SOCIAL MEDIA AND TERRORISM FINANCING

A joint project by Asia/Pacific Group on Money Laundering & Middle East and North Africa Financial Action Task Force

Project Co-leads: Egypt and Malaysia

APG Secretariat
Locked Bag A3000
Sydney South
New South Wales 1232
AUSTRALIA
Tel: +61 2 9277 0600
E mail: mail@apgml.org
Web: www.apgml.org

Contents

Abbreviations and Terminology

APG	Asia/Pacific Group on Money Laundering
CHS	Content Hosting Services, which allow users to create or upload content, for example, text, photos or videos, which is almost always public with less of a focus on connections/networks and more of a focus on general public consumption.
Crowdfunding Services	Allow users to fund a project, venture or cause within a bounded system by raising small amounts of money from many individuals.
FATF	Financial Action Task Force
FTF	Foreign terrorist fighters
Global Network	Global anti-money laundering/combating the financing of terrorism (AML/CFT) network
ICS	Internet Communication Services, which allow two or multiple users to communicate in-real time over the internet normally in text but also in voice and video and with images
IPS	Internet Payment Services
ISIL	Islamic State of Iraq and the Levant
MENAFATF	Middle East & North Africa FATF
MPS	Mobile Payment Services
MVTS	Money value transfer services
NPM	New Payment Methods
NPP&S	New payment products and services
Risk	Is a function of three factors: threat, vulnerability and consequence
SMP	Social Media Platforms
SMR	Suspicious Matter Report
SNS	Social Networking Services, which allow users to create public or semi-public profiles and other content, articulate with other users they share a connection with and also view and interact with the content these other users have created.
T	Terrorism
TF	Terrorism financing
TFI	Terrorism financing indicator
TI	Terrorism indicator
Threat	Is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the TF context this includes terrorists, terrorist groups and their facilitators, their funds, as well as past, present and future TF activities.
TPS	Traditional Payment services
Vulnerability	Comprises those things that can be exploited by the threat or that may support or facilitate its activities. In this context it could include the wider financial system and mechanisms or products used to move and store funds. Vulnerabilities may also include the features of a particular sector, a financial product or type of service that make them attractive for TF purposes.

Executive Summary

The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified with terrorist attacks across the globe carried out, for example, by small cells, and the threat posed by terrorist organizations such as Islamic State of Iraq and the Levant. Irrespective of the differences in financial requirements between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist actors seek to ensure adequate revenue and management of funds. The global anti-money laundering/combating the financing of terrorism (AML/CFT) network (Global Network) has recognised that social media services are susceptible to be abused for terrorism financing (TF).

To support Asia/Pacific Group on Money Laundering (APG) and Middle East & North Africa FATF (MENAFATF) members to combat TF, this report identifies techniques and trends, including indicators, associated with the abuse of social media services for financing acts of terrorism, individual terrorists or terrorist organisations. This report is co-led by Egypt and Malaysia.

27 jurisdictions responded to the report questionnaire and provided some case examples of TF through abuse of social media services. These cases show social networking services (e.g. Facebook), content hosting services (e.g. YouTube), crowdfunding services (e.g. GoFundme.com) and Internet Communication Services (e.g. WhatsApp) are being abused in a variety of ways for TF, as follows:

- Social networking and content hosting services are primarily used to solicit donations, promote terrorism through propaganda and radicalization. Consistent with the current limited integration of payment methods in these services, most cases provided as part of the report show donated funds are moved using traditional payment methods i.e. banks.

- Internet communication services were used in many cases to privately communicate with campaigners or terrorist groups. They mainly discussed means of support and payment methods. The vulnerabilities of these services, for example, encrypted communication and the number of active users, are factors driving their abuse for TF.

- Crowdfunding services were used in a number of cases, with campaigners often disguising the use of funds for humanitarian causes. These services often integrated traditional and new payment services, which due to their vulnerabilities may hinder TF detection and investigation by competent authorities.

To assist APG and MENAFATF members to combat TF, this report examines key challenges in the detection, investigation and prosecution of TF through the abuse of social media services, and includes measures to assist competent authorities overcome these challenges.

In acknowledgment of the prominent role of social media services in daily life and as key partners in global counter terrorism efforts, this report also highlights a number of avenues APG and MENAFATF members can work collaboratively with social media companies to prevent their abuse for TF. These avenues include increasing public awareness, supporting the removal of terrorism and TF related content, and counter-messaging.

Introduction

1. The Financial Action Task Force (FATF) in its 2015 report recognised social media services as susceptible to abuse for raising terrorist funds. The report acknowledged the prominent vulnerabilities associated with social media services, including anonymity and access to a wider range and number of potential sponsors or sympathizers[1]. Since this report, other publications have echoed similar views on the abuse of social media services for terrorist propagation and radicalisation, especially in relation to Islamic State of Iraq and the Levant (ISIL).

2. In 2016 the Asia/Pacific Group on Money Laundering (APG) and Middle East & North Africa FATF (MENAFATF) initiated a joint typologies project to identify techniques and trends associated with the abuse of social media services for financing acts of terrorism, individual terrorists or terrorist organisations. The purpose of the project is to assist APG and MENAFATF members, and the Global Network, to combat TF. This report is the primary output of the joint project.

Objectives and Structure

3. This report has three primary objectives, which are reflected in the structure of the document, as follows:

- **Part one:** Provides an overview of the key features of the global social media and TF environments.
- **Part two:** Examines the methods and trends of TF through abuse of social media services, and develops indicators for use by competent authorities to combat TF.
- **Part three:** Highlights the challenges in detecting, investigating and prosecuting TF associated with social media within the APG and MENAFATF regions, and offers measures for overcoming these challenges and collaborative approaches to prevent the abuse of social media services for terrorism and TF.

Scope

4. This report aims to provide an updated and more precise understanding of TF through the abuse of social media services, by analysis of case studies primarily provided by APG and MENAFATF members. While this report includes some discussion on new payment products and services (NPP&S) that are embedded in some social media services, it does not include an in-depth analysis of these products and associated level of ML/TF risks[2]. For example, this report does not distinguish between the different vulnerabilities of embedded Traditional Payment Services (TPS), Internet Payment Services (IPS) or Mobile Payment Services (MPS), such as PayPal, credit card payments, or bank transfers used in different crowdfunding sites; or peer-to-peer payment systems used in Internet Communication Services.

[1] FATF Report on Emerging Terrorist Financing Risks (2015)

[2] Please see FATF Report on Money Laundering Using New Payment Methods (2010) for discussion on the risks associated with New Payment Methods.

5. Furthermore, as most social media services operate through internet browsers on stand-alone computers and applications on mobile devices, this report does not distinguish between the different platforms social media services may operate on.

Methodology

6. The project was co-led by Egypt and Malaysia and supported by the APG and MENAFATF secretariats. The report relies on data from members of the global AML/CFT network and on open-source material, including reports issued by governments or international organisations, and risk assessments undertaken by relevant jurisdictions.

7. The project team collected information on abuse of social media services for TF through a questionnaire (see Appendix B), which included a request for relevant case studies and questions on the following issues:

- National policy, legal, and regulatory measures;
- Monitoring and surveillance;
- Investigation and prosecution of TF cases relating to social media;
- International cooperation;
- Collaboration with the private sector;
- Capacity building; and
- Counter-messaging.

8. The social media project questionnaire was disseminated to all APG and MENAFATF members/observers, and the AML/CFT Global Network. A total of 27 jurisdictions responded to the questionnaire including 14 APG members/observers[3], five MENAFATF members[4] and seven other members of the Global Network[5].

Disclaimer

9. This report names a number of social media and other associated companies, primarily in case studies. The authors of this report would like to stress that these companies are not supporting terrorism, TF or other criminal activities in any form. Rather, these companies are key partners in global counter terrorism efforts, and have been abused by individual terrorist, terrorist groups or criminals.

[3] Australia, Bangladesh, Bhutan, Brunei, Japan, Macau, China, Malaysia, Singapore, Thailand, United States, Vietnam, Lao PDR, DPRK and Kiribati

[4] Kuwait, Sudan, Jordan, Yemen and Egypt

[5] Azerbaijan, Czech Republic, Ethiopia, Montenegro, Spain, Turkey and Zimbabwe

Part One: Key Features of Global TF and Social Media Environments

10. This section provides an overview of the key features of the global TF and social media environments. It includes a brief discussion of the evolving nature of terrorism and TF methods and trends; and distinguishes between different social media services, their use, and vulnerabilities to TF abuse.

1.1 Evolving Nature of Terrorism and TF Methods and Trends

11. The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organisations such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfil their basic need to generate and manage funds is also evolving.

12. Terrorist organisations use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation; and social services. These financial requirements are usually high for large terrorist organisations, particularly those that aim to, or do, control territory. In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management[6].

13. The FATF and members of the Global Network have developed a large body of research examining TF methods and trends. In general, this research shows terrorist groups and individual terrorists rely on numerous sources of funds, from both criminal and legitimate activities, which they move, including internationally, using a variety of methods to end-use destinations. The FATF Report on Emerging Terrorist Financing Risks (2015) discusses traditional and emerging TF methods and trends. This report highlights traditional methods of generating funds including private donations; abuse and misuse of non-profit organizations; extorting local and diaspora populations and businesses; kidnapping for ransom; self-funding; legitimate commercial enterprise; and state sponsorship. Traditional methods to move funds include transfers through banks; money value transfer systems and the physical transportation of cash.

14. While the 2015 FATF report and subsequent research highlights that traditional TF methods and trends are prevalent today and remain a significant TF risk, emerging or new methods of generating and moving funds have been identified, particularly in association with foreign terrorist fighters (FTFs) and ISIL. For FTFs, revenue generation is primarily in the form of self-funding and support from recruitment and facilitation networks with funds moved via traditional methods and NPP&S including virtual currencies, prepaid cards and IPS[7]. For ISIL, sources of revenue include illicit proceeds from occupation of territory; kidnapping for ransom; donations including by and through NPOs; and material support from FTFs with funds moved via traditional methods and NPP&S[8].

15. In addition to the above TF methods and trends, research by the FATF and members of the Global Network highlights the abuse of social media services to generate and move funds to support the financial requirements of terrorist groups and individual terrorists. For example,

[6] See FATF Report on Emerging Terrorist Financing Risks (2015) for a detailed discuss of terrorist organisations use funds.

