TERRORISM FINANCING NATIONAL RISK ASSESSMENT

2020

SINGAPORE

Singapore's key terrorism financing (TF) risk areas

MINISTRY OF HOME AFFAIRS
SINGAPORE

MOF
MINISTRY OF FINANCE
SINGAPORE

MAS
Monetary Authority of Singapore

INTRODUCTION

OBJECTIVES

This terrorism financing (TF) national risk assessment (NRA) is a product of Singapore's ongoing review of our TF risks, and updates our earlier Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT) NRA published in 2014. The TF NRA reflects our collective experience and observations over the past few years. It presents an overview of Singapore's TF risk environment, and identifies the key risk areas within our national CFT system. The NRA seeks to further deepen law enforcement agencies, regulators/supervisors, policy makers and the private sector's understanding of Singapore's TF risks and vulnerabilities, allowing them to adopt a targeted and risk-focused approach when developing and implementing CFT strategies and risk mitigation measures.

PARTICIPANTS

In Singapore, the Risks and Typologies Inter-Agency Group (RTIG), led by the Ministry of Home Affairs (MHA) and the Monetary Authority of Singapore (MAS), oversees the identification, assessment and mitigation of TF risks at the whole-of-government level. The RTIG comprises all relevant supervisory, regulatory, law enforcement and policy agencies. The work of the RTIG is overseen by the AML/CFT Inter-Agency Committee and the AML/CFT Steering Committee[1]. Singapore's understanding of our TF risks has been further enhanced by the involvement of the private sector and academia through various projects. Singapore has established an AML/CFT Industry Partnership (ACIP)[2]. This is a public-private partnership through which agencies tap on financial institutions' insights on TF risks, as well as the financial background and financing methods employed by local radicalised individuals. The International Centre for Political Violence and Terrorism Research under the S.Rajaratnam School of International Studies (RSIS) also contributed to our risk understanding with a regional TF risk assessment of South Asia and Southeast Asia, outlining known TF typologies observed in these regions. In addition, regulators have considered if similar TF threats could materialise in their sectors.

[1] The AML/CFT Inter-Agency Committee is co-chaired by the Deputy Secretary of the MHA and the Deputy Managing Director of MAS. The AML/CFT Steering Committee is co-chaired by the Permanent Secretaries of the MHA and the Ministry of Finance, and the Managing Director of MAS.
[2] The AML/CFT Industry Partnership is co-chaired by MAS and the Commercial Affairs Department of the Singapore Police Force. For more details please refer to https://www.abs.org.sg/industry-guidelines/aml-cft-industry-partnership

METHODOLOGY

The methodology applied in the TF NRA is based on guidance published by the Financial Action Task Force (FATF)[3], and takes into account a range of qualitative and quantitative information. TF risks are a function of threats, vulnerabilities and consequences. ***(ANNEX - Detailed definitions of threat, vulnerability and risk)*** Agencies went through the following process to come up with the outcomes of the TF NRA:

Examination of the Overall Terrorism/TF Threat

Terrorist groups that posed the most significant terrorism threat to Singapore and the region were identified, and the primary ways these groups were financed were examined. The TF threats posed to the different sectors were outlined, substantiated by information from investigations and financial intelligence including Suspicious Transaction Reports (STRs), Requests for Assistance (RFAs), Mutual Legal Assistance (MLA) requests, and supported through participation in regional CFT projects and surveillance of regional and international typologies.

Analysis of Sectors' TF Vulnerabilities

Regulators/supervisors oversaw their respective sectors' vulnerability assessments, taking into consideration their sector's key TF threats, and how certain products, services and activities within the sector might be exploited for TF purposes.

Evaluation of the TF Risks of Various Sectors

The risk of terrorists/terrorist groups using a particular sector for TF was evaluated, as a function of the sector's threats and vulnerabilities (including controls), with consequences deemed to be severe. The following matrix was used to arrive at the TF risk ratings of the various sectors (i.e. H: High; MH: Medium High; ML: Medium Low or L: Low).

Risk Ratings		Vulnerabilities			
		L	**ML**	**MH**	**H**
Threats	**H**	MH	MH	H	H
	MH	MH	MH	MH	H
	ML	ML	ML	MH	MH
	L	L	L	ML	ML

[3] *The FATF's TF Risk Assessment Guidance Project, published on 31 May 2019.*

KEY TERRORISM FINANCING THREATS

The key TF threats emanate from: (i) terrorist groups such as Islamic State of Iraq and Syria (ISIS), Al-Qaeda (AQ) and Jemaah Islamiyah (JI); and (ii) radicalised individuals who are sympathetic towards the cause of the terrorist groups, predominantly ISIS. In assessing the TF threats arising from these areas, key TF activities such as the raising, moving and using of financial resources for terrorism purposes have been taken into consideration.

ISLAMIC STATE OF IRAQ AND SYRIA (ISIS)

The most pressing terrorism threat in Singapore's context emanates from ISIS. Although the group has ceded its territorial caliphate in Iraq and Syria, ISIS and its affiliates continue to be the main and best-resourced terrorist threat globally. The death of Abu Bakr al-Baghdadi[4] in October 2019 was a blow to ISIS, but the withdrawal of US troops, the Turkish invasion of northern Syria and the ongoing US-Iran tensions may have provided ISIS' new leader, Abu Ibrahim al-Hashemi al-Qurashi, space to consolidate his position. In the period since, ISIS has reportedly intensified its activities in Iraq and Syria. There continue to be arrests, attacks and foiled plots involving ISIS-linked/inspired suspects around the world, including Southeast Asia[5].

