2021

EXECUTIVE SUMMARY

ANTI-MONEY LAUNDERING COUNCIL

Caveat

This risk assessment is an update to the Second National Risk Assessment (NRA), specifically on the understanding and assessment of terrorism and terrorism financing (TF) risks in the Philippines. It also intends to determine the direction of risks based on the emerging and current issues as well as significant developments and progress done domestically and internationally, relative to the combating terrorism and its financing.

The risk assessment uses both quantitative and qualitative approaches in gauging associated risks relative to TF and terrorism. Data and information are sourced from transaction reports submitted to Anti-Money Laundering Council (AMLC); statistics and information provided by law enforcement and intelligence agencies; and published articles and studies.

The document also serves as a guidance paper for financial institutions (FIs) and law enforcement agencies (LEAs), specifically as regards their risk-based strategies. Suspicious financial indicators and triggers as well as case typologies presented in this study may aid in the identification, detection, and investigation of possible financial transactions linked to terrorism and TF.

Lastly, the document presents existing challenges that FIs, LEAs, and supervisory agencies are facing, relative to the identification and investigation of the money trail associated with terrorism and TF.

EXECUTIVE SUMMARY

The Mutual Evaluation Report (MER), which was adopted by the Asia/Pacific Group on Money Laundering (APG)[1] in August 2019, identified certain deficiencies on the assessment of threats posed by the presence and movement of foreign terrorist fighters (FTFs) in the Philippines, as well as the mixed understanding of terrorism and TF risks across all sectors. One of the noted deficiencies in the MER is on the implementation of TF-related targeted financial sanctions (TFS), which is a concern for various covered persons (CPs).[2] Also, the MER stated the lack of false positive freezing actions among FIs, relative to transactions associated with TF.

The 2019 MER further recommended that the Philippines must continuously update assessments on TF risks to enhance the understanding of emerging typologies of TF in the country, noting the following essential items:

1. Terrorism and TF cases and related events;
2. Role of FTFs as regards the activities relative to terrorism in the country;
3. Impact of Philippines' government/military responses to TF networks; and
4. Changes in the threat environment, particularly to terrorism and TF.

The Philippines, in its commitment to combat terrorism and its financing, responded to the need to establish a comprehensive legal framework for the implementation of United Nations Security Council Resolution (UNSCR) 1373 *ex parte* through the Anti-Terrorism Act of 2020 (ATA) in July 2020. This further strengthens the legal framework, alongside Republic Act No. 10168 or the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA).

The study, which is undertaken by the AMLC, with the support of the National AML/CFT Coordinating Committee – Terrorism Financing/Proliferation Financing Subcommittee (NACC-TFPFSC), utilizes the standard risk framework and the guidance of the Financial Action Task Force (FATF) on TF risk assessment. The estimates of likelihood are based on a combined assessment of the threat and vulnerability of a channel to TF activity.

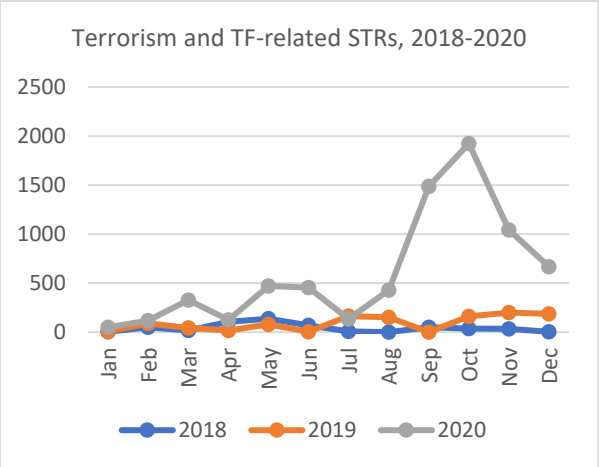
The assessments and rating are purely based on qualitative and descriptive approaches and are based on major documents published: (1) 2017 NRA of the Philippines; (2) Third MER of the Philippines; (3) 2017 to 2019 Reports of the National Police Organization for the Association of South East Asian Nations (ASEANAPOL); (4) various AMLC studies and strategic reports; and (5) various published documents by the FATF and the APG.

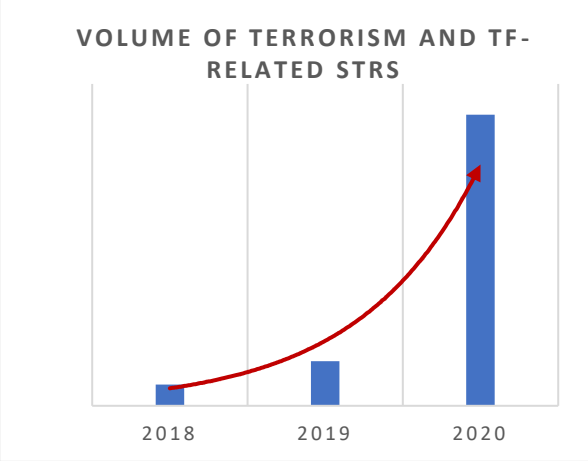
[1] The Asia/Pacific Group on Money Laundering is an inter-governmental organization, consisting of 41 member jurisdictions, focused on ensuring that its members effectively implement the international standards against money laundering, terrorism financing, and proliferation financing related to weapons of mass destruction.

