FATF

FATF REPORT

Emerging Terrorist Financing Risks

October 2015

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2015), *Emerging Terrorist Financing Risks,* FATF, Paris
www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

TABLE OF CONTENTS

ACRONYMS

AML	Anti-money laundering
CFT	Countering the financing of terrorism
CIFG	Counter ISIL Financing Group
ESAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FIU	Financial intelligence unit
FTF	Foreign terrorist fighter
GAFILAT	Financial Action Task Force of Latin America
ISIL	Islamic State of Iraq and Levant
MSB	Money service business
MVTS	Money value transfer services
NPO	Non-profit organisation
TF	Terrorist financing
UN	United Nations

EXECUTIVE SUMMARY

While the number and type of terrorist groups and related threats have changed over time, the basic need for terrorists to raise, move and use funds has remained the same. However, as the size, scope and structure of terrorist organisations have evolved, so too have their methods to raise and manage funds. The main objective of this report is to analyse recently identified terrorist financing (TF) methods and phenomena, referred to as 'emerging TF risks'.

This report highlights that **understanding how a terrorist organisation manages its assets is critical to starving the organisation of funds and disrupting their activities in the long term**. Terrorist organisations have different needs, depending on whether they are large, small, or simply constituted of a network of seemingly isolated individuals. The section on financial management explores the use of funds by terrorist organisations, not only for operational needs but also for propaganda, recruitment and training, and the techniques used to manage these funds, including allocating specialised financial roles. The report finds that authorities need to do further work to identify and target various entities responsible for these functions.

In assessing the continued relevance of traditional TF techniques (that is, those techniques identified in the FATF Terrorist Financing Typologies Report (FATF, 2008)) **the general conclusion is that while all these techniques are evolving, they still represent significant TF risks**. Jurisdictions provided a range of case studies to demonstrate the ongoing threats and vulnerabilities. Jurisdictions' national risk assessments were particularly useful in this analysis. Anti-money laundering (AML) and countering the financing of terrorism (CFT) systems and operational measures have made it more difficult for terrorist organisations to use traditional avenues to raise or move funds. However, **the adaptability of these organisations, and new threats posed by foreign terrorist fighters and small cell terror networks, require authorities to monitor how these traditional methods continue to be used**. The use of national risk assessments to conduct strategic analysis of current TF risks will help inform policy makers to implement the necessary legal and operational measures.

With respect to the section on emerging TF risks, the FATF decided to explore the threats and vulnerabilities posed by:

1. foreign terrorist fighters (FTFs),
2. fundraising through social media,
3. new payment products and services, and
4. the exploitation of natural resources.

The FTF phenomenon is not new, but the recent scaling up of individuals travelling to Iraq and Syria has been a challenge for many FATF members. **FTFs are predominantly using traditional methods, particularly self-funding, to raise the funds they require to travel to the conflict areas.** However, the novel aspect for jurisdictions is the challenge in identifying these individuals because of the relatively low amounts of funding they require and the speed with which they can acquire it. The report reveals that **financial intelligence can assist in identifying FTFs in a number of ways**. Close cooperation between authorities domestically and internationally and close

partnerships between authorities and the private sector can assist to better identify FTFs and their facilitation networks. The report also shows that further work is required to shed light on blind spots in information about FTFs, including returnees.

The role of social media in breeding violent extremism has been well reported but less is known about how it used to raise funds for terrorists and terrorist groups. The report finds that **there are significant vulnerabilities associated with social media, including anonymity, access to a wider range and number of potential sponsors or sympathisers and the relative ease with which it integrates electronic payment mechanisms**. It is also apparent that donors are often unaware of the end-use of funds supported by social media, including crowdfunding, which presents a risk that terrorist organisations can exploit.

This report finds that **electronic, on-line and new payment methods pose an emerging terrorism financing vulnerability which may increase over the short term** as the overall use and popularity of these systems grows. Many of these systems can be accessed globally and used to transfer funds quickly. While transactions may be traceable, it proves difficult to identify the actual end-user or beneficiary. This report presents a number of interesting cases, but the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear at this time and remains an ongoing information gap to be explored.

The **exploitation of natural resources for TF was raised as a substantial concern** in the context of the Islamic State of Iraq and the Levant (ISIL) but this report has confirmed that it is also relevant for other terrorist organisations and regions. The ability to reap high rewards from the natural resources sector, coupled with the weak institutional capability, particular in or near areas of conflict, creates a significant vulnerability for terrorist organisations to capitalise on. This report finds that this issue is linked with criminal activity including extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes.

This report builds on the findings of the *Financing of the Terrorist Organisation of the Islamic State in Iraq and the Levant* report (the 'FATF ISIL report', 2015) and takes into account the activities of a broader range of terrorist organisations. The project benefited from the involvement of national experts from FATF's entire global network, including law enforcement, intelligence agencies and Financial Intelligence Units (FIUs). This report also takes into account recent initiatives by the United Nations, the Egmont Group of FIUs and the Members of the Counter-ISIL Coalition, specifically Counter ISIL Financing Group (CIFG). The project involved private sector feedback via their involvement in the FATF/ Financial Action Task Force of Latin America (GAFILAT) Joint Experts' Meeting on Terrorism Financing. This engagement with the private sector to identify TF risks has also laid the groundwork for future initiatives to develop risk indicators which will be helpful to both private and public sectors.

This report was developed in a short timeframe to provide a snapshot of the TF risks we see today. It is not a comprehensive assessment of those risks and the issues discussed in the report should be subject to further study. **This report serves to raise awareness among FATF members and the private sector on the underlying issues that need to be addressed by policy and operational responses.** This research is intended to complement FATF's work to enhance countries' implementation of the FATF standards on TF.