[7] FATF Report on Emerging Terrorist Financing Risks (2015)

[8] FATF Report on Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL) (2015)

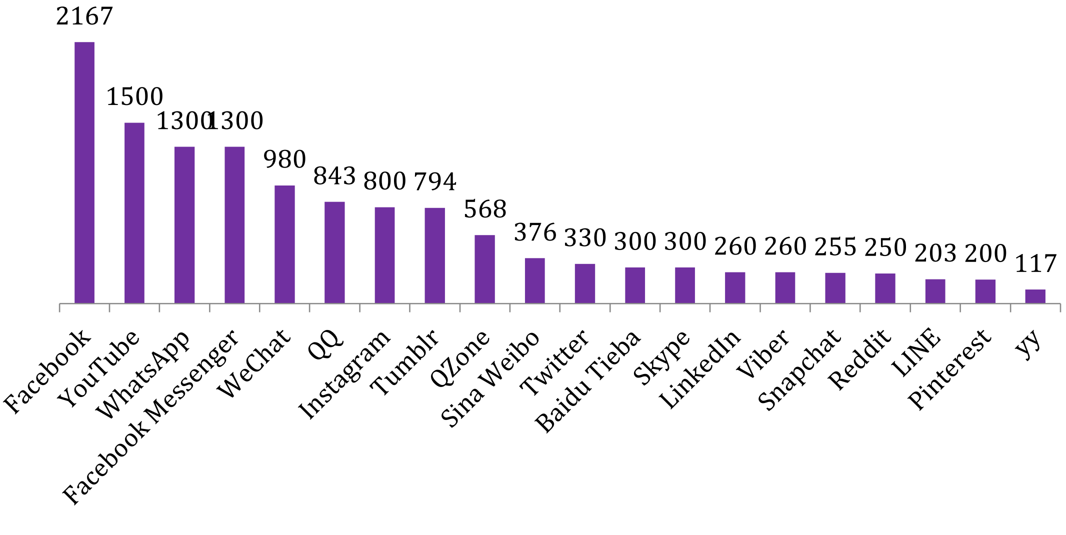
FATF's 2015 Report includes a discussion on how individuals associated with ISIL called for donations on Twitter. This report aims to supplement previous research on TF and provide key indicators for use by competent authorities to combat the financing of terrorist groups and individual terrorist via social media services.

1.2 Increasing Use and Evolution of Social Media Services and Vulnerabilities to Abuse for TF

16. Consumer needs and market share continue to drive the use and evolution of social media services. Since 2004 global use of social media services has increased dramatically. In 2010 there were 0.97 billion social media users, in 2015 there were 2.14 billion users, and in 2017 there were 2.46 billion[9] users, which equates to approximately 32% of the global population[10]. It is estimated that by 2021, 3.02 billion people will be using some form of social media service[11]. Facebook (launched in 2004) is the most popular social media service with 2.18 billion monthly active users, followed by YouTube and WhatsApp with 1.50 billion and 1.3 billion monthly active users, respectively (see Chart 1).

17. Commensurate with the dramatic increase in use, social media companies continue to develop their services to meet consumer needs, and this continually challenges definitional consensus of the term social media and research on their vulnerabilities to TF. In a 2015 review of the term social media and social media regulation, Obar and Wildman identified four commonalities of social media services, which are: (i) social media services are Web 2.0 Internet-based applications, (ii) content is principally user-generated, (iii) individuals and groups create user-specific profiles designed and maintained by a social media service, and (iv) social media services facilitate the development of online social networks by connecting a profile with those of other individuals and/or groups[12].

Chart 1: Top 20 Global Social Media Services, Ranked by Number of Active Users (in Millions) as of January 2018[13]



[9] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[10] Global population of 7.55 billion in 2017 - http://www.worldometers.info/world-population/

[11] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[12] Obar, Jonathan A; Wildman, Steve. Social media definition and the governance challenge: An introduction to the special issue (2015)

[13] Chart modified from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

18. For the analysis of case studies in this report, social media services have been categorised as follows:

- *Social Networking Services (SNS)* allow users to create public or semi-public profiles and other content, articulate with other users they share a connection with and also view and interact with the content these other users have created[14]. Common SNS include Facebook, Twitter and Instagram.

- *Content Hosting Services (CHS)* allow users to create or upload content, for example, text, photos or videos, which is almost always public with less of a focus on connections/networks and more of a focus on general public consumption. Common CHS include YouTube, Vimeo and Blogger.

- *Crowdfunding Services* allow users to fund a project, venture or cause within a bounded system by raising small amounts of money from many individuals. Common crowdfunding services include GoFundme.com, Youcaring.com and Kickstarter.com.

- *Internet Communication Services (ICS)* allow two or multiple users to communicate in-real time over the internet normally in text but also in voice and video and with images. Common ICS include WhatsApp, Instant Messenger, WeChat, and Snapchat.

19. Cases provided as part of this report show individual terrorists, terrorist groups and/or sympathizes are exploiting social media services to facilitate TF. The FATF in its 2015 report recognised prominent vulnerabilities associated with social media services including anonymity, access to a wider range and number of potential sponsors or sympathizers, and the relative ease with which some social media services may be integrated with payment methods and services. The Regional Risk Assessment on Terrorism Financing in 2016 involving South-east Asia and Australia also highlighted vulnerabilities associated with social media services and crowdfunding services, including that these services are widely accessible at a low cost and have global reach. Terrorists and their financiers mainly use social media services as communication channels to solicit funding. The volume of legitimate funding activity that occurs on these platforms may also mask the small amount of illegitimate activity. Most online activities are highly visible, and without sophisticated understanding of computing and use of encryption tools, can leave a trail that can be used for successful prosecution.

20. Input provided by APG and MENFATF member/observers echoed vulnerabilities identified by the FATF. APG and MENAFATF member/observers noted the following primary vulnerabilities:

- *Internet and mobile phone penetration:* Increased internet and mobile phone access facilitates greater abuse of social media services for TF.

- *Ease of access:* The ability to access social media services through multiple devices (e.g. via mobile phones, tablets, PCs, etc.) provides greater mobility and outreach creating new challenges for combating terrorism and TF.

- *Anonymity:* Ease by which users may set up fictitious accounts to use social media services; ability to make anonymous donations on crowdfunding sites.

- *Encryption:* The wide use of encryption mechanisms to secure messages and conversations, especially in ICS, provides terrorists/terrorist organizations with obscure channels to communicate and exchange financial data to conceal their

[14] http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full

transactions. This creates serious challenges for competent authorities in detection and disruption of their activities.

- *Immediate / real-time nature of user-generated content:* Social media services allow users to publish content immediately and/or communicate in real-time.

- *Generation of funds:* Some social media services allow users to generate income through advertisements.

- *Ease of modification*: Most social media services data can be subject to alterations by users or even complete removal in real-time. Some ICS even allow for self-destruct messages that can only last for a desired time limit, leaving no trail for tracking.

- *Provision of propaganda tools:* Most social media services provide means for sharing multimedia contents (e.g. videos, photos, sound files, etc.), allowing terrorists/ terrorist organizations to demonstrate power and influence potential sympathizers.

21. While an in-depth analysis of integrated payment methods and services is outside the scope of this report, it is important to identify which social media services are currently using NPP&S and some of the key vulnerabilities associated with these products and services. Currently the majority of SNS, CHS and ICS are not specifically designed to conduct financial transactions; however, to varying degrees, particularly ICS, have begun to incorporate IPS and/or MPS. For example, WeChat Pay allows user to make mobile payments and send money between contacts[15], and WhatsApp has recently launched a peer-to-peer payment system in India[16]. In contrast, consistent with the nature of crowdfunding services, they use a variety of TPS and IPS to raise funds such as payment by cards (debit, credit, and prepaid) and PayPal.

22. The 2010 FATF Report on Money Laundering Using New Payment Methods and subsequent FATF publications highlight some vulnerabilities of IPS and MPS that may facilitate abuse of social media services, particularly crowdfunding services, for TF. These include:

- *Non-face-to-face relationships and anonymity:* IPS and MPS may allow for non face-to-face business relationships, which without adequate customer identification and verification measures may impact on the service providers' ability to identify the individuals involved in transactions.

- *Geographical reach:* IPS and MPS may allow for global use for payments or transferring funds. Furthermore, service providers may be located in a jurisdiction with weaker AML/CFT controls.

- *Methods of funding:* IPS and MPS allow accounts and transactions to be funded in a number of different ways with IPS and MPS that may allow funding through cash (through a network of agents) and third parties, which increases AML/CFT risks.

- *Access to cash:* IPS and MPS may allow cash withdrawals.

- *Segmentation of services:* IPS and MPS payments and transactions may be conducted via and/or facilitated by multiple parties, which may be spread across several jurisdictions.

[15] https://pay.weixin.qq.com/index.php/public/wechatpay

[16] http://indianexpress.com/article/technology/social/whatsapp-payments-feature-live-india-on-android-ios-here-are-details-on-privacy-policy-5060367/

Part Two: Analysis of Cases in which Social Media Services were abused for TF

23. This section of the report examines the abuse of social media services for TF in the APG and MENAFATF regions through case studies. For each of the below subsections, the analysis focuses on how social media services are used for TF and for each case study, a non-extensive list of indicators (I) is identified. All indicators are included in a summary table in Appendix B.

24. In addition to the abuse of social media services for TF, the case studies have overwhelmingly shown a trend in the misuse of social media services for terrorism purposes, which may be conducted concurrently with TF elements or standalone. For example, in some case studies persons publicly pledged allegiance to terrorist organisations, and used social media services for radicalization and the distribution ISIL propaganda. The full text of the case studies related to abuse of social media services for terrorism are included in Appendix A of this report.

2.1 Channels used for Terrorism Financing

2.1.1 Social Networking Services (SNS)

25. Case examples provided as part of this report show SNS are primarily used to call for funding (see case 1 as an example) and/or to initially cast the net for potential sympathisers to support terrorist groups, individual terrorists or family members of the terrorists (see cases 2 and 3 as examples). SNS were also abused by terrorists or sympathisers to promote their donation campaigns and to communicate with individuals located in the conflict zones. This finding is consistent with previous research by the FATF and members of the Global Network, and consistent with the limited ability for payments or financial transactions to be made via SNS. The large number of SNS users provides perpetrators a valuable channel to propagate radical ideologies and inspire other SNS users to support terrorists or participate in terrorist financing activities. Visual media portraying terrorist elements were also used in these platforms to influence potential sympathizers. Additionally, these platforms were used by individuals and small cells to declare and publicise allegiance to UN designated terrorist organisations, such as ISIL. SNS were also abused by terrorists or sympathisers to promote their donation campaigns and to communicate with individuals located in the conflict zones.

Case Study 1 – Abuse of a SNS to solicit donations

In 2014, the Long War Journal[17] reported that person A was collecting funds for a school to instruct students in Al-Nusrah Front's (also known as Jabhat al Nusra) version of Islamic jurisprudence and the proper way to wage jihad. Several advertisements were posted on Twitter soliciting donations for the school **(TFI.1)**. In 2014, person A also posted messages and images to his Twitter account soliciting funds for jihad and inviting donors to contact him through his Twitter account, using the following tweets (translated) "#Immam_Al-Shafi'i_Institute. To donate and contact the Institute through [the Australian. Twitter handle] Increase your giving." In addition, person A posted an image on Twitter with the image soliciting funds for jihad and inviting donors to contact him. The image stated the following: "To support, please contact [the Australian. Twitter handle], member of the Al-Nusrah Front Sharia Commission." **(TFI.2 and TFI.3)**. Australia listed Person A pursuant to UNSCR1373 in 2015.

Source: Australia

[17] Foundation for Defense of Democracies that tracks Islamic extremist news and social media posts

Indicators

TFI.1	Use of SNS to call for funds to support specific organisation (a school) that involves in terrorism-related extremism and radicalization movement.
TFI.2	Use of SNS via messages and pictures to call for funds from donors to support a known terrorist front.
TFI.3	Use of SNS to initiate contact with potential donors for donation.