[2] Covered persons, as defined under Republic Act No. 9160 or the Anti-Money Laundering Act of 2001, as amended

SUMMARY OF FINDINGS

The existence of terrorism and TF threats is evident in the suspicious transaction report (STR) submissions by CPs. Exponential increase can be observed from 524 STRs in 2018 to 7,230 STRs in 2020. The monthly trend shows a surge in STRs from September to December 2020, months after the enactment of the ATA.

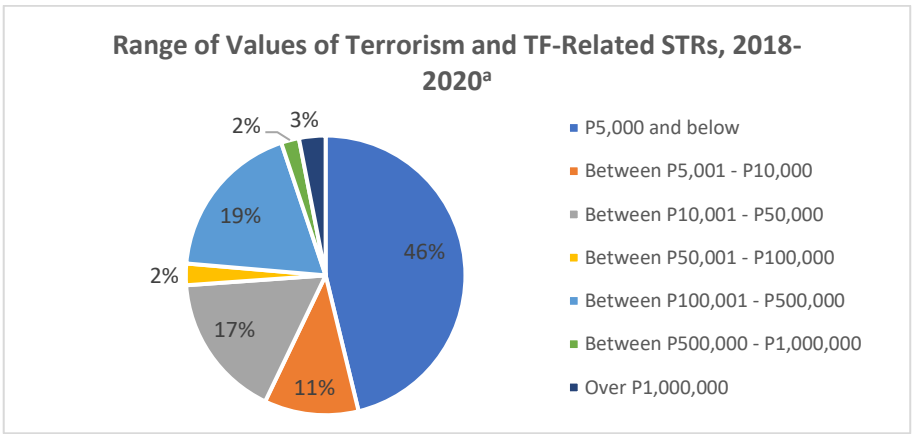




Data as of 29 December 2020; expected increases in the succeeding database extraction

Filing of STRs is expected to further increase following the designations of local threat groups as domestic terrorists in December 2020. STRs are reported through coordination between the AMLC and CPs for the possible nexus between the accounts and terrorism and TF. Further, the increase in trend can be attributed to the increasing awareness of CPs in detecting and determining possible financial transactions that may be associated with TF. Other contributory factors include the regular update of risk understanding through the engagement of the AMLC and other LEAs with CPs and industry associations; the existence of a public-private partnership between the AMLC and CPs; and the continuous coordinated efforts of various agencies in anti-money laundering and counter-terrorism financing (AML/CTF) campaigns.

Noticeably, majority of the STRs are below PhP5,000 (USD100 and below), explaining one of the red-flag indicators associated with TF, that is, structured or small amounts of frequent transactions that with no specific patterns.

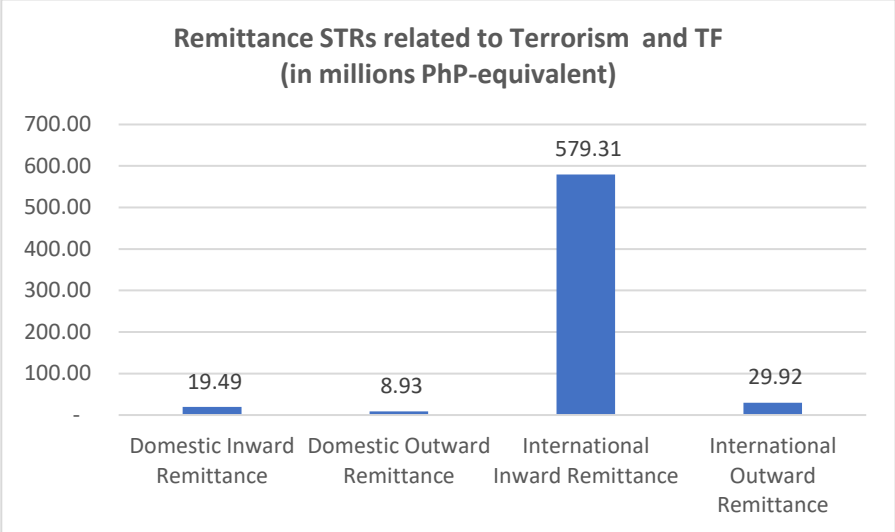


Excluded STRs that used the generic code [ZSTR code]

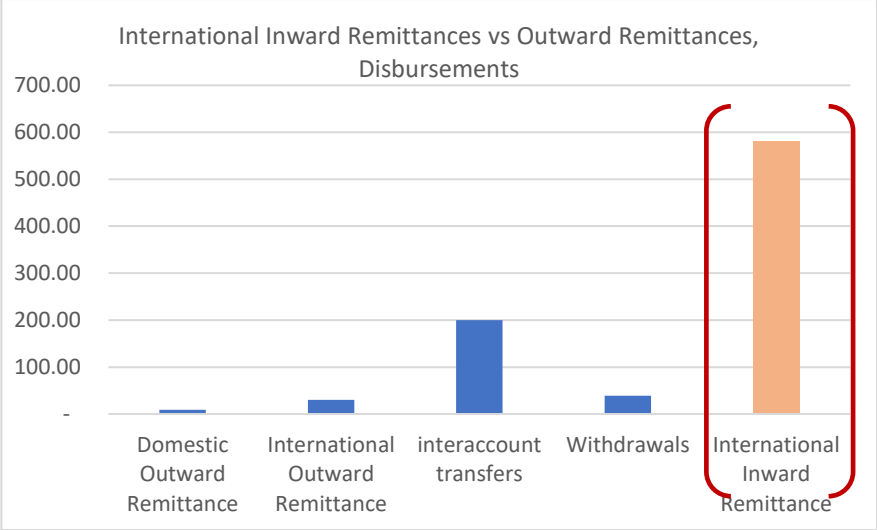
There is, however, an increase in the STR value within the transaction ranges of PhP10,001 to PhP50,000 and PhP100,001 to PhP500,000, particularly in 2020.