I. INTRODUCTION

PURPOSE, SCOPE AND OBJECTIVES

Combatting the financing of terrorism (CFT) continues to be a priority for the FATF, given the threats posed by terrorist organisations. This threat includes small terrorist cells or individual terrorists capable of committing attacks and significantly harming society. It is therefore important to identify and dismantle the financial networks of all types of terrorist groups. In February 2015, FATF members decided to conduct further research on TF methods and trends. This research is intended to complement FATF's ongoing work to enhance countries' effective and risk-based implementation of the FATF standards on TF.

The main objective of this report is to analyse recently identified TF methods and phenomena, referred to as emerging TF risks. The report will also provide an overview of traditional methods, techniques and tools in which funds are raised, moved and stored by terrorists and terrorist organisations to assess their current significance.

This report analyses the financing activities of a range of terrorist organisations from individual terrorists or small terrorist cells to well-established international networks such as Islamic State of Iraq and Levant (ISIL), Boko Haram and Al-Qaeda and its associates and affiliates. The organisations considered in this report have either been designated by the United Nations (UN) or under national listing regimes.

The report organises the work into distinct sections:

1. financial management of terrorist organisations,
2. overview of traditional TF methods and techniques, and
3. emerging TF risks.

The FATF has coordinated with similar multilateral initiatives, to identify and understand TF risk. Such efforts include working groups recently set up by Counter-ISIL Coalition members that include the Counter-ISIL Finance Group (CIFG) and Foreign Terrorist Fighters Group (FTFG). The Egmont Group of FIUs is, through a multilateral information sharing project, studying financing related to FTFs and the operational abilities of FIUs to effectively share information. In addition, recent work on FTFs has also been done by the UN.

METHODOLOGY, PARTICIPANTS AND DATA UTILISED

This report has been prepared under the co-lead of France and the United States (US) and incorporates input from a wide variety of other delegations within FATF's global network.[1] This paper builds on the FATF report on the *Financing of the Terrorist Organisation Islamic State in Iraq*

[1] Australia, Belgium, Canada, France, Germany, India, Italy, Netherlands, Norway, Portugal, Russia, Spain, Switzerland, Turkey, the United Kingdom, the United States, APG (Thailand), ESAAMLG (Kenya), GAFILAT (Peru), GIABA, MENAFATF (Egypt, Jordan, Qatar, Saudi Arabia), MONEYVAL (Israel, Ukraine), the World Bank and the United Nations contributed to this project.

and the Levant[2] and the *FATF Terrorist Financing Typologies Report*[3] including the research referenced in those reports.

Delegations have submitted information and cases studies which identify emerging trends and risks. Some of the information provided was based on strategic analysis of data available to FIUs. The observations contained in this paper are also based on available open source material and experience and knowledge provided by delegations' participation in the FATF/GAFILAT Joint Experts' Meeting on Terrorist Financing in September 2015.

TERMINOLOGY

This report uses the following key concepts[4]:

- A **risk** is a function of three factors: threat, vulnerability and consequence.
- A **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. In this report, we have use case studies to help identify specific TF threats.
- **Vulnerability**, as used in this report, 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. This report looks at vulnerabilities separately from threat and includes factors that represent weaknesses in AML/CFT controls or certain features of a country. Vulnerabilities may also include the features of a particular sector, a financial product or type of service that make them attractive for TF purposes.
- **Consequence** refers to the impact or harm that TF may cause. It includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. Given the complexity of determining consequence, the focus of this report is primarily on achieving a comprehensive understanding of TF threats and vulnerabilities.

2 FATF (2015a).

3 FATF (2008a).

4 FATF (2013).

II. FINANCIAL MANAGEMENT OF TERRORIST ORGANISATIONS

A. USE OF FUNDS

Terrorist organisations vary in size, structure, operational reach, motivations, recruitment and capabilities. Despite differences among terrorist groups, as well as between individual terrorists and supporters, there is always a common need for financial means to transform plots into terrorist acts and to support the full range of activities that terrorist organisations engage in.

Generally speaking, the overall financial requirements to maintain a terrorist organisation's infrastructure, personnel, and activities are usually very high. This is particularly relevant for large terrorist organisations and especially those that aim to control and hold territories. Since their funds are directly linked to their operational capabilities, these terrorist organisations are seeking to ensure a stable level of fundraising. Different terrorist organisations will have different fundraising and expenditure priorities, which also change and evolve during their life cycle as they build their infrastructure and expand their influence and operational capabilities.

TERRORIST ORGANISATIONS

Terrorist organisations use funds for the following broad categories:

- **Operations:** Terrorist organisations require funds to carry out specific terrorist attacks and undertake pre-operational surveillance. This includes travel to and from the target location, the use of vehicles and other machinery and purchase of a range of arms from light assault weapons to improvised explosive devices (IEDs). Funds are also required for false identity documents and basic living expenses such as accommodation, food and basic medical treatment. Terrorist organisations also need funds for personnel such as couriers to send messages or to transport cash within the country.
- **Propaganda & recruitment:** Terrorist organisations require funding to successfully recruit members and raise funds, which can be expensive as this recruitment process involves using different means. The use of the Internet provides a less expensive mechanism to facilitate the initial steps of recruitment, but the follow-up actions require additional costs. The exploitation of social media for the purposes of terrorist recruitment and propaganda has become a priority CFT issue. While many terrorist organisations have exploited social media to solicit funds from supporters[5], more complex terrorist organisations are investing funds in sophisticated

[5] For example, the US National Terrorist Financing Risk Assessment identified nine TF-related cases that involved personal fundraising online or through social media; additionally, in August 2014 the US designated an al-Nusrah Front financial facilitator who regularly solicited funds over social media.

propaganda operations that include publishing magazines[6] and newspapers, and purchasing internet domain names and administer websites. Some terrorist groups have even acquired television and radio outlets to promote their messages and worldview.