Case Study 2 – Abuse of a SNS to solicit donations and promote terrorism

This case relates to the charity "Perle d'espoir", which led to France's first prosecution of a charity for TF. This charity was created in 2012 to raise funds for humanitarian projects in foreign jurisdictions **(TFI.4)**. After a donation campaign, in August 2013 this charity bought two ambulances and medical material to build a hospital. Pictures were posted on Facebook to attest to the reality of the project and communicate with donors **(TFI.5)**. At the same time, one of the main members of this association was claiming on his personal Facebook profile that he had met with jihadists and received training to fire weapons **(TFI.6)**. Later, a new call for funds was made on social networks to buy sheep for the Eid celebration. Three members of the association were planning to deliver the funds raised. French customs control at the airport revealed each of the three members was carrying €9,900 (below the declaration threshold) **(TFI.7)**. In January 2014 assets of the association and four other members were frozen by an administrative order for six months. But two days after this order was issued, one of those individuals left France, and wrote on his Facebook wall that he had joined a terrorist organisation. He continued to post about his daily life there on Facebook, for six months, before returning **(TFI.8)**. In 2014, the association was dissolved, and two members were arrested for TF and criminal conspiracy in connection with a terrorist enterprise – most funds raised were used to support FTF **(TFI.4)**. Facebook public messages and pictures were used as evidence by law enforcement authorities.

Source: Case from France and originally included in the 2016 APG Yearly Typologies Report

Indicators

TFI.4	Use of SNS by charities to call for funds for humanitarian causes while funds were actually directed to support FTF.
TFI.5	A terrorism-related charity uses SNS to share visual media to attest legitimacy of their activities and communicate with donors.
TFI.6	Use of SNS by the members of the charity to portray involvement with terrorists including their weaponry training activities with terrorists.
TFI.7	Use of SNS to raise funds under the pretext of humanitarian cause then physically moving the funds across borders via several passengers and structuring the funds below declaration threshold.
TFI.8	Use of personal Facebook profile to declare joining a UN listed terrorist organisation and posting related daily life incidents.

Case study 3 - Use of SNS for soliciting funds for families of terrorists

A fundraising campaign claimed to provide pastoral care and financial support to the families of convicted and accused ISIL terrorists. It became the subject of four SMRs reported between 4 November 2016 and 23 May 2017 after featuring in numerous media articles. Fundraising operated primarily via Facebook, soliciting donations of money, food, gifts and vouchers for the families of parties convicted of terrorism offences. Bank account details were provided for monetary donations **(TFI.9)**.

Source: Australia

Indicators

TFI.9	Use of SNS to raise funds for the families of parties convicted of terrorism offences.

2.1.2 Content Hosting Services

26. Similar to SNS, cases provided as part of this report show CHS are primarily used, together with SNS, to share visual media portraying terrorist elements and promote terrorism in order to attract sympathisers and potential donors (see cases 4 and 5 below). This finding is consistent with previous research conducted by the FATF and members of the Global Network.

Case Study 4 – Abuse of CHS to solicit funds

Person A, a financial consultant, was radicalised by ISIL ideology through social media and furthered his interest in ISIL by studying Syria's geographical area, borders, social, economic, and cultural background which subsequently led to the creation of a blog 'Revolusi Islam.com' (Islam Revolution.com) and a Facebook page. Person A used the platforms to solicit funds from ISIL-sympathisers around the country for the benefit of the terrorist groups **(TFI.10)** and posted a bank account number that belonged to Person B **(TFI.11)**. Person B, who at that time was in Syria, surrendered his bank account password and ATM card to Person A through Person B's wife **(TFI.12)**. A portion of the funds collected were utilised to finance Malaysian foreign terrorist fighters' travel expenses to Syria. The remaining funds were distributed to the family members of individuals arrested for ISIL-related offence for their daily life sustenance. Person A was convicted for soliciting contributions for ISIL and subjected to imprisonment of 15 years.

Source: Malaysia

Indicators

TFI.10	Use of CHS to call for funds to support terrorist groups to support travel expenses of FTFs and family members of terrorists.
TFI.11	Post bank details (belonging to a known person in Syria) for donations on CHS and SNS to support travel expenses of FTFs and family members of terrorists.
TFI.12	Contact between content creator on CHS and SNS and family member of persons associated with terrorist groups.

Case study 5 - Use of multiple Social Media Services for raising of funds

A case was reported to police and advertised on pro-ISIL Telegram Channels in relation to charitable organisations operating through Facebook, Twitter and Instagram and private messaging groups (Telegram), to raise funds for the needy people in the Muslim community. Contributors were referred via social media to crowdfunding application youcaring.com. Medium of payment was via PayPal **(TFI.13)**. It is not known how much money has been raised by the subject in this manner. The sites purported to use the money to 'support Muslim mothers in need' and 'Muslim prisoners'. However the sites did not specify how exactly the contributions were to be spent or who the benefactors would be. There was suspicion the money might be sent offshore and used to support domestic terrorism activities.

Source: Australia

Indicators

TFI.13	Use of SNS, INS and crowd funding sites by a NPO to raise funds allegedly to support terrorist and terrorism activities.

2.1.3 Crowdfunding Services

27. A number of cases received as part of this report indicated abuse of crowdfunding services (see case 6 and 7 as examples). These services' ease-of-use and the way they are organised to facilitate crowdfunding campaigns give terrorists and terrorist organisation a valuable channel to generate funds. The individuals or groups involved sometimes took the form of NPOs or other groups of sympathisers who collect funds to support terrorist organisations and other terrorism-related activities.

28. Many of the cases involved public crowdfunding campaigns with declared purposes usually relevant to humanitarian causes (pastoral care, supporting families of convicted terrorists or 'mojahedin', school building, etc., see case 6 as an example) and sometimes a general purpose that included all sorts of support. The real purpose of funding was not known in many cases, yet a number of cases showed funding relevant to the following purposes:

- Financing foreign terrorist fighters' travel expenses to conflict zones,
- Sending the money offshore to support local terrorist activities in other jurisdiction,
- Purchase of propaganda materials (e.g. ISIL flags) and promoting terrorist' ideologies.

Case Study 6 – Abuse of crowdfunding services to raise funds to support known terrorist financier and family

This case was identified through SMRs in relation to person A, who was charged with financing terrorism in 2016. A GoFundMe crowdfunding campaign was created to raise money to support person A and his pregnant wife **(TFI.14)**. The cause's description stated "Recently a brother has become an *aseer* (prisoner) at the hands of the *tawagheet* (nonbelievers). The campaign raised $3,000 in two days.

Source: Australia

Indicators

TFI.14	Use of crowd funding websites to generate funds for terrorists and their family members.

Case Study 7 – Abuse of a crowdfunding services to raise donations

FINTRAC (FIU Canada) have seen instances where individuals under investigation for terrorism-related offences, including attempts to leave the country for terrorist purposes, have used crowdfunding websites prior to leaving and/or attempting to leave Canada **(TFI.15)**. In one example, a reporting entity received information from law enforcement that an individual had left Canada. This prompted an account review and an SMR being sent to FINTRAC. It contained details in regard to a crowdfunding website. Specifically, the reporting entity stated: "This account was used for four transactions, totalling CAD 61.56 (~USD 47.00) with a known crowdfunding website [web address provided]. This merchant is categorized by its merchant bank as "Professional Services" **(TFI.16)**. The company's website describes itself as an International Crowdfunding site, allowing people to easily set up a fundraising webpage and collect donations. Most of the donation options are related to conflict relief in Country A, Country B and Country C".

Source: case from Canada and originally included in the 2016 APG Yearly Typologies Report

Indicators

TFI.15	Use of crowd funding services which provides donation options to conflict relief in to raise funds prior for the locals to travel to conflict locations.
TFI.16	Use of crowd funding services which provides donation options to countries with conflict

2.1.4 Internet Communication Services

29. The use of ICS via browser and mobile phone platforms appeared in most cases provided as part of this report (see cases 8 -11 as examples). The perpetrators took advantage of the diversity and multiplicity of these platforms and the privacy, safety, and the confidentiality these platforms provide, as well as advanced encryption methods. Popular ICS were used to privately communicate with campaigners or terrorist groups, mainly to discuss

means of support and to exchange funding and account details (see cases 8 and 9 as examples), and in one case, ICS was highly relied upon for ISIL-linked communication and radicalisation.

Case Study 8 – Abuse of ICS to organise funds transfers

A convenience storekeeper was sentenced with imprisonment for eight years for knowingly dealing with properties belonging to a gazetted terrorist (the 'Terrorist') in Malaysia by allowing a deposit of MYR12130 (USD2874) into his bank account and withdrawal of MYR10000 (USD2380) for ISIL's benefit. The Terrorist, who was also the storekeeper's brother, gave instructions to the storekeeper through WhatsApp to enable deposits into and withdrawal from his bank account **(TFI.17)**. The storekeeper was promised by the Terrorist a commission of between MYR100 (USD23) and MYR300 (USD71) for each transaction **(TFI.18)**. He subsequently withdrew the funds and remitted the funds to several Iraqis located in an area close to ISIL's stronghold using remittance service providers **(TFI.19)**.

Source: Malaysia

Indicators

TFI.17	Use of ICS to organise deposits and withdrawals using the bank account of a terrorist's family member.
TFI.18	Use of ICS to organise bank and remittance transactions for financing an individual terrorist in exchange for a commission.
TFI.19	Use of ICS to organise remittance of funds to areas close to ISIL strongholds.

Case Study 9 – Abuse of ICS to facilitate donations via bank deposit

A technician at a metal-based factory was a member of a Telegram chat application group, known as 'Gagak Hitam' (Black Crow) which was led and administered by a gazetted terrorist (the 'Terrorist') in Malaysia, using 'Black Arrow' as his identity. 'Gagak Hitam' is an ISIL-linked cell in Malaysia. The technician was found to have sworn allegiance to the 'Gagak Hitam' group through the said Telegram chat group **(TFI.20)**. Using the 'Gagak Hitam' Telegram group, the Terrorist gave instructions to the members of the 'Gagak Hitam" group to deposit their 'infak' (donation) into the technician's bank account **(TFI.21)**. The Terrorist also separately instructed three individuals to deposit a combined total of MYR11090 (USD2,640) into the technician's bank account. He was sentenced to seven years' imprisonment for allowing money to be deposited and withdrawn from his bank account on the instruction of the Terrorist for the benefit of ISIL.

Source: Malaysia

Indicators

TFI.20	Use of ICS to swear allegiance to group led by listed terrorist.
TFI.21	Use of ICS, upon instruction of terrorist, to organise and to deposit donations into a member of the group's bank account.

Case Study 10 – Use of SNS and ICS are used for the purpose other than the real purpose it is intended for

An organized network, specialized in the collection of donations for the purpose of supporting external extremist organizations, was detected by security agencies through various means. These included undercover investigations, follow-up, periodic monitoring and surveillance of social media. Social media including Twitter, Telegram, WhatsApp and Instagram were used for a purpose other than the real purpose it is intended for, in order to promote collection of donations and to communicate with persons located in conflict zones.

Publicly, fundraising efforts claimed the funds would be used to help the needy, such as refugees in conflict zones. However, they were actually used to support the organization.

The actual logistics for moving monies was facilitated through private Twitter and Telegram accounts, or telephone calls **(TFI.22)**. Most of the funds were collected by the fundraisers directly. Some were privately transferred through financial institutions including banks, exchange firms or prepaid cards owned by members of terrorist organizations, or their affiliates in an effort to avert suspicion.