Cash and remittance transactions are commonly used to move and to transfer funds associated with terrorism and TF. From the sample terrorism- and TF-related STRs, it is estimated that PhP304 million are cash-related transactions, which is about 20% of the total value of the suspicious transactions. PhP263 million out of the PhP304 million, which is at 87%, are cash deposits, while only PhP39 million have been withdrawn via automated teller machines (ATMs) or over the counter.

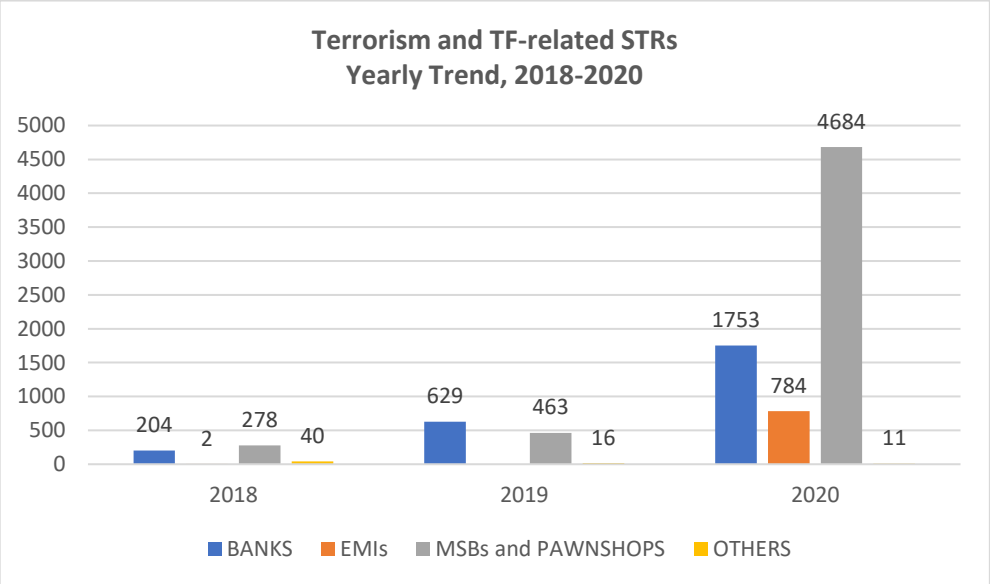
International and domestic remittances have also been reported as delivery channels to move or transfer funds. Remittance transactions account for 49% of the sample terrorism- and TF-related STRs. Notably, based on STRs, the Philippines appears as a recipient of TF-related proceeds from other jurisdictions as the international remittances account for 91% of the total remittance-related STRs. This further supports the finding that the Philippines is a destination country as regards TF, due to the comparative high volume of international inward versus outward remittances.



- The volume of withdrawals/outward remittances or inter-account transfers could not account for the value of inward remittance transactions associated with terrorism and TF. Thus, this presumes that there are undetected disbursements, withdrawals, or transfer transactions associated with TF funds.