- **Training:** All terrorist organisations seek funds to enable training of operatives and sympathisers in a number of areas including, weapons training, bomb-making, clandestine communication and ideology. In this context, terrorist groups often acquire land for use as a training camp, buildings as a safe haven for both trainers and trainee and to provide training facilities. Virtual training is also conducted via the Internet in order to reach a wide range of sympathisers.
- **Salaries and Member Compensation:** Many terrorist groups set aside funds for the salaries of their leadership and members, as well as for the families of jailed or deceased members. Providing financial security and incentives to group members can cement commitment to the organisation's goals and ideology. Terrorist groups may also provide long-term financial support to the families of deceased operatives.
- **Social Services:** Many terrorist groups use their financial resources to establish or subsidise social institutions that provide health, social, and educational services. Terrorists do this to undermine the credibility of the legitimate governments – by providing services that they say the state is neglecting – and to build support within local populations and aid recruitment efforts.

Case study 1: **Use of a school to provide material support to terrorists**

An Islamic school in southern Thailand provided a shelter for terrorists. The search of the school found guns and it was later proven that they were used in several terrorist incidents, and motorcycles which were reported to have been lost (but were in fact stolen). The search also found documents indicating forgery of receipt for stationary purchases and purchases of other teaching items in order to receive reimbursement for such items from the authorities. The school continually supported terrorist groups in various activities.

Source : Thailand

LONE ACTORS AND SMALL TERRORIST CELLS

In contrast to large terrorist organisations, small cells and individual terrorists face only minor financial needs since costs of terrorist attacks are often small. As such, lone actors and small cell terrorist networks have a much smaller funding requirement given that they do not control territory, field conventional militias, engage in recruitment or propaganda operations, operate

[6] Examples include the ISIL's "*Dabiq*" and Al Qaeda in the Arabian Peninsula (AQAP)'s "*Inspire*" online magazines.

checkpoints or deliver social services. That said, they must have the financial means to provide for their own food, shelter, communications devices, transport and any procurement requirements for terrorist plots. The text box below highlights some of the sources of funds for the attacks on the *Charlie Hebdo* office and kosher store in Paris in January 2015.

According to a Norwegian Defence Research Establishment[7] report on small cell TF, roughly 75% of the 40 violent extremist terrorist plots in Europe (between 1994 and 2013) it studied, cost less than the equivalent of USD 10 000. In terrorist plots involving lone actors and small cells, it is likely that the costs associated with the lethal component of the plot (e.g., obtaining assault rifle(s); explosives; funding pre-operational, out-of-country travel for training, etc.) represents the most expensive part of what may actually be a low cost attack.

Box 1. **General financial elements of *Charlie Hebdo* and Kosher store attacks**

The *Charlie Hebdo* and kosher store attacks, which were perpetrated with weapons, did not require a substantial amount of funds. As the three terrorists involved did not have a regular job at the time of attacks, the following sources of funding may have been used:

- A EUR 6 000 consumer loan, obtained with forged documents and cashed out.
- The proceeds of the overseas sale of a used car.
- Cash transfers linked to the sale of counterfeit goods.

Source : France

B. MANAGING RESOURCES

Like all organisations, terrorist groups must have the skills necessary to obtain, move, store and ultimately use the financial resources required to meet their aims. The long-term financial health of a terrorist organisation will impact its operational tempo, its reach, and the robustness of its campaign of violence.

Terrorist financial management requires planning and accounting for all resources and assets that the group controls, as well as its liabilities[8]. Analysis of publicly-available financial documents originally from a variety of terrorist organisations demonstrates that financial management practices (such as documenting revenue levels and sources, expenditure reporting, accounting) are particularly important for terrorist groups with advanced capabilities, and particularly those that are territorially based.

Large terrorist groups will often rely on terrorist financial managers to accumulate revenue, establish financial shelters (such as bank accounts, front and holding entities), and oversee financial disbursements. Their activities also include provisioning funds to the group's leadership, members, and operators and considering opportunities to invest any excess capital. Groups such as ISIL have

7 Oftedal, Emilie (2015), p. 7. This report is based on court convictions, and hence, the conclusions may not necessarily be the same as those based on intelligence.

8 Tom Keatinge (2014), p. 3.

actively recruited (either accidentally or intentionally) accountants, and other financial professionals, specifically to monitor the activities of financial entities within their areas of control in order to better manage revenues and minimise losses.[9] [10] The financial management function also exists in small terrorist cells, but may be less formal, and involves cell members exercising multiple organisational roles simultaneously.

Box 2. **Terrorist Financial Management: AQI/ISIL**

Financial documents from Al Qaeda in Iraq (AQI), the predecessor organisation to ISIL, show that AQI used advanced financial management practices to manage revenue sources and expenses efficiently through a specialised financing function. At the same time, it also provided an infrastructure for revenue sharing between AQI sub-units to maintain efficient and resilient capability across its area of operations in Iraq. Financial records seized by US military forces show that AQI administrative emirs made extensive use of tracking spreadsheets, expense reports, and standardized financial accounting reports.

AQI used a levy system on financing wherein local groups and cells transferred acquired revenue to "brigade" and "sector" level administrative emirs, who then passed on the funds to a provincial level administrative emir, who disbursed funds to sector-level general emirs for the financial needs of their sector after all revenue was accounted for. After dealing with the needs of sector general emirs (on the basis of need and geographic areas for priority operations), provincial administrative emirs then transferred surplus revenue to AQI general treasury via the provincial general emir. More recently, public information related to the US military operation against regional ISIL oil and finance head, Abu Sayyaf, reportedly highlights that ISIL has continued AQI's past use of advanced systems of financial management.

Source : Canada from open sources

C. CONCLUSIONS AND FINANCIAL MANAGEMENT

Working closely with counter-terrorism experts will increase awareness of the financial management strategies used by specific terrorist organisations. Areas of focus could include identification of financial collection/aggregation/accounting points within a terrorist organisation. This would include having law enforcement increase its investigative focus on the ultimate recipient of the funds within a terrorist organisation rather than just the source of funds (i.e., who receives the funds is as important as who send or facilitate the movement of the funds).