Some of the funds would actually go to charitable acts to disguise larger transactions made to extremist organizations **(TFI.23)**. The actual movement of funds was facilitated by carrying cash across borders, through alternative transfer services or exchange companies owned by nominees unknown to security agencies **(TFI.24)**. Ultimately, these funds were transferred to extremist organizations in conflict zones for the purposes of logistical support and purchase of weapons.

Source: Kuwait

Indicators

TFI.22	Use of SNS and ICS are used for the purpose other than the real purpose it is intended for, to promote operations for donations, and to communicate with persons located in conflict zones. But, there are funds would actually go to charitable acts to cover the portion of money allocated to terrorist organisations.
TFI.23	Calling of funds is made publicly but the method of collecting the funds remains discrete by accessing the private account on SNS or through telephone communication.
TFI.24	Most of the funds are collected by fund raisers, while the other part is privately transferred through banks or exchange companies or through prepaid cards "CASHU" belonging to (close or trusted) members of the terrorist organization.

Case Study 11 – Abuse of multiple platforms by organised network for collecting donations for extremist organisations

This case was detected through SMRs received by the Kuwait FIU from reporting entities. Social media services including Facebook, YouTube, Telegram, Twitter and Instagram were used. A privately-owned website, linked to a suspect, was also used. These platforms were used to campaign for donations from a significant number of followers. They advertised bank account details and phone numbers linked to persons responsible for collecting funds **(TFI.25)**.

Communication was facilitated through social media services including Twitter, Instagram, Telegram, Snapchat, Facebook and YouTube. Fundraisers' contact details including phone numbers were advertised through commercials and mobile messaging apps such as WhatsApp. **(TFI.26)**

Funds were moved through cash, ATM deposits and various internal/external transfers through banks, exchange companies, banking websites, standing orders of payment and cheques. No online payment platforms such as PayPal were used. **(TFI.27)**.

Some of the funds were used to purchase flights, or were either transferred to other countries where known terrorist organizations exist, or countries adjacent to them.

Source: Kuwait

Indicators

TFI.25	Accounts that have a large number of followers on the social media were used to raise donations, advertising bank account numbers and phone numbers of persons in charge of collecting funds.
TFI.26	Social media was used to communicate, as well as advertise fundraisers' phone numbers through commercials and mobile messaging apps such as WhatsApp.
TFI.27	Funds were moved through cash, ATM deposits and various internal/external transfers through banks, exchange companies, banking websites, standing orders of payment and cheques. They were received by persons other than those in charge of the campaign.

2.2 General Analysis and Summary

2.2.1 Detection mechanisms

30. From the provided case studies, it is clear that law enforcement and related agencies play a major role in detecting TF through abuse of social media. Monitoring and surveillance mechanisms used by these competent authorities greatly enhance the detection of social media services abuse. However, in spite of these mechanisms, monitoring and surveillance efforts are hindered by encryption implemented in some social media services, particularly in ICS. These challenges are discussed further in Part Three of this report.

31. A number of case studies highlighted the use of undercover operations to detect TF through abuse of social media. A number of cases showed TF convictions involved undercover investigations. In those cases, undercover agents benefited from the anonymity and remote communications provided in social media platforms to convince perpetrators that they were sympathizers or held ties with terrorists or terrorist organizations, which eventually led to successful convictions.

32. Additionally, cases highlighted the role of reporting entities and FIUs as one of the mechanisms to detect TF via social media abuse. In many cases, financial institutions remain a primary means for receipt and/or movement of funds for financing terrorists and terrorist groups (see below discussion of payment methods). Moreover, information sharing mechanisms between FIUs (e.g. the Egmont ESW) assisted in the detection of TF via abuse of social media, in a number of cases.

2.2.2 NPOs and social media

33. NPOs and charitable organizations appeared in several cases, including instances where images showing medical material, ambulances and food supplies being provided for humanitarian causes were published on social media services under the guise of an NPO. While it is unclear if these NPOs were part of the formal economy[18], it is apparent NPOs are used to gain credibility and legitimacy of fundraising campaigns on social media services. In addition, the linking of TF funding campaigns to humanitarian or social causes can elicit funds from unwitting donors (see below discussion on declared use of funds versus the actual use).

2.2.3 Payment methods

34. Various funding mechanisms were used to finance terrorism through abuse of social media services. Many cases revealed funds raised through social media are received and/or moved through traditional payment services such as bank accounts, which can be accessed via online banking, ATMs or payment cards. A number of cases involved conducting cash withdrawals from bank accounts and the use of hawala/cash couriers to deliver funds—in cash—into conflict zones. In addition to informal transfer schemes, structured wire transfers and checks were also used.

The use of some new payment methods (e.g. PayPal) was apparent in several cases. As mentioned earlier in this report, these payment methods may be integrated into social media services, particularly crowdfunding services. These new payment methods may increase the difficulty of detection and investigation of TF due to their vulnerabilities highlighted in Part One of this report.

2.2.4 Declared use of funds versus the actual use

35. In many cases provided as part of this report, the real use of funds was not identified. For example, humanitarian causes were commonly used as the declared use for funds, including pastoral care, schooling and medical support. This practice does not appear to hinder law enforcement actions, as many jurisdictions do not require linking TF to specific terrorist acts. In the cases where the usage of funds was identified, it was mainly linked to financing Foreign Terrorist Fighters, supporting the families of convicted terrorists or ISIL fighters, or general support for terrorists or terrorist organizations, especially in conflict zones.

[18] TI, whether they were registered and supervised by the appropriate competent authority.

Summary of Social Media and TF Indicators

Indicator		Social Media Service Used	Involved Terrorist Actor	Associated TF Components			Value of Support	
#	Description			Funds Generation (transaction method)	Method of Funds Movement	Purported use of funds (actual use of funds)	Material Support	Amount
TFI.1	Use of SNS to call for funds to support specific organisation (a school) that involves in terrorism-related extremism and radicalization movement.	SNS	unknown	Donation (unknown)	unknown	radicalization (radicalization) (Nonspecific terrorism related)	unknown	unknown
TFI.2	Use of SNS via messages and pictures to call for funds from donors to support a known terrorist front.							
TFI.3	Use of SNS to initiate contact with potential donors for donation.							
TFI.4	Use of SNS by charities to call for funds for humanitarian causes while funds were actually directed to support FTF.	SNS	FTFs	Donation (unknown)	cash	humanitarian causes (support FTFs)	unknown	€9,900
TFI.5	A terrorism-related charity uses SNS to share visual media to attest legitimacy of their activities and communicate with donors.							
TFI.6	Use of SNS by the members of the charity to portray involvement with terrorists including their weaponry training activities with terrorists.							
TFI.7	Use of SNS to raise funds under the pretext of humanitarian cause then physically moving the funds across borders via several passengers and structuring the funds below declaration threshold.							
TFI.8	Use of personal Facebook profile to declare joining a UN listed terrorist organisation and posting related daily life incidents.							
TFI.9	Use of SNS to raise funds for the families of parties convicted of terrorism offences.	SNS	unknown	Donation (unknown)	bank	Support family members of terrorists	unknown	unknown
TFI.10	Use of CHS to call for funds to support terrorist groups to support travel expenses of FTFs and family members of terrorists.	CHS/SNS	Terrorist organisation controlling territory FTFs	Donation (bank)	bank	Nonspecific terrorism related (support FTFs)	unknown	unknown
TFI.11	Post bank details (belonging to known person in Syria) for donations on CHS and SNS to support travel expenses of FTFs and family members of terrorists.							
TFI.12	Contact between content creator on CHS and SNS and family member of persons associated with terrorist groups							

TFI.13	Use of SNS, INS and crowd funding sites by a NPO to raise funds allegedly to support terrorist and terrorism activities.	SNS/INS/ Crowdfunding service	unknown	Donation (MPS)	MPS	humanitarian causes (unknown – no TF conviction)	unknown	unknown
TFI.14	Use of crowd funding websites to generate funds for terrorists and their family members.	Crowdfunding service	unknown	Donation (unknown)	unknown	Support individual terrorist and family member	unknown	AUD3,000
TFI.15	Use of crowd funding services which provides donation options to conflict relief to raise funds prior for the locals to travel to conflict locations.	Crowdfunding service	unknown	Donation (bank)	unknown	humanitarian causes (humanitarian causes)	unknown	CAD61.56
TFI.16	Use of crowd funding services which provides donation options to countries with conflict							
TFI.17	Use of ICS to organise deposits and withdrawals using the bank account of a terrorists family member	ICS	Terrorist organisation controlling territory	unknown (bank)	MVTS	Nonspecific terrorism related (Nonspecific terrorism related)	unknown	USD2,380
TFI.18	Use of ICS to organise bank and remittance transactions for financing an individual terrorist in exchange for a commission.							
TFI.19	Use of ICS to organise remittance of funds to areas close to ISIL strongholds							
TFI.20	Use of ICS to swear allegiance to group led by listed terrorist	ICS	Lone Actors/small cells	Donation (bank)	unknown	unknown (unknown)	unknown	USD2,640
TFI.21	Use of ICS upon instruction of terrorist, to organise and to deposit donations into a member of the group's bank account							
TFI.22	Use of SNS and ICS are used for the purpose other than the real purpose it is intended for, to promote operations for donations, and to communicate with persons located in conflict zones. But, there are funds would actually go to charitable acts to cover the portion of money allocated to terrorist organisations.	SNS/ICS	unknown	Donation (bank)	Cash/MVTS/prepaid cards	Humanitarian causes (Nonspecific terrorism related)	unknown	unknown
TFI.23	Calling of funds is made publicly but the method of collecting the funds remains discrete by accessing the private account on SNS or through telephone communication.							
TFI.24	Most of the funds are collected by fund raisers, while the other part is privately transferred through banks or exchange companies or through prepaid cards "CASHU" belonging to (close or trusted) members of the terrorist organization.							
TFI.25	Accounts that have a large number of followers on the social media were used to raise donations, advertising bank account numbers and phone numbers of persons in							

	charge of collecting funds	SNS/ICS/CHS	unknown	Donation (bank)	Cash/bank/ MVTS/ cheques	unknown (unknown)	unknown	unknown
TFI.26	Social media was used to communicate, as well as advertise fundraisers' phone numbers through commercials and mobile messaging apps such as WhatsApp							
TFI.27	Funds were moved through cash, ATM deposits and various internal/external transfers through banks, exchange companies, banking websites, standing orders of payment and cheques. They were received by persons other than those in charge of the campaign.							

Part Three: Challenges and Measures in Combating TF via Abuse of Social Media

36. Only a limited number of APG and MENAFATF members have experience in investigating and prosecuting terrorism and TF cases involving social media. Therefore, to support APG and MENAFATF members and the Global Network to combat TF, this section examines some key challenges in the detection, investigation and prosecution of TF via the abuse of social media services. It also identifies some key measures to assist competent authorities overcome these challenges.

3.1 Challenges and measures for detection of TF

37. Jurisdictions face challenges with identifying and assessing TF risks associated with social media in order to prioritise and target financial intelligence and investigation activities that address the specific threats faced. Few APG or MENAFATF members reported detailed assessments of TF risks associated with social media or in the jurisdictions' risk assessment, including identification of context and geographical factors that may impact social media TF vulnerabilities and consequences; social media services typologies and red flags; and social media services features and integration with payment services.