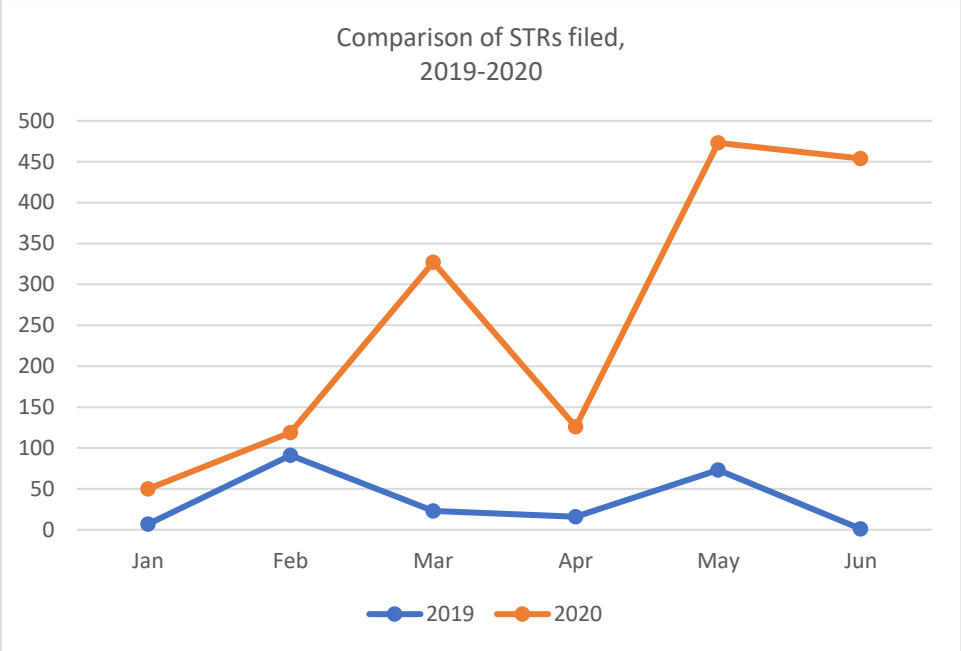


- The figure below illustrates that STR submissions by banks and money service businesses (MSBs) follow an increasing trend, registering at 194% and 489% moving average increase from 2018 to 2020, respectively. On the other hand, the use of electronic money issuers is a potential trend, with an increase of 784 STRs in 2020 from two (2) STRs in 2018.



<u>Suspicious transaction reporting during COVID-19</u>

An increase in STR filing was observed during the first few months of the COVID-19 pandemic. It can be attributed to the increase in awareness of CPs on terrorism- and TF-related transactions and close coordination with the AMLC and LEAs. For the month-on-month assessment, an increase of over 500% can be noted from March to June 2020 compared with the same months in 2019.



Foreign terrorist fighters

From 2018 to 2019 alone, the AMLC investigated about 325 foreign nationals suspected of terrorism and TF. Two hundred ninety-six (296) foreign nationals have been blacklisted; 10 are currently detained; and seven (7) have been deported to their respective jurisdictions.

The local LEA has identified 44 FTFs working with the local Daesh-inspired groups. This figure includes 24 Indonesians, seven (7) Malaysians, four (4) Saudi Arabians, two (2) Singaporeans, one (1) Pakistani, one (1) Bangladeshi, and five (5) others of unknown nationalities.

Regional threat

The incidents of terrorism appear concentrated in the Mindanao and Bicol regions of the Philippines. Nonetheless, there appears to be an establishment of operations in the regions of northern Luzon, southern Tagalog, and the Visayas. From 2017 to 30 September 2020, 2,660 incidents have been recorded by LEAs, registering a 156% increase from 1,039 incidents in the Second NRA. Over 50% of the incidents occurred in the Mindanao region, while 16% of the incidents transpired in the Region V (Bicol region). Police operations resulted in the neutralization of the 337 terrorist suspects and arrests of other 513 terrorist suspects.

Source: Law enforcement agencies

The incidents were perpetrated mostly by a domestic terrorist group at 91%, while the remaining 9% of the incidents were committed by the ISIS/ISIL-inspired terrorist groups and other threat groups. Terrorist groups herein include UN, foreign and domestic-designated terrorist groups. Atrocities/incidents perpetrated by terrorist/threat groups include shootings, harassment, encounters, bombings, and abductions/kidnappings.

Coordinated and collected efforts of LEAs and intelligence agencies caused the increase in filing of cases in courts and prosecutions. From January 2017 to September 2020, 30% of incidents/cases were filed in courts, 45% of the incidents/cases were referred to prosecutor's office, while the remaining 25% of incidents were under investigation.[3]

CONSEQUENCE ANALYSIS

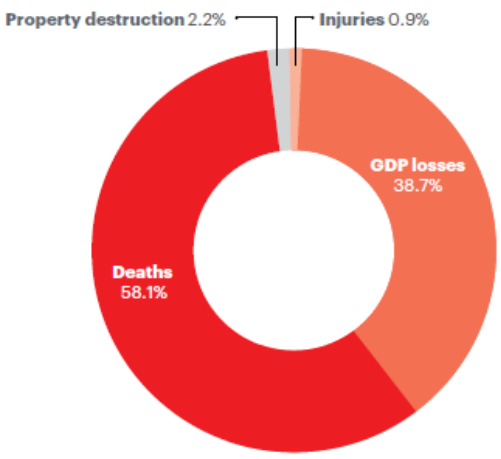
The 2019 to 2020 Global Terrorism Index (GTI) presents that the economic impact of terrorism includes the costs from four (4) categories: deaths, injuries, property destruction, and gross domestic product (GDP) losses. GDP losses refer to the country's losses in economic activity as a result of terrorism.

The breakdown of global economic impact of terrorism in 2018 as presented in the 2019 GTI report noted that deaths from terrorism account for just over 58% of the global economic impact or equivalent to USD19.3 billion. GDP losses are the second largest category contributing to 39% of the total, which is equivalent to USD12.9 billion.

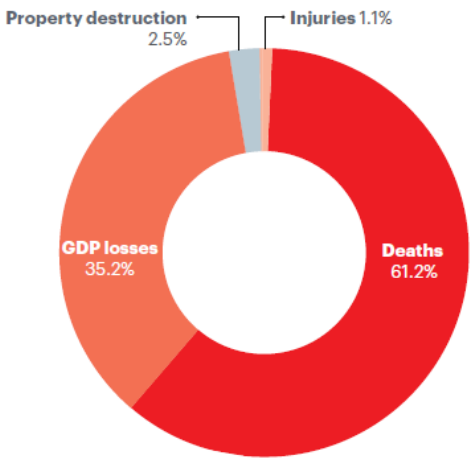
In the 2020 GTI report, the global economic impact was estimated at USD26.4 billion, registering a 20% decrease from USD33 billion in the 2019 GTI. This improvement was due to the reduction in the cost of indicators, particularly deaths due to terrorism and GDP losses.