The ongoing conflict in Syria and Iraq, ISIS' growing interest in Southeast Asia and the presence of ISIS militants in the region raise the possibility of Singapore being used by ISIS as a conduit to move funds in the region.

ISIS' GROWING FOCUS TOWARDS SOUTHEAST ASIA | In July 2018, ISIS announced a major reorganisation of its global caliphate with the incorporation of Southeast Asia, as part of its East Asia division - *Wilayat Sharq Asiyya*. This said, ISIS affiliates are expected to become financially self-sustaining. The inflow of funds from ISIS into the region for terror plots and other activities appears to continue in spite of the group's losses in the conflict zone. Regional terrorist groups and elements have also been involved in raising and moving funds across and beyond the region to support the ISIS cause, and to fund the recruitment and travel of fighters to Syria, Iraq and other conflict zones[6].

PRESENCE OF FOREIGN TERRORIST FIGHTERS IN THE REGION | Of the Southeast Asians who have travelled to join the conflict in Iraq and Syria, a few have returned and plotted attacks in their home countries. Given ISIS' defeat in Syria and Iraq, more may seek to return.

TF TYPOLOGIES | ISIS is believed to have smuggled some US$400 million out of Iraq and Syria via established criminal and *hawala*[7] networks, and experienced financial facilitators. Its core continues to provide resources to its affiliates, including those in Southeast Asia, albeit at a reduced level. Known means of transfers involve cash couriers, money remittances, bank transfers, virtual currencies and online transactions.

As for terrorists/individuals within the region raising and moving funds to support terror activities, funds could come from legitimate sources such as salaries, charities (misused), illegitimate sources such as criminal proceeds. Funds could be transferred via similar means.

AL-QAEDA AND JEMAAH ISLAMIYAH ELEMENTS

There are signs that Al-Qaeda and Jemaah Islamiyah are regrouping and may resume planning large-scale attacks, which require funds to be raised or moved.

AL-QAEDA (AQ) | Far from being a spent force, AQ has adopted a "long-game strategy" of building local alliances and socialising local communities through its regional affiliates. In January 2019, the UN reported that AQ remains resilient and active and is stronger than ISIS in some regions.

JEMAAH ISLAMIYAH (JI) | While Singapore's JI network was disrupted in 2001/2002, and there has also been no indication of any attempt by the JI to regroup in Singapore, the regional JI has not abandoned its armed jihad goals. Since end-2010/ early-2011, JI has reportedly adopted a "no-bomb policy for the time being" and focused instead on *dakwah* – missionary activities like above-ground preaching and recruitment aimed at broadening JI's base.

TF TYPOLOGIES | Prior to its disruption in 2001/2002, the Singapore JI network was largely self-financed. The funds were used to finance the Singapore JI's local activities, as well as channelled to the JI leadership in Malaysia. The Singapore JI members eschewed the commercial banking system, primarily because these institutions were interest-generating and hence regarded as *haram* (forbidden).

[4] Baghdadi was named caliph when ISIS announced the establishment of the Islamic Caliphate in June 2014. He remained the leader of ISIS until October 2019, when he died after detonating a suicide vest while cornered by US forces in Idlib, Syria.

[5] As Baghdadi's deputy, Qurashi reportedly ran ISIS' day-to-day operations and was at the centre of the group's decision making. As such, it has been assessed that there would be more continuity than change for ISIS under his leadership.

[6] MHA's Singapore Terrorism Threat Assessment Report 2019, published on 22 January 2019 (www.mha.gov.sg/newsroom/press-release/news/singapore-terrorism-threat-assessment-report-2019)

[7] Hawala is a value-transfer system that relies on a network of brokers to send money to various locations instantaneously and frequently without a paper trail. An individual transfers money from one location to another by depositing money with a local agent, who informs his counterpart abroad to pay the recipient; the two agents settle their accounts later.

RADICALISED INDIVIDUALS

Singapore continues to detect radicalised individuals, both from the local and foreign worker populations, who are sympathetic towards ISIS' cause. Amongst them, Singapore has convicted 11 individuals for TF from 2016 to-date[8]. All of their activities relate to the raising and/or moving of funds out of Singapore, using fairly unsophisticated channels (e.g. through remittance agents) and methods, to support terrorist activities abroad.

RADICALISED SINGAPOREANS | Since the rise of ISIS, there has been a corresponding increase in the number of self-radicalised Singaporeans detected. A total of 29 Syria-related radicalised Singaporeans have been dealt with under the Internal Security Act (ISA), as of September 2020. The ISA allows the Government to detain or impose Restriction Orders on individuals who pose a threat to Singapore's internal security, which includes involvement in terrorism-related conduct.

Singapore continues to detect a small number of radicalised Singaporeans who had intended to travel abroad and fight alongside ISIS. For instance, Singaporean A, who was detained under the ISA, had intended to join the Marawi City siege in 2017. **[BOX EXAMPLE 2.1]** Four other Singaporeans were also known to have travelled to Iraq and Syria to participate in the conflict there.