38. The primary challenge in the detection of TF through abuse of social media services is the significant number of social media services, user accounts and amount of social media usage. For example, in an "internet minute" in 2017 ~4.1 million videos were watched on YouTube; ~500 thousand photos were shared on Snapchat; ~450 thousand tweets were sent on Twitter; and ~48 thousand posts were made on Instagram[19].

39. To support the detection of TF, some APG and/or MENAFATF members have implemented the following mechanisms or a combination of the following mechanisms:

- Designated teams to monitor and conduct surveillance on social media services, on a 24-hour basis, which may involve mechanisms such as keyword searches, review of general trending topics and virtual undercover operations. These 24-hour "cyber patrols" aim to detect different kinds of crimes on the internet, with emphasis on activities related to terrorism. They may focus on public forums, public websites and other identified public information sources. (See case study 12).
- Implementation of legislation requiring internet service providers and internet content providers to be responsible for conducting their own surveillance and monitoring on social media to ensure that their services do not contain terrorism-related content.
- Multi-agency coordination mechanisms that involve national security authorities, FIUs and LEAs to exchange intelligence including on TF and social media-related issues (often meeting as frequently as on a monthly basis).

40. Many jurisdictions lack national and agency-level policies and procedures to combat TF and abuse of social media services for TF, particularly those based on comprehensive risk assessments. Policies and procedures should include, for example, identification and actions to rectify gaps in legal frameworks, and policies and procedures for LEAs and other competent authorities to investigate TF via abuse of social media and to reach out to the private sector on risk mitigation.

[19] https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/

Case 12 - Designated Monitoring and Surveillance

During the course of regular social media monitoring, the Social Media Monitoring and Surveillance Team (SMMST) identified an account in the name of person A. The account was being used to propagate radical ideologies and to incite social media users' participation in ongoing jihad. The account was also used to publicly call for donations towards the destruction of secular Bangladesh and the establishment of Khilafah **(TFI.28)**.

The account recently published the arrival of a terrorist who was on the verge of conducting an attack. The SMMST sought help from the relevant social media firm to identify the account's owner, and an arrest was affected through their provided information as well as mobile phone tracking.

During the investigation, the SMMST learned person A was a fictitious name and the actual individual is an active member of a Bangladesh Government-designated entity Ansar Al Islam Bangla Team (ABT). A case has been filed against the person under the Anti-Terrorism Act, 2009 and Information Technology and Communication Act, 2006. SMMST are conducting ongoing investigations to identify any associates.

Source: Bangladesh

Indicators

TFI.28	Use of social media services by a member of domestic-designated entity to disseminate terrorist propaganda and donations for the establishment of Khilafah using a fictitious name.

3.2 Challenges and measures in investigation and prosecution of TF

41. In addition to challenges in the detection of TF through abuse of social media services, competent authorities face significant challenges in investigation and prosecution. Some high-level challenges and associated measures to overcome challenges identified from responses to the project questionnaire include:

42. *Tracing and Identifying Persons:* Social media account owners may use various methods to conceal their real identities in order to avoid detection. For example, the owner and user of the social media account may be different, which makes it challenging for investigators to identify who is actually posting content. Furthermore, social media content changes frequently as users can add and delete content quickly. This poses challenges to investigators in identifying the perpetrator of the message or supposed purpose of the fundraising exercise.

43. The identification of the persons involved in TF through abuse of social media often relies upon the information maintained and provided to competent authorities by social media companies and/or internet service providers (ISPs) and telecommunication providers. The provision of traffic data, content data and subscriber information may be complicated when these companies are based in foreign jurisdictions, subject to foreign (and sometimes stricter) data protection laws and/or different record-keeping requirements. To overcome these challenges, competent authorities should establish and maintain relationships, including formal agreements with points of contact and regular meetings with social media companies, ISPs and telecommunication companies for the provision of user information. To support global counterterrorism efforts and other law enforcement activities, some social media companies, for example Facebook, have developed mechanisms and guidelines to facilitate requests for data.

44. In addition to these efforts, as many of the case studies provided as part of this report show banks and MVTS are involved in the receipt and movement of funds, competent authorities—in coordination with FIUs—should use 'follow the money' techniques to trace and identify persons.

45. *Analysis of Digital Forensic Evidence:* Capability and capacity for analysis of complex and rapid digital forensic evidence poses a significant challenge in the investigation and prosecution of TF cases. To overcome these challenges, some competent authorities have implemented specialized units to provide assistance or technical advice and awareness-raising to LEAs. In addition, competent authorities need to develop various investigative tools such as forensics analysis techniques, data mining techniques, social network analysis; and implement software for scanning websites and social media content.

46. *Transnational Nature and Obtaining Evidence:* The transnational nature of TF via abuse of social media creates challenges in the investigation and prosecution of cases, including search and seizure of computers and other electronic devices/evidence in another jurisdiction, and the preservation of evidence. Identifying a suitable means of communication with social media companies and the time usually taken to reply to LEAs and prosecution requests can easily constitute a challenge, especially when there are no legal obligations binding these social media companies to reply to requests originating from foreign jurisdictions.

47. While jurisdictions that responded to the questionnaire did not always have mechanisms in place for gathering or exchanging financial intelligence specifically on the topic of abuse of social media for terrorism and TF issues, they use existing mechanisms and cooperation platforms to exchange intelligence on TF and social media-related issues including:

- Liaison Officer networks – jurisdiction uses their Liaison Officer network in foreign jurisdictions to ensure effective exchange of information or to obtain information;
- Egmont Group – for FIU-to-FIU exchange of information;
- Police-to-police cooperation – for instance, Interpol, ASEANAPOL, Europol; and
- Signing MoUs with foreign jurisdictions.

Part Three: Collaborative Approaches to Preventing the Abuse of Social Media for TF

48. In acknowledgment of the prominent role of social media services in daily life, this section provides a number of avenues for APG and MENAFATF members/observers to work collaboratively with social media companies and other relevant private and public sector entities to prevent TF and the abuse of social media for TF.

3.3 Increasing public awareness of abuse of social media for TF

49. Issuing guidance on crowdfunding to the public and NPOs to prevent these charitable organisations from misuse for other purposes, such as TF.

3.4 Supporting the removal of Terrorism and TF related content

50. Some APG/MENAFATF members highlighted the need to establish and maintain effective communication channels with social media companies, in order to support the removal or restriction of identified social media accounts, profiles, pages, groups, and content used for terrorism/TF. This is particularly important in reference to persons associated with UN designated individuals and entities because competent authorities often have information on related parties and associates, which are not included in relevant designation listings.

3.5 Counter-Messaging

51. To address the spread of terrorism-related ideologies and propaganda on social media services, a number of APG and MENAFATF members have implemented a preventive strategy aimed at countering falsely disseminated information and simultaneously educate and raise community awareness, as follows:

- Awareness-raising campaigns, conducted through television and social media accounts to educate the public to increase vigilance, and awareness on terrorism and TF issues including abuse of social media.

- Specific and significant funding to limit the impact of violent extremist narratives on domestic audiences, by working with civil society, industry and other sectors to build greater understanding of terrorist propaganda and an evidence base on how to counter its extremist ideologies; limit access to propaganda online; and to undermine the appeal of extremist messages through leadership messaging and community led counter-narrative activity.

- The creation of a Centre against Terrorism and Hybrid Threats (CTHT). The CTHT is essentially a specialised analytical and communications unit which monitors threats directly related to internal security including terrorism and extremism. Based on its monitoring work, CTHT evaluates detected challenges and proposes appropriate responses. It also disseminates information and spreads awareness among the general public including by working openly with civil society, the media, etc.

- Establishment of a counter-messaging centre which strives to suppress the dissemination of terrorism ideology across society particularly to the youth, specifically in relation to ISIL, by countering the erroneous propaganda and ideology circulated through social media platforms.

- A group of volunteer religious teachers called the Religious Rehabilitation Group has established an online presence to counter radical narratives and easy access for individuals seeking clarification on ideological concepts purveyed by terrorist groups. The group also uses a parallel mobile phone application.

Conclusion and Recommendations

52. The cases provided as part of this report and previous publications by the Global Network show social media services are being abused in a variety of ways for TF, and that collaborative effort across both public and private sectors at both the domestic and international level is required to combat this abuse and related TF. In accordance with the information provided as part of this report and the FATF standards, all APG and MENAFATF members are encouraged to undertake steps to combat TF through social media:

- *Identify, assess and understand TF risks including those associated with social media*: The risks posed by abuse of social media services for TF should be specifically addressed in the jurisdictions' risk assessment, including identification of context and geographical factors that may impact social media TF vulnerabilities and consequences; social media services typologies and red flags; and social media services features and integration with payment services.
- *Policies/procedures and domestic legal frameworks:* Based on an effective understanding of TF risks including those associated with social media, jurisdictions should implement national and agency-level policies and procedures to combat TF and abuse of social media services for TF. Policies and procedures should include, for example, identification and actions to rectify gaps in legal frameworks, and policies and procedures for LEAs and other competent authorities to investigate TF via abuse of social media. This work necessitates involvement by both the public and private sectors.
- *International engagement:* A key TF-related social media vulnerability is the cross-jurisdictional nature of the social media services. To overcome this challenge, competent authorities should strengthen both formal and informal international cooperation.
- *Capacity building and engagement with social media companies:* In general terms information provided as part of this report highlight competent authorities (including analysts and investigators, prosecutors and judges), technical understanding of social media services, associated payment technologies and monitoring tools present a challenge. Therefore, emphasis should be placed on the strategic collaboration between public and private industry for the following purposes:
  i. Closing the technical knowledge gap on social media services, payment methods and related technology;
  ii. Establishment of policies and common understanding on the operational challenges in monitoring, prosecuting and investigating TF activities where social media services are abused, including developing effective measures to prevent abuse of social media services for TF;
  iii. Periodic sharing of emerging risks, typologies and red flags including new platforms' features; and
  iv. Collaboration in new areas of research and studies on the detection, prevention and combat misuse of social media for T/TF.

- As evident in the case studies, jurisdictions may consider establishing specific task forces or committees comprising of the FIU and relevant national security agencies specialised in gathering intelligence, monitoring, and possible investigations as well as prosecution of social media-related T/TF offences.

APPENDIX A – Social Media and Terrorism Cases

53. The cases included in this annex were provided as part of this report, but mainly relate to abuse of social media for terrorism, and therefore are not included in the main body of this report. While a detailed analysis of all cases is outside the scope of this report, indicators have been identified for each case and in general terms, these cases primarily relate to abuse of social media services to:

- *Publicly pledging allegiance to terrorist organisations:* A number of ISIL supporters or aspiring FTF have openly expressed support for ISIS and its violent terrorist activities or posting pledge of allegiance to ISIL leader al-Baghdadi on the social media page;
- *As a primary platform for aspiring FTF to reach out and make contacts with terrorists for either travelling arrangement to waging jihad in conflict areas or plan terrorist attacks domestically:* There are a few cases which involved persons who are ISIS-supporters and established contact with terrorists online for the purpose of getting married and providing medical assistance and training to jihadi fighters in Syria. Additionally, social media services were also abused by suspicious individuals or foreign nationals to use religion as pretext to influence or recruit locals into marriage based on the doctrine of jihad, or plan to use a jurisdiction as a transit point or alternative route to travel to a known conflict area; and/or
- *Abuse of social media features to promote ISIL call for violence, voice support for ISIS operations and attack, and to distribute ISIS propaganda and communications:* In one case, a platform for ISIL supporters has been relocated to three different locations within the application with each move creating a distinct channel with a distinct URL since its initiation. This reflects another ISIS strategy to self-preserve their existence in the social media sphere. Terrorists also used multiple social media platforms simultaneously to maximise publicity and popularity of ISIS as well funds collected from sympathisers worldwide.