Terrorist financial management usually happens within geographic safe havens or within secure social networks, making it very difficult to penetrate and influence these actors directly. Financial managers and facilitators within terrorist organisations could be targeted with targeted financial sanctions, law enforcement or military actions. An increased focus could be placed on building state capacity for collecting and disseminating intelligence on terrorist financial managers.

9 Ottawa Citizen, (2014).

10 Telegraph (2014).

III. TRADITIONAL TERRORIST FINANCING METHODS AND TECHNIQUES

This section outlines the areas of research undertaken by the FATF (and members of its Global Network) on TF methods and risks. While FATF has conducted research on the money laundering risks associated with new payment products and services (NPPS), to include virtual currency, this research has not yet fully addressed TF risks. Therefore, NPPS are addressed in Section IV.C of this report. The key piece of FATF research on TF is the Terrorist Financing Typologies Report published in 2008. Since then, FATF has continued to develop valuable insights on areas of TF concern including abuse of the non-profit sector (NPO)[11] and the financing strategies employed by terrorist organisations such as Al-Qaeda and the Taliban, [12] ISIL[13] and Boko Haram[14]. TF risk has also been identified as part of wider studies such as FATF's 2011 report on organised maritime piracy and related kidnapping for ransom.

In general, previous research has shown that terrorist organisations rely on numerous sources of income and that they use a range of methods to move funds, often internationally, to their end point without being detected. Previous reports make it clear that terrorist organisations raise funds through inherently criminal means (for example, drug trafficking) and through legitimate activities (for example, collection of donations). This section is broken down into two main categories on generating revenue and moving funds. The topics within these categories are not organised according to risk and are intended to only provide a general overview.

A. GENERATING REVENUE

PRIVATE DONATIONS

Donations to terrorist organisations can come from a wide-variety of sources. An analysis of TF-related law enforcement cases and prosecutions in the United States since 2001 found that approximately 33% of these cases involved direct financial support from individuals to terrorist networks. [15] There is also a movement for newer terrorist organisations to look for different small-scale sources and Section IV of this report addresses fundraising though social media.

Wealthy private donors can be an important source of income for some terrorist groups. For example, the FATF ISIL report acknowledges that ISIL has received some funding from wealthy private donors in the region. Previous FATF reports have also recognised the important role that sponsors play in sustaining some terrorist organisations.

---

[11] FATF (2014a).

[12] FATF (2013b).

[13] FATF (2015).

[14] FATF (2013c).

[15] US Department of Treasury (2015), p. 44.

ABUSE AND MISUSE OF NON-PROFIT ORGANISATIONS

Terrorist entities target some non–profit organisations (NPOs) to access materials and funds from these NPOs and to exploit their networks, thus intentionally abusing the NPO. A 2014 FATF study[16] found that the abuse of NPOs, or the risk of unintentional misuse, manifests in five different ways:

- diversion of donations through affiliated individuals to terrorist organisations;
- exploitation of some NPO authorities for the sake of a terrorist organisation;
- abuse of programming/program delivery to support the terrorist organisation;
- support for recruitment into terrorist organisations and
- the creation of 'false representation and sham NPOs' through misrepresentation/fraud.

The report found that traditional transnational terrorist organisations, which mainly attempt to exploit some legitimate NPOs or create 'sham' NPOs, comprise a large number of the cases demonstrating the threat to the NPO sector.[17]

Importantly, the study also found that the NPOs at most risk of terrorist abuse are those engaged in 'service' activities which are operating in close proximity to an active terrorist threat.[18] NPOs that send funds to counterpart or 'correspondent' NPOs located in or close to where terrorists operate are vulnerable to exploitation. Unless proper due diligence is done on the counterpart NPO with sound auditing of how donated money is used, control over the use of donations can be weak and at risk of diversion to terrorist organisations.

The 2014 FATF NPO Typology report identified ongoing terrorist abuse in the global NPO sector. However, a few jurisdictions noted an increase in the misuse of some NPOs providing humanitarian assistance, either to raise funds, or to move funds to countries neighbouring a crisis zone. While no definitive conclusions can be drawn by these limited examples, according to Australia, charities and NPOs which operate in crises and war zones are at increased risk of being infiltrated and exploited by terrorist groups in these areas. Australia has also advised that funds sent to Syria and neighbouring countries for humanitarian aid are at increased risk of being used for financing terrorism if they are sent through less-established or start-up charities and NPOs that do not have proper due diligence measures/controls in place, according to the cases identified by Australia.[19]

16 FATF (2014a).

17 FATF (2014a), p. 76.

18 FATF (2014a), p. 74.

19 AUSTRAC (2014).

Case study 2: **Diversion of funds collected by a charity**

A client was receiving donations/small amounts of money from different people located in Germany in his account in Switzerland. He informed the bank that he could not open an account for his charity in Germany due to legal restrictions and so he was using his private Swiss banking account for collecting donations. The donations were meant to be withdrawn in cash and brought personally to Tanzania to build a fountain. According to the bank statements different reasons were declared by the donators: "Donation Africa Fountain", "Donation Streetwork", "Tansania Orphanage", "Mosque Building", "Koran School" etc.

Media reported that the NPO "Africa Fountain" was close to extremists related to terrorism.

Source: Switzerland

Case study 3: **Possible links between FTFs and a charitable foundation**

Netherlands noticed that some *stichtingen* (foundations) and NGO's, working in the field of e.g., charity and religion, could be linked to FTFs. As of yet there is no hard evidence of TF, but involvement of FTFs in the periphery of these legal entities has been established, and people associated with the foundations have been found to travel to Syria with large amounts of cash.

Donations were received from foreign countries, and then transferred through bank accounts of foundations that did not share similar goals or activities but were chaired by or related to the same individual. Money was eventually withdrawn from bank accounts, which made it hard to trace its end-use.