The figures below illustrate the share of the total economic impact of terrorism by indicator. Deaths from terrorism remained the largest category in the model at 61.2%, the costs of which are estimated at USD16.2 billion. This was followed by GDP losses at 35.2% with an equivalent value of USD9.3 billion (2020 GTI Report).

[3] The Second NRA only recorded 2% of incidents/cases filed in courts while 9% of incidents/cases were referred to prosecutor's office.
Data from local law enforcement agency.



Source: 2019 GTI Report



Source: 2020 GTI Report

From information collected by one LEA, 905 individuals, including 530 civilians were killed or wounded in terrorist operations from 2017 to August 2020.

In addition to destroying lives and property, terrorism discourages business activities, production, and investment. It diverts government resources away from the economy to security services. Terrorism and TF also impact trade as these raise the costs of doing business with terror-affected countries. This may result in the increase of the prices of products, thus, reducing the exports and imports of these nations.

In a travel advisory[4] issued by the United Kingdom government as regards the emergence of the COVID-19 pandemic, it specified that terrorists are very likely to carry out attacks in the Philippines. It further mentioned that terrorist groups have the intent and capability to carry out attacks anywhere in the locality, including Metro Manila and places visited by foreigners, such as shopping malls, entertainment establishments, public transport (including airports and the metro system), and places of worship.

The impact of terrorism and TF is **high**. It directly affects the reputation of the country in the international community, which may have a domino effect: It affects not just the economy but also the trade, GDP, flow of remittances, tourism, and international relations with other jurisdictions. Also, terrorism and TF have a big impact on a domestic level, particularly on the lives affected by the attacks, including destroyed property as well as psychological and social effects on people.

OVERALL ASSESSMENT

Based on the Second NRA and this study, the overall risk of the Philippines to terrorism and TF is **high**. Notable improvements and mitigation efforts, including the enhanced continuing collaboration and cooperation of the LEAs, intelligence agencies, CPs, and the AMLC were, however, instituted to match the high TF vulnerability. The evolving and emerging threats

[4] Terrorism – Philippines travel advice by the government of the United Kingdom (Covid-19 travel guidance, https://www.gov.uk/foreign-travel-advice/philippines)

continue to challenge the financial system as well as the government's policies and mechanisms against terrorism and TF.

Terrorism threat is rated **high**, given the high number of violent incidents associated with terror/threat organizations. The emergence of suicide bombers and the rise in the numbers of FTFs attest to the **high** rating of terrorism threat in the country. Most of the identified suicide bombers are FTFs. There was, however, an incident in June 2019, where Filipinos were implicated in a suicide bombing incident. The noted involvement of various Islamic State (IS)-inspired groups as well as the known influx of FTFs in the country added challenges to the security efforts of the Philippine government. While most terror-related incidents have been situated in the Mindanao and Bicol regions during the period of the assessment, widespread operations appear to have been established as evidenced by the increase in incidents in the northern and southern Tagalog regions of Luzon; and the Visayas regions.

While the Philippines has improved its GTI ranking from ninth in 2019 to 10th in 2020, GTI reports still identify the Philippines as one of the countries in the Asia Pacific Region with the most impact from terrorism. Said reports also pinpoint the NPA to be the group responsible for over 35% of deaths and terror-related incidents in the Philippines.

In 2020, despite the COVID-19 pandemic, there were still noted attacks carried out by several terror groups. This may mean that their operations continue despite the lockdowns and may further infer that terrorist funding continues as terrorist attacks may not be operationalized without funding and support.

Threat posed by TF is **high** as terrorist/threat organizations in the country appear to have a systematic and a more established method of raising funds for their operations. Terrorist/threat organizations predominantly raise funds from their own sources through illegal activities with kidnap for ransom and extortion as the preferred means. While the total amount raised by these organizations remains largely unknown, the high number of threat incidents recorded by LEAs indicate that these terrorist/threat organizations are well-funded.

Threat groups also resort to legitimate means to raise funds. Among the fundraising methods are the use of non-profit organizations, family funding, and legitimate business fronts. The use of legal entities (particularly non-stock, non-profit) as front companies is also identified as one of the means for channeling the funds of terrorist groups in the country.

The use of funds is generally for operational purposes, such as the purchase of arms and vehicles, rather than for financial gain. Threat groups also use part of the funds raised to support the communities where they operate. The groups provide basic needs, livelihood support, and even educational opportunities to these communities. In turn, the communities shield them from government forces, even if these communities are aware of the nature and source of the funds. Additionally, said groups utilize said funds for training, whether in or out of the country.

Vulnerabilities are present, but the government as well as the private and public sectors have done multifarious efforts to mitigate said vulnerabilities. Notable are the increase in the filing of terrorism-related cases and increase in prosecutions.

During the period of the assessment, 30% of incidents/cases resulted in the filing of cases in courts, and 45% of the incidents/cases were referred to prosecutor's office. These were accomplished through coordinated and collected efforts of LEAs and intelligence agencies.