CASE STUDIES OF ABUSE OF SOCIAL MEDIA SERVICES FOR TERRORISM

Case 1

Donald Ray Morgan sentenced on May 13, 2015 to 243 months' imprisonment, to be followed by a term of supervised release. Morgan pleaded guilty to attempting to provide material support to a designated foreign terrorist organization and to possession of a firearm by a felon. Specifically, Morgan waived indictment and pleaded guilty to one count of attempting to provide material support to a designated foreign terrorist organization, the Islamic State of Iraq and al-Sham ("ISIS"), in violation of 18 U.S.C. § 2339B. According to court documents, Morgan admitted to knowingly attempting to provide support and resources beginning in January 2014 until on or about August 2, 2014, including his own services, to al-Qa'ida in Iraq and the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization. On at least one occasion, Morgan unsuccessfully attempted to travel to Syria to join ISIL/ISIS. Morgan also frequently used social media and an interview with an American journalist to express his support for ISIL/ISIS and violent terrorist activities **(TI.1).**

Source: United States of America

Indicators

TI.1	Use of SNS to express support for ISIS and violent terrorist activities.

Case 2

Heather Elizabeth Coffman in 2015 pleaded guilty to one count of wilfully and knowingly making a false statement involving international terrorism, in violation of 18 U.S.C. § 1001. The Information resulted from an FBI investigation of several U.S. based individuals who were allegedly conspiring or attempting to provide material support to the Islamic State of Iraq and Syria (ISIS). Coffman's sentencing is set for May 11, 2015. Coffman was initially arrested on November 14, 2014, pursuant to a criminal complaint alleging that Coffman made a false statement involving or promoting international or domestic terrorism, in violation of 18 U.S.C. § 1001(a). As part of the investigation, an FBI undercover employee (UCE) met with Coffman multiple times in Richmond. During these meetings, Coffman discussed her support of ISIS and her attempts to facilitate the UCE's and another individual's travel to Syria with the intent of joining ISIS. After her arrest, the parties agreed to extend indictment for a period of time for plea negotiations. Consistent with the Plea Agreement and Statement of Facts, Coffman pleaded guilty by Information to wilfully and knowingly making a materially false, fictitious, and fraudulent statement involving international terrorism during a November 13, 2014, interview by FBI Special Agents. That false statement revolves around when she was asked by the FBI agents whether she knew if an individual (her then on-line boyfriend or husband who resided outside the U.S.) had talked to anybody else or other people about ISIS and she responded that she did not know anybody he talked to, in violation of 18 U.S.C. § 1001(a). The statement was false because, as Coffman well knew, she previously had put her then on-line boyfriend in contact with a foreign national living outside the United States, whom she believed was an ISIS fighter is Syria, and that person had, in turn, communicated with her on-line boyfriend to facilitate his travel to Turkey to join ISIS **(TI.2).** The Statement of Facts ("SOF") also details additional activities of Coffman, including the fact that from June 2014 through November 2014, Coffman used multiple Facebook accounts to publicly support ISIS and jihadist fighters. The SOF further delineates multiple steps that Coffman took to facilitate her then on-line boyfriend's travel to Syria to join ISIS, explaining that Coffman explored options with him to travel to Syria in order to fight for ISIS and die a "Shaheed," including contacting a foreign national who represented himself as an ISIS fighter in Syria and connecting the two so that his travel to Syria could be facilitated. The SOF also delineates Coffman's interactions with an FBI UCE, including discussions that she had with the UCE which outlined her attempts to facilitate both the individual's, and the UCE's travel to Syria to join ISIS.

Source: United States of America

Indicators

TI.2	Use of multiple SNS accounts to publicly support ISIS and jihadist fighters and to assist a friend to be in contact with an ISIS fighter in Syria.

Case 3

Zakaryia A. Abdin, an 18 year old United States citizen residing in Charleston, was charged by criminal complaint with attempting to provide material support to the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B. Abdin was arrested by the FBI after travelling to the Charleston airport, and once in the airport, taking substantial steps towards travelling overseas. Abdin had purchased a ticket to Jordan, and upon arrival, his intention was to travel to Egypt to join ISIS. The investigation has revealed that Abdin has been involved in extensive online communications with an individual whom he believed to be a member of ISIS, but who was actually an FBI undercover employee. During these communications, Abdin pledged his allegiance to ISIS, and expressed his desire to travel overseas to fight on their behalf **(TI.3)**. If he was unsuccessful in travelling overseas, his plan was to engage in an attack domestically.

Source: United States of America

Indicators

TI.3	Use of online communications with an individual whom he believed to be a member of ISIS and pledging allegiance to ISIS, becoming FTF and domestic attack.

Case 4

On January 16, 2017, the FBI arrested Noor Salman who was residing with family in the San Francisco area. On January 12, 2017, in the Middle District of Florida, a grand jury returned an indictment, that was later unsealed, which charges Salman with one count of aiding and abetting Omar Mateen by providing and attempting to provide material support or resources to the Islamic State of Iraq and Syria (ISIS), that resulted in death, in violation of 18 U.S.C. § 2339B, and with one count of obstruction of justice, in violation of 18 U.S.C. § 1512. Salman is the wife of Mateen, the now-deceased terrorist who killed 49 people at the Pulse nightclub in Orlando, Florida in the early morning hours of June 12, 2016. Just before entering the club, Mateen posted his pledge of allegiance to ISIS leader al-Baghdadi on his Facebook page **(TI.4).** Investigators discovered that in the weeks prior to Mateen's deadly attack, Salman provided support and assistance to Mateen as he prepared to conduct a terrorist attack in the United States on behalf of ISIS. Salman's support and assistance included scouting possible attack locations with Mateen, ensuring that Salman had access to Mateen's bank accounts once Mateen had martyred himself, and engaging in a spending spree with Mateen designed to provide Salman with jewellery and other valuable items that she could sell after Mateen was dead. Forensic computer and cell phone evidence, coupled with Salman's statements to the FBI, show that Salman was aware of Mateen's radicalization and interest in ISIS videos and other violent jihadist material. Through text messages recovered from Mateen's phone—but deleted from Salman's cell phone—the FBI learned that Salman invented a cover story that they used to hide Mateen's whereabouts from his family the night he prepared to conduct the attack. Salman also deleted various text messages she had exchanged with Mateen that night and attempted to cover up her role in the attack by sending him text messages that would suggest she did not know he was going to conduct an attack. Only these self-serving text messages were not deleted from her phone. In the hours following the attack, Salman provided law enforcement with several voluntary statements. Salman's statements initially concealed her knowledge of, and involvement in, the attack, but eventually Salman admitted she had lied to law enforcement about her prior knowledge of the attack.

Source: United States of America

Indicators

TI.4	Use of SNS to pledge of allegiance to ISIS leader al-Baghdadi.

Case 5

Mohamed Ibn Albaraa (a/k/a Mohamed Zuhbi), ("Albaraa"), a 24 year-old Australian citizen, and Asher Abid Khan ("Khan"), a 21 year-old United States citizen, charged with material support-related offenses. Specifically, Khan is charged with three counts of 18 U.S.C. § 2339B, conspiring to provide, attempting to provide and providing material support to the Islamic State in Iraq and the Levant ("ISIL"); two counts of 18 U.S.C. § 2339A, conspiring and attempting to provide material support to terrorists; and one count of 18 U.S.C. § 956(a), conspiring to commit murder, kidnapping, or maiming overseas. Albaraa, is charged with two counts of 18 U.S.C. § 2339B, conspiring to provide and providing material support to ISIL; one count of 18 U.S.C. § 2339A, conspiring to provide material support to terrorist; and one count of 18 U.S.C. § 956(a), conspiring to commit murder, kidnapping or maiming overseas. Khan is currently residing with his family in Spring, Texas, on supervised release, pending trial. Albaraa is a fugitive residing overseas. If convicted, both Khan and Albaraa would face a sentence of up to life imprisonment. Beginning in early 2014, Khan and, a friend, "S.R.G.", devised a plan to travel to Turkey and on to Syria for the purpose of joining and waging jihad on behalf of ISIL. In furtherance of their plans, Khan located a Turkish-based foreign terrorist fighter facilitator, Albaraa, using the Internet, and later asked Albaraa: "I wana join ISIS can you help?" Then, during online communications with another individual, Khan explained: "I wanna die as a Shaheed [martyr]." **(TI.5)** Ultimately, "S.R.G." made it to Syria and joined ISIL with the assistance of Khan and Albaraa. Khan had been temporarily living in Australia with a relative and made it to Istanbul, Turkey, where he was to meet S.R.G. in their shared goal to join ISIL. However, Khan's family sent him false information regarding his mother's health and he returned home.

Source: United States of America

Indicators

TI.5	Use of SNS to establish contact with FTF facilitator for the purpose of travelling to Turkey and on to Syria in order to join and wage jihad on behalf of ISIL.

Case 6

A 18 year old Shannon Maureen Conley pled guilty to conspiracy to provide material support to ISIS as an Al Qaeda affiliated terrorist organization, in violation of 18 U.S.C. 371. The judge accepted the plea, ordered a full presentence report to be prepared, and ordered that the defendant undergo a psychiatric evaluation before sentencing would be imposed. Sentencing is scheduled for January 23, 2015. The charge to which Conley pled guilty relates to her attempts to support ISIS. Conley was arrested, based on probable cause, on April 8, 2014, at Denver International Airport as she was about to board a flight to Germany en route to Turkey. She was initially charged on April 9, 2014, and has remained detained since her arrest. Conley initially came to the attention of law enforcement for suspicious activity at the campus of a small religious institution in Colorado. In numerous interviews with law enforcement over the past several months, Conley stated that she was interested in traveling overseas to commit jihad, had researched Islam, had joined a group called US Army Explorers and had trained with the group, and showed law enforcement agents an annotated book about Al Qaeda tactics for carrying out guerrilla warfare. She is a convert to Islam. She met a man online who identified himself as a soldier for the Islamic State of Iraq and Syria fighting in Syria, and made plans with him to travel to marry him in Turkey, live with him and provide medical assistance and training to jihadi fighters in Syria **(TI.6).** When she was arrested, she was about to board a flight to Germany that was scheduled to connect to a flight bound for Istanbul, and thereafter, onto Adana, Turkey, where she was to meet people associated with the ISIS soldier who were to escort her to Syria.

Source: United States of America

Indicators

TI.6	Use of SNS for an aspiring FTF to find contact with ISIS fighters in Syria to realise her mission and plan to marry him and train to be jihadi fighter there.