Source: The Netherlands

PROCEEDS OF CRIMINAL ACTIVITY

Previous FATF reports indicated that terrorist organisations will engage in a variety of illegal activities to generate funds. For example, terrorist organisations engaged in identity theft to raise funds via credit card fraud. Insurance and loan fraud has also featured as a means to raise funds (see insurance fraud case study from Spain below).

Smuggling of goods, including cigarettes, and associated tax fraud have also been identified as fundraising tools for terrorist organisations. Smuggling of cigarettes is an increasing TF threat in some regions such as West Africa. The FATF published a report on the illicit tobacco trade[20] which referenced a number of TF threats associated with smuggling. The smuggling and selling of antiquities and cultural artefacts were mentioned in the FATF ISIL report and continues to be of concern in areas where terrorist groups operate and have easy access to antiquities.

Bank robberies have also been identified as a viable option for terrorist organisations to access large sums of money. In addition to the references in the FATF ISIL report, bank robbery was a source of funds for the terrorist organisation Jemaah Islamiah (JI) including in the financing of one of the suspects involved in the 2002 attack in Bali Indonesia. Recently, a Dutch returnee from Syria

[20] FATF (2012).

was arrested in possession of firearms. The investigation showed that he was preparing an armed robbery, and he was suspected of planning to use the proceeds to finance terrorism.[21]

An FATF study on the opiate trade in Afghanistan[22] found that the multi-million dollar profits of drug trafficking networks have leaked into the funds of terrorist organisations. According to the United Nations Al-Qaeda & Taliban Sanctions Monitoring Team's assessments, out of the total 2011/2012 budget of the Taliban of USD 400 million - one third was raised from the poppy trade.[23] There have also been indications of links between drug trafficking and TF in West Africa, and involving groups, such as FARC and Hezbollah.[24] Terrorist organisations can receive revenue from drug trafficking, often permitting or facilitating this activity in areas where the terrorist organisation operates.

There are recent examples of TF involving tax crimes. The FATF ISIL report contains two case studies involving the use of tax refunds to fund FTFs. In other cases this may involve the failure to disclose actual sales made by a business to the tax authorities. These profits were then channelled to fund the terrorist group's activities. In Finland, four Finnish citizens were arrested in October on suspicion of having committed offences including tax fraud in order to finance extremist activities in Syria and Finland.[25]

A number of delegations increasingly see fundraising through criminal activity. See Section IV on for further examples involving criminal activity involving FTFs. Below are more detailed case studies involving criminal activity through extortion, and kidnapping for ransom.

Case study 4: **Insurance fraud simulating traffic accidents**

Since 2007, members of this plot committed several sporadic frauds to obtain benefits without raising suspicion, such as faking traffic accidents and hiring bogus policies. Compensations provided by insurance companies were quickly withdrawn in cash.

An increase in the number of frauds was observed in 2012, and a chronological overlap was established between the most obvious cases of fraud (involving members of a terrorist cell) and terrorists sent to join terrorist organisations like Movement for Unity and Jihad in West Africa (MUJWA or MUJAO) and ISIL.

It was clear that the individuals needed to obtain funds quickly, because they disregarded the need to keep their operations secret by faking numerous and rough traffic accidents which exposed them to detection.

Source : Spain

[21] Europol (2015), p.10.

[22] FATF (2013b).

[23] United Nations Security Council (2012).

[24] FATF (2013c); US Department of Treasury (2015), p.29.

[25] Europol (2015), p. 10.

Case study 5: **Use of counterfeit currencies for TF**

Indian authorities investigated a large criminal conspiracy involving nine persons, including a US citizen and a Canadian citizen who cooperated with members of *Lashkar-E-Taiba* (LeT) and *Harkat-Ul Jihadi Islami* (HUJI), both designated as terrorist organisations by Indian authorities.

On multiple occasions and over a number of years, the defendants would receive legitimate cash (e.g., Euro, US dollars) as well as counterfeit Indian/Pakistan currency from sympathisers of the terrorist organisation. For example, on one occasion the defendant received USD 25 000 to establish an immigration office in Mumbai, which was in fact a cover for his travel and maintenance while carrying out the reconnaissance of potential targets for attacks by LeT. This individual also received sufficient high quality fake Indian counterfeit currency notes for use in India.

The funds were also used to conduct reconnaissance of vital installations in India and Denmark to carry out terrorist attacks on behalf of terrorist organisations LeT and Huji. In addition, funds collected were used to make videos to support future attacks by LeT and Huji.

Source : India

EXTORTING LOCAL AND DIASPORA POPULATIONS AND BUSINESSES

FATF reports have recognised that terrorist organisations extort local populations as a way to sustain their activities. The 2014 report on the Afghan opiates trade suggests that the Taliban uses funds collected from local populations to sustain local operations, whereas donations go to the Taliban Financial Commission that reports to the senior leadership of the Taliban.[26] In the same vein, the Kurdistan Workers' Party (PKK) is known to collect funds from extortion and businesses. PKK revenue streams include the so-called taxing of illegal drugs during shipment to Turkey prior to reaching the European markets, protection and arbitration taxes', human trafficking and cigarette smuggling.[27] Similarly, ISIL extorts the income of all inhabitants in areas where it operates. The 2014 FATF report noted that Iraqi government employees remaining in ISIL territory travel to Kirkuk and elsewhere to withdraw their salaries in cash, and return to ISIL-held territory where their salaries are then "taxed" by ISIL at rates of up to 50%.[28] Furthermore, ISIL has reportedly imposed specific "taxes" on the movement of goods in parts of Iraq where it operates and extorts money from the local population (including "taxes" on customer withdrawals from private banks, fuel and vehicle taxes and school fees for children) or so-called "charitable giving" (soliciting involuntary "donations" to purchase momentary safety or temporary continuity of business). In the past, the Liberation Tigers of Tamil Eelam (LTTE) used extortion on members of the Tamil diaspora who resisted making donations to the organisation – in Canada, average extortion rates for targeted individuals and families were between CAD 2 500 and CAD 5 000, and were often more for business owners. [29]

[26] FATF (2013b).