Cash transactions remain to be the mode for transfer of value for Philippine terrorist/threat organizations. The physical movement of cash leaves no paper trail, and it is not hindered by AML/CTF safeguards present in the formal financial system. Remittance transactions have also been reported to be the delivery channel by which funds are transferred, especially from abroad. MSBs and banks are the most used channels in moving funds. There were also noted unregistered MSBs that are utilized by terror groups to further avoid detection and to easily move funds in and out of the country.

One of the emerging threats noted in TF is the evolution of virtual currency and/or cryptocurrency. The value of STRs associated with bitcoins or virtual currency from 2019 to 2020 is estimated at PhP1.77 million. Suspicious transactions reported by CPs, albeit limited at the time of the assessment, indicate an emerging use of bitcoins/cryptocurrencies. There are also anecdotal incidents of terrorist groups using crypto-assets in the Marawi siege.

Another emerging threat identified is the use of social media, social circles, or crowd-sourcing platforms. These platforms serve as means to express their ideologies, recruit potential fighters, and spread fear.

Cross-border linkages to TF and terrorism are evident in typologies and reported transactions and are supported by the external threats study in 2018, which identified the Philippines as a destination country of funds related to TF.

The rising number of STRs received by the AMLC indicates an increasing level of awareness among CPs as regards identification and detection of financial transactions that are possibly associated or directed for TF and other relevant crimes. Red-flag indicators and the nature of transactions are evident in STR submissions. Corollary to that, there was also an improvement in the number of cases investigated related to TF.

For the given period, the total amount frozen compared with the estimated amounts raised is at minimal level. Despite that, the issuance of sanctions freeze order, designations of local threat groups as terrorists, and enhanced due diligence and prevention of terrorists from using the financial system contribute to the disruption of funding for terrorism activities.

The awareness of the usefulness of intelligence-gathering and -sharing for TF is evidently shown in cases and case typologies. This shows that agencies are already developing an appreciation for the strong connection of TF to terrorism and terrorism-related incidents.

Domestic and international coordination mechanisms are instrumental in providing better responses to threats posed by terrorism and TF and, thus, should be further strengthened. Recent experiences have shown that close domestic and international coordination among the AMLC and relevant government agencies yielded positive results. The operationalization of several domestic coordination mechanisms (i.e. National Law Enforcement Agency Coordinating Committee [NALECC], NACC, and their respective subcommittees) is likewise a

significant factor in ensuring opportune investigations and effective information-sharing and actions against terrorism and its financing. Likewise, the creation of the Anti-Terrorism Council (ATC) poses a stronger foundation in coordination, cooperation in information-sharing, and policy initiatives against terrorism and TF. Various domestic coordination mechanisms, massive awareness campaigns, and CTF trainings as well as the operationalization of the Public-Private Partnership Program (PPPP) address a whole-of-government approach in combating terrorism and its financing as well as other related crimes.

More than domestic efforts, the country's leaders also recognize the significant contribution of all international initiatives and cooperation in addressing terrorism issues. Over the past years, synergies of the international community have achieved remarkable results, which the Philippines continues to support to fully address terrorism crimes that transcend boundaries.

Further, this calls for stronger coordination and collaboration between the public and the private sector as FIs have the data necessary to detect and identify terrorist linkages and networks while government agencies are the primary agencies that investigate and prosecute alleged suspects of TF and terrorism.

Other LEAs' initiatives have also leveled up as they expand to include domestic, international, and inter-agency coordination.

It is important to note that there is an increasing level of awareness among CPs. Government coordination with CPs and the private sector must be further strengthened.

There are also noted challenges in the campaign against terrorism and TF, and this may be addressed by inter-agency and inter-sector coordination as well as international cooperation.

RECOMMENDATIONS AND PROPOSED ACTION PLANS/MITIGATION STRATEGIES

TF is not only a domestic issue as it also poses cross-border challenges. A collaborative multisector response to mitigate the risk exposures to TF, as well as the involvement of various relevant agencies and the private sector, is needed. This will help further strengthen the national system against TF and other terrorism-related acts.

- While the government, through various LEAs and supervisory agencies, has intelligence leads, banks and other CPs have additional information that may be needed to confirm and strengthen said leads. Thus, there is a need to further strengthen the relationship between the private and the public sector. This may be carried out by expanding the PPPP framework. The PPPP promotes trust and confidence among sectors and agencies by sharing priorities and challenges as well as sharing best practices to further lessen and combat TF.

- Red-flag indicators, suspicious triggers, and case typologies serve as guidance to CPs in identifying terrorism and TF activities. Thus, there is a need to continuously update and disseminate red-flag indicators, suspicious triggers, and case typologies to regulators and the private sector, particularly to CPs as they are the first line of defense

in the disruption of TF-related activities. It is notable to highlight that disrupting financial transactions of terrorist groups are expected to disrupt their operations.

- Risk information must be continuously shared with CPs for a more efficient and proactive reporting of suspicious transactions; and with relevant agencies and regulatory bodies for the continuous update of their risk understanding.

- Various outreach programs across all segments of the society, including schools and rural areas, specifically in far-flung areas in the Mindanao and Bicol regions must be conducted as these places are mostly the target of attacks and/or operations.