RADICALISED FOREIGN WORKERS | Singapore continues to detect radicalisation among foreigners working and living in Singapore. **[BOX EXAMPLES 2.2 AND 2.3]** The presence of a significant foreign community could also enable terrorist groups to use Singapore as a base for terrorism fundraising amongst their own nationals here, or as a conduit for TF purposes.

TF TYPOLOGIES | From the known TF cases, the main modalities include self-funding from individuals' salaries or savings and transfers via licensed money remittances. **[BOX EXAMPLE 2.4]** The amounts involved in the known TF cases are not large. Our investigations also revealed that none of the cases were linked to organised crime, as Singapore remains inhospitable for organised crime groups to establish roots[9].

Singapore's relative affluence means that locals and those working here potentially possess greater means and access to raise or move funds for terrorism-related activities. Self-radicalised individuals who have been convicted for TF offences include a local businessman, as well as foreign workers (who possessed sufficient discretionary funds to contribute towards terrorist activities).

To better understand the risks posed by self-radicalised individuals, the authorities have commenced a study to better understand the financial behaviour of terrorist actors. **[BOX EXAMPLE 2.5]**

Box Example 2.1 – Singaporean A Convicted of TF

Singaporean A travelled to Turkey in February 2014 under the guise of providing humanitarian aid. He said that he was in touch with non-profit organisations (NPOs) for this trip, even obtaining funding of S$1,000 from an unregistered online group. He had intended to find an opportunity to sneak away and join ISIS, but was unsuccessful in doing so. In October 2014, he sent S$450 from his personal earnings, via Western Union, to an individual in Turkey[10], for the publication of ISIS propaganda. In January 2020, Singaporean A was sentenced to 33 months' imprisonment under the Terrorism (Suppression of Financing) Act (TSOFA)[11].

Box Example 2.2 – Three Indonesian Foreign Domestic Workers Convicted of TF

Three female Indonesian foreign domestic workers were radicalised in 2018 via social media, and were investigated by Singapore's Internal Security Department (ISD) for their support of ISIS and Jamaah Ansharut Daulah (JAD). Parallel TF investigations by the Commercial Affairs Department (CAD) found that they had sent amounts ranging from S$100 to S$1,200, via a licensed remittance agent, to two charities in Indonesia purportedly linked to JAD, to support JAD militant causes and the families of JAD members who had been detained or killed as a result of JAD-related activities. Prior to their arrests, they had been working in Singapore for a period of six to 13 years. Between February and March 2020, they were sentenced to imprisonment terms of 18 to 45 months under the TSOFA.

[8] As of September 2020.

[9] Singapore remains inhospitable for organised crime groups to establish roots. We mount operations to disrupt organised crime threats. Our capabilities are further enhanced through new legislative tools in the form of the Organised Crime Act, and through setting up dedicated units to fight organised crime such as the Organised Crime Branch in the Criminal Investigation Department of the Singapore Police Force.

[10] This individual was also designated by the US Treasury's Office of Foreign Assets Control (OFAC) in 2016 for providing logistical support and facilitating the movement of tens of thousands of dollars and foreign fighters for ISIL.

[11] Singapore's legislation to counter terrorism financing.

RADICALISED INDIVIDUALS

Box Example 2.3 – Six Bangladeshi Workers Convicted of TF

In 2016, six Bangladeshi workers were sentenced to two to five years' imprisonment under the TSOFA. These Bangladeshis were part of a pro-ISIS clandestine group making preparations for armed *jihad* in Bangladesh. The group, which called itself the "Islamic State in Bangladesh" (ISB), comprised eight Bangladeshi nationals working in Singapore and saw itself as an ISIS affiliate. Although they had initially wanted to travel to Syria to join ISIS, they subsequently decided to focus their plans on returning to Bangladesh instead, as they felt it would be too difficult for them to make their way to Syria. Of the eight ISB members who were detained, six were found to have been involved in the raising of funds for ISB causes[12]. The six had amassed a sum of S$1,360, which was intended for the procurement of weapons for their *jihad* in Bangladesh. The monies were collected in cash. At the time of arrest, the group had neither planned nor decided on the means of transferring the monies.

Box Example 2.4 – Singaporean B Convicted of TF

In October 2019, Singaporean B was sentenced to 30 months' imprisonment under the TSOFA. He sent S$1,145 from his personal earnings to two intermediaries through a licensed remittance agent and a payment platform. The monies were meant for a radical preacher in Jamaica, who supports the use of armed violence by ISIS, to set up an Islamic caliphate.

Box Example 2.5 – Preliminary Key Findings of the Financial Study of Radicalised Individuals in Singapore

The financial study on radicalised Singaporeans is conducted in two phases, with government agencies formulating preliminary insights in the first phase and collaborating with financial institutions in the second phase.

The first phase comprised an analysis of the individuals' financial background and their methods of financing (including the raising, moving and using of funds). It was found that a vast majority of the radicalised individuals did not engage in, or planned to engage in, terrorism financing activities. It was assessed that this was likely due to these possibilities: (i) these individuals were interrupted early in their radical trajectories before they had developed concrete plans of securing funding; (ii) the individuals had likely been more consumed by other practicalities and challenges that they had to surmount in their desire to join ISIS, such as how to get past border security, especially after Turkey clamped down on the flow of fighters, or how to link up with ISIS once in Syria; and/or (iii) the actual cost of travelling to conflict zones was not prohibitively high.