[27] Europol TE-SAT reports (Europol, 2015, 2014, 2013).

[28] FATF (2015).

[29] Human Rights Watch (2006).

KIDNAPPING FOR RANSOM

Kidnapping for ransom (KFR) is a growing source of revenue for terrorist groups, including ISIL.[30] Paid ransoms to terrorist groups are reported to range from EUR 600 000 to EUR 8 million per ransom[31], with each ransom potentially producing between 5 – 50% of a terrorists group's total annual funding, depending on factors such as the size of the group and the local economic conditions in the geographic region of operations. The US government estimates that, between 2008 and 2014, terrorists including al-Qa'ida, ISIL, and both groups' affiliates and allies, generated at least USD 222 million in ransom payments.

A Counter-ISIL Finance Group Kidnapping for Ransom Communiqué was issued on 13 May 2015 based on United Nations Security Council resolutions 2133 (2014), 2161 (2014) and most recently 2199 (2015).[32] In addition to all cooperative efforts to prevent kidnappings, the Communiqué calls on jurisdictions to deny kidnappers the benefits of their crimes, and bring them to justice. These messages are also highlighted by the Global Counterterrorism Forum (GCTF) in the Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists.[33]

While there is no standard template for KFR, specific groups which have been listed by the UN and other entities have engaged in KFR. This includes but is not limited to: The Organisation of Al-Qaida in the Islamic Maghreb (AQIM), Abu Sayyaf Group (ASG), Al Qaeda in the Arabian Peninsula (AQAP), ISIL[34], Harakat-Ul-Ansar (HUA), as well as several terrorist groups in Pakistan.[35]

Cash often plays a significant role in KFR. Following the delivery of a ransom payment in physical cash, cash couriers move the cash to the terrorist group. [36] Ransom payments can also be paid through financial institutions, such as banks, exchange houses, insurance companies, lawyers, or alternative remittance systems such as hawalas.[37] Following the trail of funds is further complicated by the fact that a kidnapping can occur in one jurisdiction and the ransom payment be made in another.[38] There have also been examples of funds which have been raised by relatives (on behalf of the victim), through the sale of assets and loans, and through the use of trusts to store the donation for a ransom payment.

[30] FATF (2011), p 26.

[31] FATF (2011), p 28 and 31.

[32] US Department of State (2015).

[33] CGTF (nd).

[34] FATF (2015a).

[35] FATF (2011).

[36] FATF (2011), p 33.

[37] FATF (2011), p 26.

[38] FATF (2011), p 26.

Self-funding

Previous FATF reports have recognised that the amounts of money needed to fund small attacks can be raised by individual terrorists and their support networks using savings, access to credit or the proceeds of businesses under their control. The FATF's ISIL report provides a description of different self-funding techniques used primarily by foreign terrorist fighters (FTFs). See Section IV for further information on self-funding by FTFs.

LEGITIMATE COMMERCIAL ENTERPRISE

Several law enforcement investigations and prosecutions have found a nexus between a commercial enterprise, including used car dealerships and restaurant franchises, and terrorist organisations, where revenue from the commercial enterprise was being routed to support a terrorist organisation. One case involved the shipment of used cars to Western Africa. The shipment of cars to the Middle East is considered as another fund raising scheme for a particular terrorist organisation. According to an Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) member, used car dealerships imported cars from countries such as the United Kingdom, Japan and Singapore and generated revenue from the sale of these cars as part of a complex money laundering scheme, which was then funnelled to terrorist groups. The owners of those car dealerships were from areas with a high risk of terrorism.

Case study 6: **Trade based financing of terrorism**

Following the designation of company A as an unauthorised association in Israel, the company was not able to import goods through Israeli ports. Despite these restrictions, company B, a local company that imports and markets basic food products, cooperated with company A to circumvent these limitations. Company B first imported goods into Israel and then an accomplice, company C, released the goods from the port and stored them. Later, company B transferred the goods to company A in a high-risk territory for TF. As part of the settling of accounts, company A transferred funds from its accounts to company B. The value of the goods and transfers was estimated at several million in Israeli new shekel (NIS).

Source: Israel

Case study 7: **Terrorist funds sent through a front telecommunication enterprise**

In a few months, the bank account of a company A, a telecommunications enterprise, collected more than EUR 600 000 in cash. This company received large amounts of transfers, with no economic purpose, from different legitimate French companies from various economic sectors, but whose managers were originally from the same foreign country X. Some of them were suspected to have links with a terrorist organisation. EUR 500 000 was sent by the company A to a parent company B in the country X.

Source: France

STATE SPONSORSHIP OF TERRORISM

A variety of publicly-available sources and national governments have claimed that certain terrorist groups have been, and continue to be, financially supported by a number of national governments. While the FATF has not developed a typology specific to state sponsored terrorism, the funding of terrorism, or the resourcing of a terrorist entity, by any state, is incompatible with adherence to FATF standards and principles, as well as the International Convention for the Suppression of the Financing of Terrorism, and paragraphs 1(a) and 2(a) of United Nations Security Council Resolution 1373 (2001). The possibility that states may choose to provide financial support to terrorist organisations is a longstanding terrorist financing threat to international peace and security, as well as to the stability of regional financial and political systems, and fundamentally undermines the effectiveness of FATF activities that are intended to support governments in adopting best practices to detect, deter, and otherwise disrupt terrorist financing.

B. MOVEMENT OF FUNDS

The following is a short summary of the key mechanisms used to move terrorist assets. All financial institutions used to move funds are potentially vulnerable to TF by facilitating illicit fund transfers.[39] Previous FATF studies have shown linkages between local extremist groups and international terrorist organisations, with the international groups providing support to the local groups and therefore requiring the movement of funds internationally.[40] For the time being, ISIL appears to be an exception as it generates most of its funding within the territory where it operates and receives a relatively small amount of its revenue from external sources.