- Various livelihood programs that may help the poor and the marginalized, especially to those that were greatly affected by terrorist attacks, for the purpose of raising financial income must be conducted.

- Thematic and targeted capacity building initiatives must be conducted as these may help CPs, particularly MSBs and other small and stand-alone banks operating in the grassroots level, as they may have limited access to AML/CTF tools and technology and may have very minimal knowledge of ML/TF typologies and red-flag indicators and triggers.

- Targeted risk-based supervision of NPOs must be implemented. Similar to MSBs and small and stand-alone banks, the NPO sector may need thematic and targeted capacity building initiatives to increase their level of awareness relative to risks posed by terrorism and TF.

- Designation of terrorists and known terrorist organizations in accordance with UNSCR 1373 should be fully implemented under the ATA and TFPSA. Identifying, publication and effective preventative measures for seizing/freezing of these known terrorists and terrorist organizations will increase awareness of all financial sectors, the general public and other business sectors which potentially will increase ST reporting and investigations/prosecutions relating to terrorism and TF. Implementation of processes for communicating nationally listed persons and organizations to reporting entities, financial sector, enforcement agencies and the general public are needed in order for these efforts to be successful.

- The government agencies may consider reassessing its capacity and resources dedicated to combating terrorism and terrorism financing.

- Best practices must be continuously shared not just among government agencies but also between the private and public sectors. This may further strengthen compliance and investigations regarding terrorism and TF.

RED-FLAG INDICATORS AND SUSPICIOUS TRIGGERS

A. Indicators as observed by covered persons

Based on the survey conducted by the AMLC in 2020, respondent CPs were able to pinpoint some of the behavioral manifestations of possible and suspected terrorist group members. The following are some of the observations:

1. Preparation. Individuals who decide to travel overseas to participate in hostilities in a conflict zone need time and resources to prepare. Thus, these individuals may demonstrate the following:

   - ➢ Person/account activities indicate sale of personal possessions;
   - ➢ Airline tickets to countries in conflict, i.e., Iraq, Syria, Turkey, etc. are purchased;
   - ➢ Donations are made to NPOs linked to terrorist activities;
   - ➢ Funds from social assistance, student loans, or other credit products ("debt financing") are used;
   - ➢ Available credit products, including maxing out credit cards, not making payments, and transferring balances to personal debit accounts are exploited;
   - ➢ Accounts show signs of unexplained increase in deposits and money flow; and
   - ➢ Multiple small amounts of money are deposited into the account by various unrelated individuals via cash.

2. En route (the period from departure from their homes to arrival at their destinations). Noted behaviors of said individuals travelling to conflict zones to participate in hostilities are:

   - ➢ Customer notifies the bank on travelling to a third country via a country contiguous to a conflict zone but subsequent financial activities indicating that the journey was not completed;
   - ➢ Financial activity, such as debit or credit card usage, along a known travel corridor to a conflict zone, is evident; and
   - ➢ Receipts of wire transfers inside or along the border of a conflict zone are evident.

3. Arrival in the conflict zone. Foreign fighters may still have some access to either personal resources or to those of friends, family, or supporters outside the conflict zone. The following may be noted:

   - ➢ Person receives money transfers from family or friends within the vicinity of a conflict zone;
   - ➢ Stated purpose of transactions for online fund transfers are "infaq," "jihad," "dana mujahid," "ISIS," and "Allahhuakbar;"
   - ➢ Public information and media coverage may be found, indicating that the person has travelled to a conflict zone;
   - ➢ Accounts have turned dormant; and

- ➢ Multiple cash withdrawals, leaving a minimal balance in the account with last withdrawal, have been made at the international airport.

4. Return home. This stage is critical in terms of public safety, since returning foreign fighters may bring their combat experience and connections to terrorist groups home. There is also a risk where the returnees would continue to act as facilitators or supporters of terrorist activity or even as participants in future attacks (this is also one of the key findings in the noted red-flag indicators and suspicious triggers).

   - ➢ Dormant account is reactivated;
   - ➢ Person begins to receive new sources of income, i.e. new employment or social assistance; and
   - ➢ Person sends or receives domestic or international transfers.

5. Interrupted travel. Some individuals may be prevented from reaching a conflict territory by the authorities or may change their course of action for other reasons. These individuals may continue to plot or facilitate domestic attacks or to attempt to facilitate the travel of others. While the frequency of such attacks may be low, their impact on public safety can be significant.

   - ➢ Person made travel-related purchases, such as airline tickets or visas, which were subsequently refunded;
   - ➢ Person indicated that they would be travelling out of the country, but their transaction history suggests that the travel did not occur; and
   - ➢ Public information may be found, indicating that the person was prevented from travelling for security reasons.

B. Suspicious indicators and triggers

The study identified red-flag indicators and suspicious triggers that may illustrate patterns of transactions associated or linked with TF. Indicators and triggers are extracted and gathered from STRs; various reports of other financial intelligence units and other international groups/organizations; and respondent CPs to the survey conducted by the AMLC as CPs know firsthand how transactions behave.