Amongst those who tried or planned to raise funds, however aspirational or preliminary in nature, self-funding from legitimate or existing income sources was the most common method. Those who gave money for terrorism purposes or to terrorism-linked individuals predominantly used licensed remittance agents. The sums involved were small and did not involve complex or peculiar transaction patterns that would trigger suspicion.

In the second phase of the study, authorities will be leveraging the CFT Operational Group set up under ACIP. The involvement of financial institutions, including remittance agents, allows us to deepen our understanding of the financial behaviour of terrorist actors by identifying any commonalities and patterns in their financial transactions.

SUMMARY OF TF THREAT

While we cannot discount the possibility of a terrorist attack in Singapore, our assessment is that the TF threat of raising and moving of funds for terrorists and terrorist activities overseas is currently more pertinent in Singapore's context. Radicalised individuals pose the most salient TF threat to Singapore. Nevertheless, we remain cognisant of the global terrorism and TF threat posed by ISIS, AQ and JI, especially in light of the ideological influence these terrorist groups have over radicalised individuals in Singapore. In the next segment, we will discuss how these threats may seek to exploit vulnerable sectors in Singapore to raise and move funds for terrorists and terrorist activities overseas.

Law enforcement and supervisory authorities in Singapore are on the alert for emerging and potential TF typologies that may arise as a result of the COVID-19 pandemic. For instance, as travel between countries has been minimised and financial institutions and other service providers move towards offering more digitalised services, there may be an increased use of online transactions or virtual currencies/assets, including amongst terrorists, terrorist organisations and their supporters.

[12] *Investigations did not indicate that the other two had been involved in the raising of funds for ISB causes. They were eventually repatriated.*

TERRORISM FINANCING VULNERABILITIES AND RISKS

A country's vulnerability to TF is inherently linked to its TF threats and context. For Singapore, our status as an international financial centre, a transport hub with good connectivity and a substantial number of transient visitors, and physical proximity to countries with active terrorist groups, increase our exposure to TF threats.

AREAS AT RISK OF BEING EXPLOITED FOR TF

This section expands on the key areas that terrorists can exploit to raise, move and use funds. Other sectors not identified in this report are assessed to be low risk for TF, in light of their low exposure to TF threats and vulnerabilities, and taking into account known TF typologies and existing AML/CFT controls.

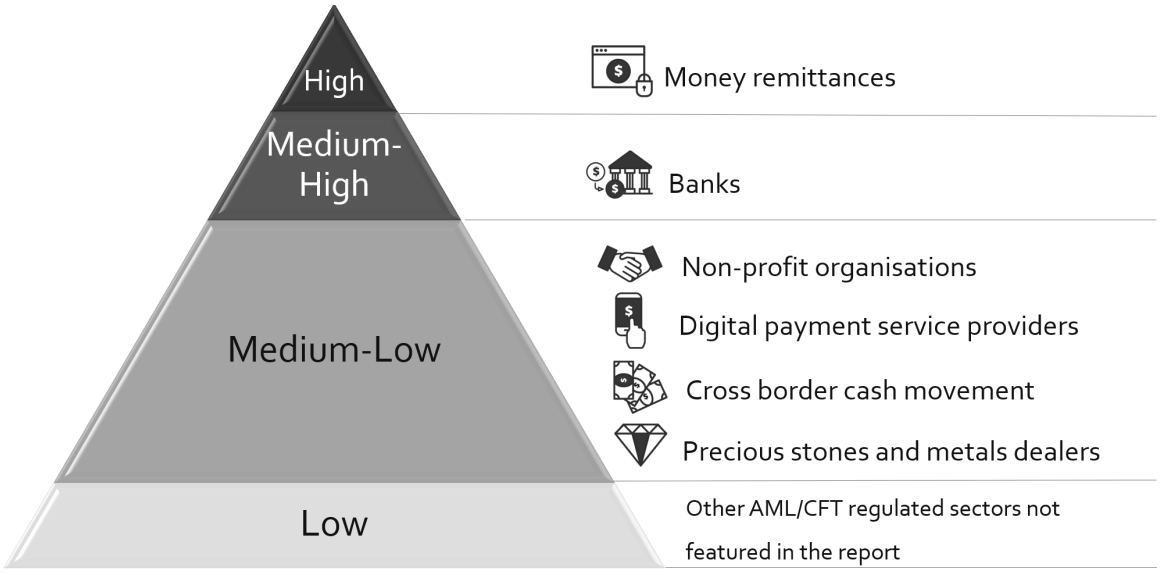

Diagram 1: TF Risk Ratings

MONEY REMITTANCES

HIGH RISK

KEY EXPOSURES TO TF THREAT AREAS

Terrorist financiers are known to use money remittance (cross-border money transfers) channels widely to move funds, both into, out of, and within the region. International typologies also suggest the use of unlicensed remittance channels (including *hawalas*) to facilitate TF fund flows.

TF threats have also materialised in this sector in Singapore. There have been five TF prosecutions in 2019 involving the movement of funds through money remittance agents by local sympathisers to support terrorism-related activities abroad. Based on investigations and cases prosecuted by law enforcement agencies to-date, unlicensed money remitters have not been used for TF activities in Singapore. Nevertheless, authorities in Singapore remain vigilant to such risks, in light of international typologies indicating abuse of this sector for TF.