FUNDS TRANSFERS THROUGH BANKS

The banking sector continues to be the most reliable and efficient way to move funds internationally, and remains vulnerable to TF. The 2014 Afghan drugs trafficking report noted that the Taliban are believed to have used the regulated banking system (as well as money service businesses) to move the proceeds from drug trafficking. Several FATF reports have referred specially to the use of the bank accounts of NPOs to move funds to terrorist organisations.[41]

[39] The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF however the overall risk should be determined through an assessment of the sector. Different entities within a sector will pose higher or lower risk depending on a variety of risk including products, services, customers, and geography.

[40] FATF (2013c).

[41] FATF (2013c), p 33; FATF (2014a).

Case study 8: **Use of the banking sector to transfer international donations for TF**

An ongoing investigation in India alleges that Hizb-ul-Mujahideen (HM) has been receiving funds originating from Pakistan through different channels in support of its terrorist activities in India. HM is claimed to be actively involved in furthering terrorist activities in India and has raised over INR 800 million within the past eight years. This group has been designated as a terrorist organisation by India, US and the EU.

Funds raised in other countries are also reportedly being transferred or diverted to trusts and front organisations of HM in Pakistan. Once the money reaches India, it is distributed through various conduits at various places to the active terrorists and families of killed HM terrorists. It is further alleged that the banking sector was extensively used for transfer of funds to various bank accounts for the aforementioned activities. Funds have also been moved via money value transfer services (MVTS).

The funds are mainly used to financially support members of active and killed militants of the organisation, including family members. HM allegedly incurs expenditure on mobile communication, medical treatment of militants, arms and ammunitions, clothing and other military equipment.

Source: India

The banking sector is an attractive means for terrorist groups seeking to move funds globally because of the speed and ease at which they can move funds within the international financial system. The sheer size and scope of the international financial sector gives terrorist groups and financiers the opportunity to blend in with normal financial activity to avoid attracting attention. According to Australia, terrorism financing through the banking sector is often small-scale and can be difficult to distinguish from the large number of legitimate financial transactions undertaken each day. Some cases have involved structured deposits of cash into bank accounts followed by international funds transfers out of Australia. More complex methods have used accounts of both legitimate and shell business with an international presence as fronts for sending funds offshore through mainstream financial channels.

A concern also noted in the FATF ISIL Report is the risk that ISIL may seek to exploit the Iraqi and Syrian bank branches or other financial institutions that it controls to conduct international transactions. This would allow ISIL to more easily receive funds to finance its activities as well as send payments abroad to procure weapons and other goods in order to function.

While AML/CFT mitigation measure put in place by financial institutions are likely making it more difficult to move terrorist funds through the financial sector, the risk remains. Traditional products can be abused for terrorist financing. For example, sympathisers of a terrorist group can open savings accounts and provide the debit card associated with the card to a member of the terrorist organisation to enable to access cash via withdrawals from overseas bank ATMs.

MONEY VALUE TRANSFER SYSTEMS

19. Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to TF. In conflict-prone countries where access to banking services is limited

and terrorist groups operate, remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activity. Remittance providers are especially vulnerable to abuse for TF where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license (thus operating without any AML/CFT controls). The biggest TF threat involves agents or employees who knowingly facilitate funds transfers on behalf of terrorist groups, including the falsification of transaction reporting to obfuscate or anonymise details. Migrant communities and families rely heavily on MVTS to remit funds home; this provides a channel for commingling TF with legitimate family transfers. It also makes it difficult to detect TF from normal family and community remittances.

Case study 9: **Complicit MVTS Agent**

An individual raised funds for Al-Shabaab from within the Somali diaspora in Missouri and elsewhere and used a variety of licensed money service businesses (MSBs) with offices in the United States to remit the money to Somalia for general support of Al-Shabaab fighters. The co-conspirator, who worked for one of the MSBs involved, helped the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information. The MSB worker and other conspirators used fictitious names and phone numbers to hide the nature of their transactions.

Source: United States

Many of FATF's TF-related reports have highlighted how alternative remittance systems, especially where there is insufficient AML/CFT regulation, are exploited to facilitate TF. For example, the Taliban are believed to have used the regulated banking system to launder the proceeds of drug sales but apparently returned to the use of MVTS after the implementation of more stringent Afghan banking rules.[42] The TF in West Africa report highlights the use of MVTS to provide funds to recruit FTFs and aid their travel to conflict zones. Similarly, the ISIL report notes that a common methodology for financing FTFs is to send money via money remitters who have agents operating in border areas close to ISIL held territory. The Afghan opiates report identifies the use of MVTS to move the proceeds from drug trafficking. FATF's 2013 report on hawala and other similar service providers[43] considered the issue, noting that terrorists exploit money transmitters as 'a function of geography, culture and financial access' and that countries of high risk for this sort of abuse are also areas where these services were a legitimate and principal vehicle for value transfers, but where such providers were not subject to appropriate AML/CFT regulation or lacked AML/CFT controls.[44]

[42] FATF (2013b), p 43.

[43] This report covered money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time (p 12).

[44] FATF (2013d), p 41.

PHYSICAL TRANSPORTATION OF CASH

Cash continues to be a prevalent aspect of terrorist operations. FATF's report on TF in West Africa found that in almost all the cases it studied, cash was used and terrorist suspects were often in the possession of large amount of cash.[45] While funds may be raised in a number of ways, often they are converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies. The increase of bulk cash smuggling across borders between conduit countries and high risk areas has also been noticed.

Case study 10: **Cash couriers**

Over a period of three consecutive days three individuals declared a total amount of some EUR 90 000 in cash to customs officials at the airport in Brussels. The funds are said to originate from NPO A from Germany as part of humanitarian aid in Burundi, Benin and Zimbabwe. The three couriers are all Belgian nationals and have been living in Belgium for a long time.