These indicators may aid CPs in detecting and identifying possible transactions; and in pinpointing alleged persons-of-interest behind said transactions. Also, the following provide information to relevant LEAs on how transactions relative to TF evolve through time:

- Remittance transactions that are in structured or layered amounts to/from high-risk locations known for terrorism. Amounts are structured to avoid reporting requirements indicated in the AMLA, as amended;
- Customer transactions involving goods/merchandise that are dual-use or proliferation-sensitive;
- Unusual dealings in dual use goods/products/technology, which are not in line with the profile of customer;

- Amount involved is not commensurate with the declared business or financial capacity of the client. Value of the transaction/s is grossly over and above what the client is capable of earning;
- An observed and maybe sudden deviation from the client's profile as well as from the client's past transactions;
- Insufficient, incomplete, and suspicious information from the customer;
- Wire transfers between accounts that have no visible legal, economic, or business purpose, particularly if the said transfers are through countries, which are identified or connected with terrorist activities;
- Sources/counterparties/senders and/or beneficiaries of wire transfers, who are citizens of countries, which are identified or connected with terrorist activities;
- Multiple deposits or withdrawals that cannot be satisfactorily explained or do not make economic or business sense;
- Transactors are individuals, who have no known connection or relation with the accountholder;
- Client is receiving suspicious remittances from a country, where none of his family members are working or residing;
- Client is reported and/or mentioned in the news to be involved in terrorist activities;
- Client is under investigation by LEAs for possible involvement in terrorist activities;
- Transactions of individuals, companies, or NGOs/NPOs that are suspected to be used as "fronts" in sending or receiving funds to/from a terrorist individual, organization, association, or group of persons;
- NGO/NPO does not appear to have expenses that are normally related to relief or humanitarian efforts;
- Volume and frequency of transactions of the NGO/NPO are not commensurate with its stated purpose and activity;
- Cash or other transactions, which are not in line with the normal usage for the product as well as with the verified expectations of transaction behavior;
- ATM/over-the-counter withdrawals or wire transfers to jurisdictions, which are found to be of high risk for TF activities;
- Irregularities in the debit/credit transactions to individuals/organizations, whether domestic or international;
- Unusual or suspicious use of several channels, local branches/individuals, to make credits;
- Concealment of beneficial ownership of funds or lack of transparency as regards the ultimate beneficial owner of the funds associated with a certain transaction;
- Multiple individuals sending funds to one beneficiary, where the relationship between those individuals and the beneficiary is questionable;
- Cash transactions in multiple locations, where the client has no known connections, specifically in domestic and international high-risk areas;
- Transactions of individuals, companies, or NGOs that are affiliated with or related to people suspected of being connected to a terrorist group or a group that advocates the violent overthrow of a government;
- Deposits with immediate withdrawals, cash withdrawals or foreign exchange transactions for remittance or transfer of funds even below the threshold amount;

- An inactive account that suddenly has a certain amount of money or more and that is quickly transferred or withdrawn;
- Rapid movement of funds in one's account. After the account is opened, the customer receives deposits and transfers/withdraws immediately;
- Customer frequently deposits or withdraws cash on behalf of another person, or an account is frequently deposited or withdrawn cash by a third party;
- Remittances to/from foreign countries or foreign currency exchange transactions involving a customer, a related party, and the like whose address or location is in a country or region which is identified as high risk (for terrorism or terrorism-related crimes) by FATF;
- Transactions involving a customer or another related party requesting remittance to politically unstable regions, such as those known to be under the control or presence of terrorists;
- Source of funds for a certain transaction (i.e. wire transfer) is accumulated by frequent cash deposits by the customer or accumulated by frequent cash deposits from unspecified sources;
- Large number of deposit or withdrawal transactions in small denominations, which is unusual for a customer's business profile;
- Sudden emptying of or closing of an account after multiple transactions;
- Payments to personal accounts, MSBs, or charities that are located in conflict zones or neighboring regions;
- Customer appears to have accounts with several financial institutions in one area for no apparent reason;
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection;
- Customer repeatedly uses an address but frequently changes the names involved;
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds;
- Unusual transactions like sending fund transfers to seemingly unrelated individuals from a customer, who just returned in the country;
- Client cannot provide adequate explanation and supporting documents relative to origin/source of funds and usage/purpose thereof;
- Noted transactions from countries or geographic areas identified by credible sources as providing funding or support for terrorism activities;
- Sources of funds are vaguely stated, unknown, or inconsistent or are from a donation/commission;
- Observed multiple cash donations/fund/wire transfers/deposits in small amounts;
- Use of charitable institutions as front institutions to gather and/or accumulate funds;
- A significant change in the account balance of the client;
- Sending and receiving transactions from NGOs, religious orders, agricultural, charitable institutions, which are operating in a high-risk location; and
- Individuals and NGOs that receive funds for purposes of paying/remitting revolutionary taxes, donations, or financial aid.

It must be noted that the indicators and triggers are not intended to be comprehensive and conclusive. Although they are considered to be helpful indicators and triggers, they may not be present at all times. It must be noted that one must neither be restricted nor limited with

the list of red-flag indicators and suspicious triggers incorporated in this paper because TF and other related or associated crimes continue to evolve. It is advised that if the CP suspects that a certain transaction has a high probability of being linked to TF, it is highly encouraged that said transaction be reported.