Case 7

In February 2015, the Internal Security Department thwarted an attempt by a local woman to help a foreign man who had intended to join the activities of a terrorist organisation. Investigations revealed that she had been in contact with the foreign national since August 2014 via social network and continued to do so despite knowing his intention to join ISIL **(TI.7)**. The local woman, who is now being held under a Restriction Order, facilitated the man's entry into the country, sought employment for him and planned to marry him in Brunei, which would have enabled him to prolong his stay in the country before pursuing with his plan to join the terrorist group. The ISD warned that Brunei Darussalam is vulnerable to being used as a transit point for individuals intending to travel to conflict zones in order to avoid detection by authorities. This case demonstrates the potential use of social media as a way of suspicious individuals or foreign nationals to use religion as a pretext to influence or recruit locals into marriage based on the doctrine of 'jihad', or plan to use Brunei as a transit point or an alternative route to travel to a known conflict area.

Source: Brunei Darussalam

Indicators

TI.7	Use of SNS to make contract with foreign national who intended to join terrorism organisation and subsequently provide safe harbour/transit (employment) in the country prior to joining the terrorist group.

Case 8

Robert Lorenzo Hester, Jr. was charged in a criminal complaint with attempting to provide material support to the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B. Hester was arrested by the FBI while meeting with an individual whom he believed to be a member of ISIS, but who was actually an FBI undercover employee. Hester had met with this individual six times since November 8, 2016, to plan a violent attack in the United States on behalf of ISIS. Hester initially engaged with online confidential sources and an online FBI undercover employee since at least August 2016, in discussions about a global jihad and the need to attack the United States government **(TI.8)**. Hester identified categories of potential targets for attack, including "oil production" facilities, "military bases," "federal places," "government officials" and "Wall Street." After meeting the undercover employee in November, he purchased a number of items that the undercover employee said would be used to construct bombs. He also provided information on storage units that could be used to hold weapons to be used for the attack, and agreed to obtain additional supplies for the operation. He repeatedly expressed to the undercover employee a willingness to assist in what he believed would be a murderous terrorist bombing and gunfire attack.

Source: United States of America

Indicators

TI.8	Use of internet to plan global jihad and violent attack domestically.

Case 9

Said Azzam Mohamad Rahim was charged with six counts of false statements involving international terrorism, in violation of 18 U.S.C.§ 1001. These counts relate to alleged false statements that Rahim made to law enforcement officers on March 5, 2017, during a voluntary interview. In approximately April 2016, the FBI became aware of a mobile phone application used by ISIS supporters and opened an investigation into several individuals who use that application to support ISIS. The FBI's investigation has centred on individuals using a radiostyle, audio, push-to-talk, direct messaging, mobile application that allows users to communicate either one-on-one with other individuals or over a group channel that can support up to two thousand five hundred (2,500) users simultaneously. The investigation determined that one channel was created on June 30, 2014, and that its primary purpose was to function as a platform for ISIS supporters to discuss ISIS leaders, promote ISIS calls for violence, voice support for ISIS operations and attacks, and to distribute ISIS propaganda and communications **(TI.9)**. Further, the investigation has shown that Rahim was active on this channel. Since its initiation, that channel has been relocated to three different locations within the application, with each move creating a distinct channel with a distinct URL **(TI.10)**. Rahim was active on all four channels. A review of airline records revealed that on February 11, 2017, Rahim purchased an airline ticket for Lufthansa flight 439 departing Dallas-Fort Worth International Airport (DFW) on March 5, 2017, at 4:10pm for Amman, Jordan (via Frankfurt, Germany), and Lufthansa flight 693 returning from Amman, Jordan on May 9, 2017. On March 5, 2017, Rahim arrived at DFW airport and after passing security agreed to a voluntary interview by FBI agents. In that interview, Rahim made multiple false statements, including the ones for which he was charged in a criminal complaint. The FBI made a probable cause arrest at DFW immediately following his interview. On March 6, 2017, in the Northern District of Texas, Said Azzam Mohamad Rahim made his initial appearance pursuant to a complaint issued March 6, 2017, charging him with knowingly and wilfully making material false statements and representations involving international or domestic terrorism to the FBTI. On March 15, 2017, Rahim had an initial appearance and detention hearing on those charges.

Source: United States of America

Indicators

TI.9	Use of internet channel (unknown) for supporters to discuss ISIS leaders, promote ISIS calls for violence, voice support for ISIS operations and attacks, and to distribute ISIS propaganda and communications.
TI.10	Since its initiation, that channel has been relocated to three different locations within the application, with each move creating a distinct channel with a distinct URL.

Case 10

Saifullah Ozaki Sajid Chandra Debnath Abu Musa (Ozaki) is a converted Muslim (possibly in 2000) from Hindu. He lived in the South Eastern area of Bangladesh and studied in a renowned Bangladeshi college. In 2002, he received a scholarship and moved to 'country-6' to continue his studies. Later, Ozaki started working as an Associate Professor of a university in the same country. He converted a local woman and married her in 2007 and has three sons and one daughter. He obtained citizenship of country-6 in 2012. Ozaki collected funds in the name of charity from different persons in Bangladesh as well as from other countries, for the purposes of sending funds to a Conflict Zone through 'country-1'. He received some funds when his associates visited him, or by hundi. He travelled to country-1 thrice to donate funds to an ISIL facilitator named 'CC', who is a citizen of 'country-7' (a conflict zone) and staying at 'country-1'. More so, he sent invitation letters from country-6 to radicalised Bangladeshi persons who were trying to travel to conflict zones. Ozaki travelled to many countries to attend seminars/conferences. But, under the cover of such conference, he collected funds and met with IS facilitators.

Ozaki communicated with 'B-2' and other persons interested in becoming foreign fighters for ISIL. He used secret means of communication like Wickr, WhatsApp, Telegram, Threema, Surespot, Chat Secure, Skype, Facebook, Protected text, Pidgin, Viber etc., for the purposes of Dawah, communication, and collection of funds for charity from different persons. He used a FB group named “Islamic Learning Forum” to recruit and share information/Dawah by uploading/posting Jihadi audios/ videos. He also used “At Tamkin” for Dawah by uploading/publishing Jihadi audios/ videos and “DABIQ” magazine **(TI.11)**. In 2015, Ozaki left country-6 for the conflict zone with family members.

Ozaki and his associates transferred funds to different countries using different social media applications. They shared information relating to money transfers, amounts, locations and PIN codes through various applications. Funds were collected in the name of charity from Bangladesh, country-6, country-2 and Middle Eastern countries. Funds were also couriered by people to conflict zones. Mr. A-2 sent total 70 lacs taka to Ozaki at different times. Moreover, credit cards were used to draw money at the closest destination to the conflict zones. The case was first detected by proactive social media monitoring and surveillance. Actual amounts of funds gathered are not known.

Source: Bangladesh

Indicators

TI.11	Use of multiple social media platform to communicate with ISIL supporters, disseminating terrorism-related materials and to raise funds.

Case 11

Relevant authorities in Brunei Darussalam have identified a number of foreign nationals working in the country who are suspected to have links to militant groups in the immediate neighbouring countries. These individuals are active on social media platforms such as Facebook. Their Facebook pages show that they are actively sharing visual media portraying terrorist elements **(TI.12)**. These individuals are being monitored by the authorities as there is a potential for them to raise funds for terrorism-related purposes through the medium of self-funding using funds obtained legitimately **(TI.13)**.

The Internal Security Department in cooperation with other intelligence and enforcement agencies detained and deported four foreign nationals for their involvement in extremism and terrorism-linked activities. The individuals were in possession of propaganda materials related to ISIL and had admitted to downloading as well as sharing IS online videos and other materials available on the Internet. At the same time, they were also believed to be communicating with suspected IS members based overseas via a social media platform **(TI.14)**.

Source: Brunei Darussalam

Indicators

TI.12	Use of SNS to actively share visual media portraying terrorist elements.
TI.13	Use of SNS to raise funds for terrorism-related purposes through self-funding using funds obtained legitimately.
TI.14	Use of SNS for communication with suspected terrorist group members based overseas.

Case 12

The case involves a charity set up in 2010 to support humanitarian projects in Africa and the Middle-East. Its Chairman was a webmaster for another humanitarian association who specialized in e-marketing. The website displayed numerous pictures of projects, and the page offered several options to make donations via credit card, PayPal, cash transfers, or cheques **(TI.15)**. The Facebook page displayed two links: one to make a donation and one to share the call for donations **(TI.16 and TI.17)**. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below €500 – almost €2 million was received in total **(TI.18)**. A quarter of those funds were collected in personal PayPal accounts, and then withdrawn by cash, or wire transferred to accounts of other charities **(TI.19)**. In this case, the authorities could not prove elements of TF.

Source: France (originally included in the 2016 APG Yearly Typologies Report)

Indicators

TI.15	Embedded donation link using IPS and TPS.
TI.16	Use of CHS and SNS to call for donations for humanitarian causes.
TI.17	Use of CHS and SNS to promote sharing calls for donations.
TI.18	Number small donations received by cheque and wire transfer.
TI.19	Collection of donated funds in IPS account and withdrawn in cash or wire transferred to other accounts.

Summary of Social Media and Terrorism Indicators

Indicator		Social Media Service Used	Involved Terrorist Actor
#	Description		
TI.1	Use of SNS to express support for ISIL and violent terrorist activities.	SNS	Terrorist organisation controlling territory
TI.2	Use of multiple SNS accounts to publicly support ISIL and jihadist fighters and to assist a friend to be in contact with an ISIS fighter in Syria.	SNS	Terrorist organisation controlling territory FTFs
TI.3	Use of online communications with an individual whom he believed to be a member of ISIS and pledging allegiance to ISIL, becoming FTF and domestic attack.	unknown	Terrorist organisation controlling territory FTF / Lone actor
TI.4	Use of SNS to pledge of allegiance to ISIL leader al-Baghdadi.	SNS	Terrorist organisation controlling territory
TI.5	Use of SNS to establish contact with FTF facilitator for the purpose of travelling to Turkey and on to Syria in order to join and wage jihad on behalf of ISIL.	unknown	Terrorist organisation controlling territory FTFs
TI.6	Use of SNS for an aspiring FTF to find contact with ISIL fighters in Syria to realise her mission and plan to marry him and train to be jihadi fighter there.	SNS	Terrorist organisation controlling territory FTFs
TI.7	Use of SNS to make contract with foreign national who intended to join terrorism organisation and subsequently provide safe harbour/transit (employment) in the country prior to joining the terrorist group.	unknown	Terrorist organisation controlling territory
TI.8	Use of internet to plan global jihad and violent attack domestically.	unknown	Terrorist organisation controlling territory / Lone actor
TI.9	Use of internet channel (unknown) for supporters to discuss ISIL leaders, promote ISIL calls for violence, voice support for ISIS operations and attacks, and to distribute ISIL propaganda and communications.	unknown	Terrorist organisation controlling territory
TI.10	Since its initiation, that channel has been relocated to three different locations within the application, with each move creating a distinct channel with a distinct URL.		
TI.11	Use of multiple social media platform to communicate with ISIL supporters, disseminating terrorism-related materials and to raise funds.	CHS/SNS	Terrorist organisation controlling territory
TI.12	Use of SNS to actively share visual media portraying terrorist elements.	SNS	Terrorist organisation controlling territory
TI.13	Use of SNS to raise funds for terrorism-related purposes through self-funding using funds obtained legitimately.		
TI.14	Use of SNS for communication with suspected terrorist group members based overseas.		