KEY VULNERABILITIES

DEMOGRAPHICS OF USERS AND TRANSACTIONS WITH COUNTRIES MORE EXPOSED TO TERRORISM/TF RISKS | Money remitters often offer cheaper remittance services than banks and are, at times, more efficient. These characteristics appeal to Singapore's large population of migrant workers, who are the largest and most frequent groups of users of money remitters. Some of the countries in the region that local remittance agents frequently transact with are also known to be more exposed to terrorism/TF risks.

The demographics of users and known transaction corridors, relating to countries in the region that are more exposed to terrorism/TF risks, increase our susceptibility to foreign terrorism-related actors using Singapore as a base to raise funds amongst locals and foreigners here.

UNEVEN STANDARDS IN TF DETECTION CAPABILITIES ACROSS THE SECTOR | Through MAS' supervision of remittance agents in Singapore, improvements in the industry's level of risk awareness and AML/CFT controls have been observed over the years, although such improvements are not consistent across the sector.

Some of the more established players, which account for a substantial proportion of the total transaction volume in the sector[13], have deployed advanced data analytics capabilities to monitor transactions and detect TF-related red flags. However, remittance agents that are smaller in scale may not have sufficient resources to deploy advanced tools and have generally relied on more traditional know-your-customer and screening checks to detect TF. Thus far, known local TF cases have shown that TF transactions often involve small amounts and are funded from legitimate sources such as salaries and profits from businesses. This makes it challenging for remittance agents to detect potential TF cases.

Given that TF threats have materialised in this sector, MAS will continue to engage the sector to further strengthen their awareness of their TF risks and AML/CFT obligations. A TF thematic review of remittance agents and banks will be conducted to test their TF risk understanding and examine the effectiveness of their controls to detect and deter TF-related fund flows. The observations and findings from the TF thematic review will be distilled into a guidance paper to provide sound CFT practices for all financial institutions to adopt.

[13] *As of December 2019, there were 127 licensed remittance agents in Singapore.*

MONEY REMITTANCES (CONT.)

HIGH RISK

KEY VULNERABILITIES (CONT.)

USE OF UNLICENSED MONEY REMITTERS | We recognise that there is a segment of remitters that operate outside the regulatory ambit. There is limited information about this segment in terms of its size, number of players and transaction volumes. These players typically do not comply with existing AML/ CFT obligations such as customer due diligence, STR filing and record keeping requirements. The unregulated and inherently opaque nature of unlicensed remitters, as well as the typical users of their services increase their susceptibility to misuse for TF. Nevertheless, authorities have worked together to put in place processes to mitigate such risks, including leveraging on intelligence to identify unlicensed players and holistic upstream efforts to encourage users to utilise licensed remittance solutions through outreach and by providing easier access to licensed services.

BANKS

MEDIUM-HIGH RISK

KEY EXPOSURES TO TF THREAT AREAS

Terrorist financiers are known to use the banking sector to raise and move funds into and out of the region. These typologies are well reported in the region and around the world (e.g. due to the ubiquity of banks and ease of transacting through them).

Based on investigations and cases prosecuted by law enforcement agencies to-date, TF activities were not conducted through banks in Singapore, although a small amount of funds/assets relating to persons of interest would have been initially deposited with the banks. Nevertheless, we remain vigilant to the risk of Singapore's banking system being used as a conduit by terrorists and their financiers, given Singapore's position as an international financial centre. Pertinent to our identified TF threat of radicalised individuals providing funds for terrorism-related activities abroad, is the challenge of detecting transactions in banks that are small in amount and frequently indistinguishable from legitimate transactions.

KEY VULNERABILITIES

STATUS AS INTERNATIONAL FINANCIAL CENTRE | Singapore's status as an international financial centre exposes it to large international money flows.

In addition, our close geographical proximity to countries with active terrorist activities or terrorist groups makes us vulnerable to being used as a conduit for TF purposes. Singapore's sophisticated and interconnected banking system, with a wide range of accessible and efficient online financial services, also increases its risks of being exploited to raise or move funds for illicit purposes.

While we are cognisant of the possibility of our banking system being exploited for TF purposes, the banks' exposure to customers that pose higher TF risks, including from sectors such as foreign charities and NPOs[14], remains low.

CHALLENGE IN DETECTING TF SINCE TRANSACTIONS ARE OFTEN IN SMALL AMOUNTS AND INDISTINGUISHABLE FROM LEGITIMATE TRANSACTIONS | Banking transactions are closely linked to our everyday lives, from drawing salaries, paying bills and building up savings. Monies moved or stored by a terrorist or a sympathiser could be legitimate until they are used to fund terrorism-related activities. Furthermore, local cases have shown that radicalised individuals and sympathisers are known to transact in small amounts and fund terrorism-related activities from legitimate sources such as salaries or savings. It is thus not easy to differentiate these transactions from the individuals' normal financial activity in the absence of additional intelligence or indicators.

While banks' TF risk awareness and AML/CFT control measures are generally well developed, it is important to continue engaging the banks, through ongoing dialogue with MAS and law enforcement agencies, and industry events. This will enable them to keep abreast of the latest TF risks and typologies, and adopt relevant risk mitigation measures. As part of the TF thematic review of remittance agents and banks, MAS will examine the effectiveness of banks' processes and controls, including their use of more sophisticated monitoring capabilities, in relation to detecting and tracing fund flows linked to terrorist activities and responding quickly to authorities' information requests and directions.

