organized crime and terrorism, including its financing. It is important to continuously enhance the capacity of the relevant practitioners to detect and deter such links, including by analysing regional trends and experience of other States in this regard. States should also conduct targeted research and continuously collect information to enhance their understanding of the nature and scope of such linkages to inform a strategic approach to disrupting them.

The following are examples of technical assistance recommended during the reporting period:

- Provide training and other forms of assistance to enhance the capacity of the relevant authorities to detect and deter links between terrorism, its financing and organized crime, including human trafficking, illegal trade in weapons, drugs or cultural property.
- Support the establishment of platforms and partnerships to allow for proactive and effective consideration of potential links between organized crime and terrorism financing, including through parallel investigations, strategic research and analysis.

10 S/2021/655.

XIII. Highlights and Conclusions

Most States are generally aware of the terrorism-financing threats emanating from United Nations-designated transnational terrorist groups such as ISIL and Al-Qaida and associated entities, as well as from certain local groups designated pursuant to their national sanctions regimes. However, insufficient progress has been made in analysing the other evolving risks relating, for example, to the financing of terrorism based on xenophobia, racism and other forms of intolerance. Almost no States have adequately assessed, at the strategic level, the risk that terrorists may benefit from the financial proceeds of transnational organized crime. Moreover, many States do not consider the gender-specific implications of terrorism-financing and CFT measures and rarely evaluate the vulnerabilities of non-financial economic sectors such as the construction or pharmaceutical sectors, as noted by the Council in its resolution 2462 (2019).

The gaps identified by CTED in States' criminalization of terrorism financing often relate to the financing of FTF travel and to the failure to provide for a definition of funds that covers economic resources of any kind and is not limited to financial assets. However, the biggest challenge appears to be ensuring effective investigation and, as appropriate, prosecution of terrorism financing based on the required mental elements of the offence, especially in cases where such financing is not linked to any particular terrorist act.

In order to keep pace with the rapid evolution in financial tools and terrorism-financing methods, there is an urgent need to enhance the specialized expertise of personnel engaged in handling increasingly complex cases that involve advanced investigation techniques and complex international cooperation mechanisms. The key obstacles to the detection, investigation and prosecution of cases that involve misuse of social media and encrypted messaging platforms for terrorism-financing purposes relate to the sheer volume of social media services, user accounts, and social media usage; the difficulty of tracing and identifying the individuals involved; the complexities involved in the analysis of digital forensic evidence; and the transnational nature of procedures for obtaining evidence. Many States are also encountering challenges in their efforts to address the risks associated with cryptocurrencies and other emerging payment technologies, either leaving them in under-regulated "grey zones" or over-regulating them, thus curtailing the opportunities offered by that sector in terms of financial innovation and efficiency.

Many States also continue to face challenges with respect to the integration of human rights obligations into CFT measures and cooperation with civil society actors in developing policies to ensure risk-based supervision of the non-profit sector. As reflected in Section XI above, only a few States have adopted dedicated measures to evaluate, and eventually mitigate, the impact of CFT measures on

exclusively humanitarian activities, including in conflict zones with active terrorist activity[11].

CTED will continue to work closely on monitoring and supporting Member States' efforts to implement the requirements of the relevant international instruments, including the relevant Security Council and General Assembly resolutions, on the prevention and suppression of terrorism financing, as well as good practice standards and recommendations developed by FATF, while ensuring compliance with their obligations under international human rights law, international humanitarian law, and international refugee law. The Security Council Guiding Principles on Foreign Terrorist Fighters: the 2015 Madrid Guiding Principles + 2018 Addendum (S/2015/939 and S/2018/1177); CTED's Technical Guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions (S/2019/998); the Framework document for Counter-Terrorism Committee visits to Member States aimed at monitoring, promoting and facilitating the implementation of Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017), 2462 (2019) and 2482 (2019) and other relevant Council resolutions (S/2020/731); and CTED's recently enhanced stocktaking tools serve as useful references for CTED's continued engagement with all relevant stakeholders in this regard, including the related capacity-building efforts.

11 See Section XI above.

https://www.un.org/securitycouncil/ctc/

@UN_CTED @UnitedNationsCTED @un_cted

cted@un.org