TI.15	Embedded donation link using IPS and TPS	CHS/SNS	
TI.16	Use of CHS and SNS to call for donations for humanitarian causes		
TI.17	Use of CHS and SNS to promote sharing calls for donations		
TI.18	Number small donations received by cheque and wire transfer		
TI.19	Collection of donated funds in IPS account and withdrawn in cash or wire transferred to other accounts		

APPENDIX B – Project Questionnaire

TERRORISM FINANCING AND SOCIAL MEDIA PROJECT

Social media provides new opportunities for terrorist organisations and individuals to promote their cause, recruit followers and raise funds for their activities. Social media allows users to create and share their own content through websites and mobile applications with varying degrees of anonymity and encryption. While there an increasing variety of social media platforms, key platforms include Facebook, Twitter, YouTube, Instagram, WhatsApp and Snapchat.

A number of reports have identified the use of social media for terrorist propaganda, radicalisation to causes and organisation of terror activities, especially in relation to Islamic State of Iraq and the Levant (ISIL). However, questions remain on how social media are being, or might be, abused for terrorism financing (TF).

The Middle East and North Africa Financial Action Task Force (MENAFATF) and the Asia Pacific Group on Money Laundering (APG) have initiated a project on TF and social media that aims to identify techniques and trends associated with the abuse of social media for financing acts of terrorism, individual terrorists or terrorist organisations.

To assist in developing a holistic view of what is being undertaken to counter the abuse of social media for TF, we appreciate your assistance in completing the following questionnaire. The questionnaire has two parts:

- Case studies and typologies on abuse of social media for TF
- Questionnaire on measures to counter the abuse of social media for TF

We encourage you to seek input from all areas of government including financial intelligence units, counter terrorism units, law enforcement agencies, prosecutorial agencies and other agencies that have a role in this area.

In finalising the report, we may also seek the views of the private sector.

We recognise that some information may be sensitive. Please let us know if you do not want your jurisdiction or organisation attributed to any of your responses.

You are kindly requested to send the responses to this questionnaire to the APG Secretariat at mail@apgml.org by 14 June 2017.

PART A: SOCIAL MEDIA CASE STUDIES

Please provide case studies and typologies related to all aspects of the abuse of social media for TF.

We are seeking case studies and typologies related to all aspects of social media and how it may relate to terrorism financing. This includes but is not restricted to abuse of social media by the terrorists or sympathizers for raising, moving and using funds for terrorism purposes including the dissemination of propaganda, radicalization, recruitment, communication or networking, training, planning, operations and social services (such as medical treatment, establishing and subsiding social/health/educational institutions).

We are seeking cases involving the widest possible range of social media platforms. This includes any internet based platform that enables uses' to create and share content. For example, relationship network sites (e.g. Facebook or Myspace), media sharing networks/sites (e.g. YouTube or Instagram), discussion forums (e.g. Quora), social publishing platforms (e.g. blog sites such as Penzu), e-commerce sites (e.g. crowd funding sites such as Gofundme), and internet-based messaging services (e.g. WhatsApp and Snapchat).

In addition, we welcome case studies and typologies on any social media platform, recognising that in some jurisdictions smaller or less known platforms may be popular, and new platforms are continually being developed and launched.

Please provide case studies in relation to abuse of social media for terrorism financing, which may cover the following:	
1.	Exploitation of NPOs' pages on social media platforms
2.	Fake crowd funding using social media or crowd funding sites
3.	Fundraising through cybercrimes using social media platforms
4.	Foreign-terrorist fighters generating funds for travel or as cash couriers through social media
5.	Individual mule account (sympathizers, family members of terrorists, etc.)
6.	Other cases related to social media and terrorism/terrorism financing (e.g. financing TF via on line commercials appearing on terrorist group pages in social media)

Note:

In case studies, jurisdictions are requested to describe, at minimum, the following:

1) How the case is detected (upon complaint, proactive monitoring and surveillance, STR, etc.);
2) Facts (on the social media/sites involved and purpose of these sites);
3) How the funding/donation is called for:
   a. privately or publicly;
   b. purpose of funding (as advertised and actual purpose for TF);
4) Do they have electronic payment platforms built into the social media such as Paypal, Square and CASHU among others);
5) Medium of payment and how the payment is instructed to be made (online banking, ATM, credit card, e-wallet, prepaid card, etc.);
6) Medium of communication with the content creator (private messages in the social media or mobile messaging apps e.g. FB messenger, WhatsApp, Skype, etc.);
7) Amount of funds gathered and movement of funds collected (how the funds moved, and the recipient's location);
8) End use of funds; and
9) Any other relevant information.

PART B: QUESTIONNAIRE ON MEASURES TO COUNTER THE THREAT OF SOCIAL MEDIA TO TERRORISM FINANCING

Recognizing the global threat of terrorism and TF and the broad range of ways social media can be abused by terrorists or sympathizers, it is essential to continually reinforce existing counter measures to respond to these threats. The aim of this part of the questionnaire is to obtain a comprehensive understanding of what different jurisdictions are doing to prevent the abuse of social media for terrorism and TF. Jurisdictions are kindly requested to provide as much detail as possible in response to the below questions.

Risk Assessment

1. Has your jurisdiction conducted a terrorism and terrorism financing risk assessment at regional or national level?

2. What elements of social media abuse are captured in the risk assessment, and what is the risk of social media abuse for terrorism financing purposes in your jurisdiction?

3. If there is no risk assessment or the conducted risk assessment did not capture the below aspects, please provide feedback on:
   (a) What are the major types of threats relevant to the abuse of social media for TF identified by the competent authorities in your jurisdiction (e.g. propaganda, radicalization, recruitment, communication or networking, training, planning, operations, social services, etc.)? What is the weight of these threats in your jurisdiction?
   (b) What are the vulnerabilities identified by competent authorities that are regarded as a factor increasing the risk of the abuse of social media for TF?
   (c) Where relevant, do you believe that social media abuse is not a significant threat for TF cases in your country and why?

4. Based on the experiences of the competent authorities in your country, please provide the following data for the period covering 2014 to 2016:

   (a) Number of detected cases where social media has been abused for TF.
   (b) Social media platforms used.
   (c) Number of social media group/activities/schemes detected in each platform.
   (d) Number of followers for each group detected (at the time the group/activities/schemes was detected).
   (e) Location of the moderators/owners where social media content originated from?
   (f) Average amount of funds collected for TF purposes through each social media group.
   (g) What are the payment methods used to finance TF in identified cases (e.g. prepaid cards, PayPal, wire transfers, etc.).

National policy, legal and regulatory measures in place

5. Are there any gaps in your jurisdiction's legal framework which prevent or impede the investigation and prosecution of terrorism or TF facilitated through social media? Please elaborate.

6. Has your jurisdiction passed legislation to permit disclosure/sharing of information between social media companies, internet service providers and law enforcement agencies in suspected terrorism or TF cases? Please elaborate.

7. Does your jurisdiction have policies, laws or regulations that require stricter terms of use and/or counter-measures to be imposed by social media companies and internet service providers for any extremism/TF/T data content and reporting obligations of these companies, providers and developers to the authorities? Please elaborate.

8. Do you have a national action plan to address the risks associated with the abuse of social media for terrorism/TF including participation of relevant authorities and the private sector (telecommunications regulators, social media companies, internet service providers)? Please elaborate.

Strengthening monitoring and surveillance of the social media network

9. Does your jurisdiction's law enforcement or intelligence agencies have a mechanism/s for monitoring and surveillance of the social media network to detect terrorism/TF activities? If possible, please elaborate on how the monitoring and surveillance is conducted.

10. In your jurisdiction, is there domestic cooperation (ad-hoc or permanent) between relevant national security agencies (police, ministry of home affairs, and ministry of communications, security intelligence agencies) and the FIU for gathering and sharing TF intelligence related to social media? Please elaborate.

11. Does your jurisdiction have international cooperation mechanisms with foreign FIUs or counterparts for gathering financial intelligence relating to the abuse of social media for terrorism/TF? Please elaborate.

12. Does your jurisdiction undertake other measures to mitigate the risks of abuse of social media for TF? Please elaborate.

Terrorism financing investigation: challenges and solutions

13. What are the main challenges faced by investigators in initiating and completing investigations related to TF involving social media (for instance, in gathering evidence which is permissible in court)? Please elaborate.

14. What are the main challenges faced by investigators in seeking assistance from social media companies, internet service providers and/or telecommunications regulators during an investigation? Please elaborate.

15. How do the investigators overcome the above challenges? Please elaborate.

16. Do investigators seek and obtain assistance from international/foreign law enforcement bodies such as INTERPOL? Please elaborate indicating the frequency, types of assistance, etc.

17. What are the IT tools used during investigation of cases relating to misuse of social for TF purposes?

18. Do you employ specific technical skills in investigation of cases relating to abuse of social media for TF purposes?

19. Please provide any additional information you believe is relevant to challenges and / or solutions faced by your jurisdiction during the investigation of TF related to social media.

Prosecution: challenges and/or solutions

20. What are the main challenges faced by prosecutors in prosecuting cases in relation to social media abuse for T/TF? Please elaborate.

21. What are prosecutors' experiences with social media companies, internet service providers and/or telecommunications regulators in prosecuting T/TF cases? Please elaborate.

22. How do the prosecutors overcome any challenges in working with social media companies (national and international)? Please elaborate.

23. Please provide any additional information you believe is relevant to challenges faced and / or solutions reached by your jurisdiction during the prosecution of social media TF cases.

International engagement/cooperation

24. Does your jurisdiction have information sharing arrangement and/or collaborative surveillance with foreign jurisdictions (particularly on the updated routes for Foreign Terrorist Fighters (FTF), and information on high-risk terrorists, FTF, and lone wolfs) in matters relating to social media abuse for T/TF. For example, Bilateral, in participation with FSRBs, using INTERPOL-platforms (police to police, EGMONT Group of FIUs, or through other international cooperation platforms. Please elaborate.

Collaboration with the private sector

25. Does your jurisdiction have collaboration/partnerships between competent authorities and private sector companies involved in social media and/or electronic payment platforms? Please elaborate.

Capacity building

26. Does your jurisdiction have training (leveraging on any existing domestic or international initiatives) for the private sector[20] and competent authorities[21] like policymakers, investigators, prosecutors and judges in T/TF issues related to social media? If yes, please provide further information. If not, is there any training planned for the future on this matter?

Additional questions

While the following questions are broader in scope than the current study, responses may assist in providing insight and options for other jurisdictions based on current practices being utilised.

Counter-messaging

27. Is a counter-messaging/counter narrative approach being undertaken in your jurisdiction to counter abuse of social media for T/TF purposes? Please elaborate.

Preventive measures

28. Does your jurisdiction implement other related preventive measures to counter the misuse of social media for T/TF purposes? Please elaborate.

[20] Examples of training to the private sector include dealing with cybercrime, red flags associated with TF etc..

[21] Examples of training to competent authorities include obtaining digital evidence, cross-border investigation and understanding of new high risk payment system, etc..