[14] This would include foreign NPOs and charities which is a sector that has been traditionally identified as higher risk for TF based on international typologies and academic research. For instance, there has been known involvement of NPOs in TF activities in the region, many of which appeal for donations to help families of terrorists who have been incarcerated or killed during counter-terrorism operations. NPOs have also been known to be used as conduits in the region for funds received from the ISIS central command in the Middle East, to support ISIS-inspired terrorist groups. See section on NPOs for additional details.

NON-PROFIT ORGANISATIONS

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

International and regional typologies have shown that terrorist financiers are known to use NPOs as the means to raise, move and use funds. International aid flowing into liberated areas of Iraq and Syria could present opportunities for ISIS to generate funds. Within the region, pro-ISIS groups reportedly raise funds through supporters working in Muslim charities and *dakwah* centres, though not necessarily with the knowledge or approval of the organisations involved. Besides the possible diversion of legitimate funds for TF due to weak internal controls, the sector is also seeing an emergence of online fundraising movements that call on sympathisers to donate to families of jihadists, terrorist detainees and martyrs.

The local NPO sector comprises 3,084 entities[15]. These are predominantly registered charities, but also include a number of Companies Limited by Guarantee (CLGs), mosques and societies. These NPOs fall under the regulatory purview of the Commissioner of Charities (COC), Accounting and Corporate Regulatory Authority (ACRA), Majlis Ugama Islam Singapore (MUIS) and Registry of Societies (ROS) respectively.

Singapore's NPO sector is largely domestically-oriented. Only three out of ten charities engage in some form of overseas work and/or make donations and/or provide funding or services to beneficiaries outside Singapore[16]. An even smaller proportion of charities within this group conduct these activities in higher-risk jurisdictions. Mosques assist the fundraising efforts of Rahmatan Lil Alamin Foundation (RLAF), a registered charity under the purview of the COC, to support humanitarian relief efforts for people affected by natural disasters in the region. Other than supporting such efforts through RLAF, mosques are not allowed to raise or donate funds to any person or entity outside Singapore. CLGs and societies which are not part of the charity sub-sector, are even more domestically-focused and would typically not be involved in foreign fundraising.

Thus far, there has been no indication of foreign sources of funding flowing in to Singapore via our local NPO sector to support domestic terrorism-related activities, nor has there been any indication of funds raised by local NPOs being moved to fund terrorism-related activities abroad. Notwithstanding, we are cognisant of the possibility that funds raised in Singapore for charitable purposes, in particular for humanitarian relief use in or near conflict and other crisis zones, could be diverted for TF purposes.

KEY VULNERABILITIES

Given that the diversion of funds from local NPOs for TF has been identified as a threat, the charity sub-sector which has relatively more exposure to overseas activities, is assessed to be more vulnerable to TF.

VARIED LEVELS OF AWARENESS OF TF RISKS | Findings from surveys and focus group discussions indicate a higher level of TF risk awareness in recent years amongst charities. Some charities have provided training for staff and volunteers to raise awareness and understanding of TF risks. The COC has also collaborated with various partners including academics to conduct sharing sessions and focus group discussions to enhance the charities' TF risk understanding. However, the level of TF risk understanding still varies amongst the registered charities[17]. Larger charities tend to have a better understanding of risk management. While the others may not, they are keen to find out more about appropriate measures to protect themselves against potential TF abuse. Hence, there is room for improvement in relation to the awareness and understanding of TF risks amongst registered charities.

[15] *As at 31 December 2019.*
[16] *Based on a survey conducted by the COC in May 2018, as part of Singapore's Charity Sector Vulnerability Assessment.*
[17] *Focus group discussions indicate that less than half of the participating charities were able to cite at least one example of why charities might be vulnerable to TF abuse.*

NON-PROFIT ORGANISATIONS (CONT.)

MEDIUM-LOW RISK

KEY VULNERABILITIES (CONT.)

The COC plans to conduct more targeted outreach to the higher-risk sub-set of charities, to increase awareness of key TF risk indicators and educate them through the sharing of case studies.

GUIDELINES, REPORTING MECHANISMS ON THE DISBURSEMENT OF FUNDS TO BENEFICIARIES AND DUE DILIGENCE | The low awareness of TF risks appears to be interlinked with other vulnerabilities noted from the assessment of the charity sector. Charities may not be as sensitive to detect suspicious activities or red flags and put in place adequate safeguards such as guidelines relating to overseas disbursement of funds or due diligence checks on external stakeholders. As such, these measures which are necessary to help charities detect suspicious transactions before, during and after the disbursement of funds overseas and to prevent the organisation from being used as a conduit for TF, may not be formalised or comprehensive.

That said, as part of the COC's regulatory regime to mitigate TF risks in the charity sector, checks are conducted to ascertain that applications for permits to raise funds for foreign charitable purposes are bona fide.

DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

Digital payment tokens (DPTs, also referred to as virtual assets/currencies) have emerged as a potential means for terrorist financiers, particularly tech-savvy militants, to raise and move funds across borders. Known international typologies include using DPT service providers to solicit DPTs online and then transfer the DPTs through multiple hops within a short duration to a wallet address associated with extremist sites.

However, there is as yet, no evidence of widespread usage of DPTs[18]. This could be because many of the technological innovations are unavailable in terror ridden zones such as Mindanao, Philippines, due to the absence of infrastructure in financial technologies and poor internet connectivity[19]. Nonetheless, arising from COVID-19, we have noted indications that terrorists and terrorist groups may be looking to make greater use of virtual currencies to support their nefarious activities, and this is an area which the relevant authorities in Singapore continue to monitor closely.

While there are also no known domestic TF cases involving the use of DPTs, we are cognisant of the higher inherent TF risk posed by the anonymity, speed and cross-border nature of transactions facilitated by DPT service providers, and we are watching this space closely. Aligned with international standards, DPT service providers in Singapore are subject to the Payment Services Act (PS Act) and corresponding AML/CFT regulations, which came into effect on 28 January 2020. Singapore's status as a FinTech hub has made it an attractive place of business for DPT exchanges, and our high digital literacy increases the likelihood of the adoption of DPTs. However, DPT activities remain relatively small (in terms of volume) compared to the traditional sectors and have yet to gain significant traction in Singapore[20].

KEY VULNERABILITIES

ANONYMITY, SPEED AND CROSS-BORDER NATURE OF TRANSFERS ASSOCIATED WITH DPTS | DPTs are susceptible to TF abuse because of: (i) the anonymity they offer; (ii) the convenience they provide as a near-instantaneous value transfer medium; and (iii) the cross-border nature of the transactions[21]. Anonymity-enhancing features (such as mixers, tumblers and Internet Protocol anonymisers) and privacy coins make DPTs more attractive for TF, as they enable terrorists and their financiers to obfuscate their identities, counterparties and physical locations. Their cross-border nature and ability to make high-value transactions quickly make this an attractive means to raise or move assets compared to more traditional methods. These factors make DPT transactions that are potentially TF-related more challenging for law enforcement agencies to trace and detect.

[18] RSIS Southeast Asia Report, page 9: "Indonesia's Financial Intelligence Unit informed that PayPal and Bitcoin are often used by militants to move funds to avoid detection by the authorities. The source of money via PayPal had originated from Bitcoin. However, the scale of their usage may be limited to tech-savvy militants only."

[19] RSIS Southeast Asia Report, page 24: "Technological innovations for finances are unavailable in Mindanao due to the absence of infrastructure in financial technologies and poor internet connectivity."

[20] MAS' Financial Stability Review Box B (November 2018), "Monitoring Digital Token Markets: An Early Look at Frameworks and Techniques".

[21] FATF's Guidance for a risk-based approach to virtual assets also affirms that virtual assets have characteristics such as increased anonymity, which may make them more susceptible to abuse by criminals, money launderers and terrorist financiers.

DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

MEDIUM-LOW RISK

KEY VULNERABILITIES (CONT.)

LACK OF ROBUSTNESS OF AML/CFT CONTROLS AND TF RISK UNDERSTANDING DUE TO NASCENT REGIME | Given that DPT service providers only recently came within MAS' regulatory ambit, the levels of TF risk awareness and AML/CFT controls are lower compared to the other financial sectors. In this regard, MAS has stepped up its supervisory and engagement efforts. MAS has also organised and participated in a series of industry engagement sessions to raise the industry's awareness of ML/TF in the lead up to the enactment of the PS Act. Robust AML/CFT-focused licensing checks have been instituted to uphold standards across the sector.

MAS will also apply a risk-based approach in its supervision of DPT service providers, which will include inspections to examine the sectors' effectiveness in combatting TF. This will be complemented by MAS' surveillance of the DPT sector to identify areas or entities of higher risks, and proactively detect entities that may be operating or providing DPT services illegally without a licence.

CROSS-BORDER CASH MOVEMENT

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

Terrorist financiers around the world have been known to use cash couriers as a means to physically move funds across borders to finance their activities. Unlike transactions in the regulated sectors, cash transactions do not leave a digital footprint.

These typologies are well reported in the region, perpetuated by cash-intensive economies, porous borders, loose maritime boundaries and proximity to conflict zones. The known routes do not involve Singapore and there is no indication of cross-border cash movement[22] (CBCM) relating to TF in Singapore to-date[23].

Nevertheless, we are cognisant that our proximity to countries with active terrorist groups makes us vulnerable as a potential location to pick up and transit funds for foreign terrorist fighters travelling to conflict zones.

KEY VULNERABILITY

Singapore has stringent border controls and a robust framework to detect illicit CBCM. This stems from strong collaboration and intelligence sharing between various law enforcement agencies, including the Immigration & Checkpoints Authority, Singapore Customs and CAD. Nevertheless, our sectoral deep-dive has identified the following vulnerability.

ANONYMITY ACCORDED TO SMALL AMOUNTS OF MONIES BROUGHT ACROSS BORDERS | Singapore continues to detect a small number of radicalised individuals intending to travel out of the region to fight alongside ISIS. The risk of cash being carried out of Singapore to fund terrorist activities abroad remains present, especially if these individuals should leave Singapore undetected. International typologies also recognise that given the small amounts of monies typically associated with terrorism, that they would frequently fall below the reporting threshold[24]. To mitigate these risks, the use of targeted intelligence and close inter-agency cooperation are important.

Thus far, the monies associated with known local TF cases are typically small and fall well below the CBCM reporting threshold. The small amounts associated with TF therefore accords anonymity if they are passed through our borders.

[22] This analysis addresses the physical movement of cash and bearer negotiable instruments across Singapore's borders, and does not address the cross-border movement of funds, such as through electronic transfers, and domestic transfers.

[23] Based on the analysis of cases so far, the common purposes of CBCM include: business, gambling and personal use. The proportion of non-declaration cases was also found to be low compared to the number of Cash Movement Reports filed, and none of them had TF links. Most of the non-declaration cases related to a lack of awareness or pure absentmindedness. In these cases, there were no strong suspicions that the sources of monies were tainted or linked to any form of illicit activities, and there were usually supporting documents to substantiate the source or destination of the funds.

[24] Singapore's reporting threshold for CBCM is S$20,000.

PRECIOUS STONES AND METALS DEALERS

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

International and regional typologies indicate relatively few instances of terrorist financiers using precious stones and precious metals (PSPMs) to move or raise funds for terrorism. However, PSPMs have high intrinsic value in a relatively compact form and tend to maintain or increase their value over time. This means that PSPMs could be a good store of value and accepted as an alternative to monies, whether in Singapore or in conflict-ridden and terror-prone states.

Following Singapore's implementation of a cash transaction reporting regime for precious stones and metals dealers (PSMDs) in 2014, we have in March 2018, established a division within the Ministry of Law (MinLaw) to supervise PSMDs for AML/CFT. From April 2019, the PSMD sector has been subjected to a full suite of AML/CFT supervisory measures under the Precious Stones and Precious Metals (Prevention of Money Laundering and Countering the Financing of Terrorism) Act (PSPM Act).

This assessment covers the regulated dealers[25] of precious metals, precious stones and precious products as defined within the PSPM Act[26]. The sector has a diverse range of value-chain activities, including retailing in physical stores, wholesale/ distribution, manufacturing, second-hand goods dealing and online platforms. Locally, there are no known cases of PSPMs being used for TF activities to-date. Nevertheless, the inherent characteristics of the sector and the nascency of supervisory efforts may pose vulnerabilities to misuse for TF.

KEY VULNERABILITIES

VARIED LEVELS OF AWARENESS OF TF RISKS AND AML/ CFT CONTROLS DUE TO NASCENCY OF REGIME | Being a sector with a diverse range of activities and scale of operations, the levels of TF risk understanding and AML/CFT controls are varied. Further, the sector was only subjected to the full suite of AML/CFT supervisory measures from April 2019.

MinLaw's assessment revealed that the subgroups of (i) precious stones; (ii) precious metals; and (iii) precious products have a higher level of TF vulnerability due to lower levels of risk awareness and controls. MinLaw plans to conduct outreach to raise the sector's awareness of their TF risks. MinLaw will continue to prioritise the monitoring and supervision of higher-risk PSMDs.

PRECIOUS STONES | The ***retail sector for precious stones*** is assessed to have a lower level of awareness and controls. This vulnerability is amplified for dealers that are more likely to transact with transient customers. There is also a higher vulnerability in the second-hand dealers market, where a standardised valuation methodology for the re-sale of precious stones (due to the multiple variations in carat, cut, clarity and colour for precious stones) will be difficult to implement.
PRECIOUS METALS | ***Second-hand dealing of precious metals*** is common as the purchase and resale of gold or silver bullions as an asset are prevalent amongst the investment savvy crowd. This subgroup is assessed to have a lower level of awareness and controls.
PRECIOUS PRODUCTS | Precious products are most likely to dominate the ***second-hand dealing market.*** However, there is limited information on how these dealers operate and with whom they transact.

DIFFICULTY IN TRACING SPECIFIC ITEMS | The difficulty in tracing specific items and the global market for PSPMs make it easier for terrorist financiers to exploit cross-border, multi-jurisdictional situations in order to obscure paper trails, rendering it more difficult for law enforcement agencies to conduct investigations.

[25] Regulated dealing refers to the (a) manufacturing; (b) importing or possessing; (c) selling; and (d) purchasing for resale of any precious stone, precious metal or precious product; and (e) selling or redeeming asset-backed tokens.

[26] As at 24 April 2019, there were 1,921 registered dealers in the PSMD sector, operating 2,418 outlets amongst them.

CONCLUSION

The global terrorism landscape is constantly evolving. For example, the threat posed by right-wing extremism has increased and in some countries, is even starting to present as a serious threat. Consequently, TF risks, both internationally and domestically, will continue to change. Singapore recognises that we need to remain vigilant to both existing and emerging threat as well as vulnerabilities in relation to terrorism and more specifically TF.

Singapore has thus developed and implemented a comprehensive whole-of-government approach to identify, monitor and mitigate TF risks. This includes working closely with the private sector and academia to enhance our collective understanding of TF risks. This risk assessment outlines the key TF threats and vulnerability areas within our national CFT system, taking into account our collective experience over the years. It will aid authorities in focusing our CFT efforts on the higher-risk areas, and will also be used to formulate our national CFT strategy. It also provides private sector stakeholders with an updated overview of Singapore's TF risks, and they should continue to remain vigilant to existing and emerging TF risks.

Singapore remains committed to combatting TF through our continuous efforts to monitor and assess potential and emerging TF threats and vulnerabilities, as well as develop and implement effective and risk-targeted law enforcement, regulatory and supervisory measures to mitigate the TF risks faced by Singapore. Given the global nature of terrorism and TF, we will continue to maintain close working relationships with our overseas law enforcement, intelligence, regulatory and supervisory counterparts, and contribute actively to regional and international forums such as the FATF, the Asia/Pacific Group on Money Laundering, the CTF Summit and the INTERPOL's Project PACIFIC Working Group.