Accounts were held by the three individuals. A Belgian coordinating body of a radical Islamic organisation transferred money to these accounts. Over a period of one year a total amount of nearly EUR 20 000 was withdrawn in cash. Some EUR 10 000 was transferred to Turkey.

According to the German FIU, NPO A was one of the largest Islamic organisations in Germany. NPO A is said to be linked with NPO B, which had been banned in Germany for allegedly supporting a terrorist organisation. All of NPO B's board members also played a major role in NPO A.

According to information from the Belgian intelligence services the three individuals reverenced above are known to be involved in local branches of a radical Islamic organisation. Given the nature of the transactions and the links between the two NPO referenced above, Belgian authorities suspect that at least part of the funds described above could have been used to support terrorist activities.

Source: Belgium

C. CONCLUSIONS ON TRADITIONAL TF METHODS AND TECHNIQUES

The traditional TF methods and techniques described above continue to be prevalent today and are still considered significant TF risks. The implementation of AML/CFT regulations has assisted to safeguard some aspects of the international financial sector but terrorist organisations, and the risks posed by them, are constantly evolving. The FATF will continue to monitor these areas to ensure that the current framework effectively applies to the evolving nature of how these methods and techniques are being used. The use of national risk assessments to conduct strategic analysis of current TF risks will help inform policy makers implement the necessary legal and operational measures.

[45] FATF (2013c), pp 32-33.

IV. EMERGING TERRORIST FINANCING THREATS AND VULNERABILITIES

Foreign terrorist fighters (FTFs), social media, new payment products and services, and the exploitation of natural resources are new trends that have not been subject to an in-depth TF study by the FATF. The aim of this section is to provide a broad overview of these issues and identify information gaps and challenges where they exist.

A. FOREIGN TERRORIST FIGHTERS (FTFS)

The issue of FTFs is not a new phenomenon, but the recent scale of the issue in relation to the conflict in Syria and Iraq is disturbing. United Nations Security Council Resolution (UNSCR) 2178 raises concern about the establishment of international terrorist networks, which is relevant considering the range of countries that FTFs originate from.

While FTFs are not presently considered to be a significant source of funding for ISIL or Al-Nusrah Front (ANF), they contribute to the larger TF threat posed by these groups. More importantly, FTFs are considered one of the main forms of material support[46] to terrorist groups, and thus remain a significant TF threat. Self-funding by individuals and funding by recruitment/facilitation networks are assessed as the two most common methods used to raise funds for FTFs.

FUNDING NEEDS OF FTFS

The funding needs of FTFs are generally modest and include transportation, accommodation while in route, outdoor clothing, camping goods, mobile phone/plans, food and other general living expenses. FTFs are likely to have some expenditure requirements just prior to entering the conflict zone, including the purchase of weapons. In some early instances, FTFs were relied on to bring additional funds with them when they joined the terrorist group. In the current context, particularly related to ISIL, FTFs appear to be more valuable as human resources than as funds-providers. ISIL claims to provide for FTFs and family members once they reach the conflict zone.[47]

Box 3. **Analysis of Saudi Arabian FTFs**

In 2014, Saudi Arabian authorities undertook an analysis of the account information of 1 150 individuals who travelled to the Syrian/Iraq conflict zone. The analysis revealed that three out of four of these individuals were between the ages of 20 and 30. Their sources of income included: payments from friends and relatives, loans, salary and government social support payments.

For the most part there was normal account activity in comparison to the level of income. Activity

[46] This includes "financial assets, economic recourses, property of every kind." See FATF Glossary regarding "Funds and other assets".

[47] Keatinge, Tom (2015).

also included the withdrawal of funds from international locations. As a result of this analysis, Saudi Arabian authorities blocked bank accounts related to those individuals.

Source: Saudi Arabia

SELF-FUNDING

Individuals often use funds from legitimate sources (e.g., employment income, social assistance, family support, bank loans) to finance their travel to the conflict zone. In some cases, investigations have revealed that small businesses were intentionally established and used to generate revenue that supported FTF travel. Some jurisdictions have also noted the sudden sale of assets including personal belongings and assets purchased on credit just prior to the FTFs planned travel.

In this respect, there are some similarities between FTFs and small terrorist cells. According to Norwegian studies[48], extremists who have plotted attacks in Western Europe most commonly relied on funding from the cell members' own salaries and savings. The vast majority of the cells studied (90%) were involved in income-generating activities, and half of them were entirely self-financed. Only one in four received economic support from international terrorist organisations.

Cases have been reported about FTFs continuing to receive social security or other government paid benefits from their home countries after travelling to a conflict zone. This practice is attributed to varying circumstances in different jurisdictions, including relevant authorities being unaware of the involved person's status or unable to process such information timely. It has also been reported that authorities are unable to act on information on the involved person's status, because their status as FTF is deemed not to affect their eligibility for these benefits.

Box 4. **Social security and other government paid benefits**

Between November 2013 and April 2015, Netherlands authorities have stopped payment of social security benefits to 85 FTFs. Current legislation provides various grounds to cease such payments, such as travel to a foreign country without permission of relevant authorities in the case of unemployment benefits, and residence in a country with which the Netherlands has no social security agreement.

- The current practice is thus to stop payments because requirements for eligibility are no longer met, not because the recipient is a FTF. This has proven to be a lengthy and sometimes challenging process:
- Even where information on the status of FTFs is made available through interagency co-ordination, the relevant authority needs to establish on the basis of its own research that a recipient is no longer eligible for benefits. The recipient does not have the obligation to provide proof that he or she is still eligible.
- The requirements for certain categories of benefits are such that even after travelling to a conflict zone, a FTF may still be eligible. This can be the case when the beneficiary is not required to remain in the Netherlands to receive benefits, such as student benefits, general old

[48] Oftedal, Emilie (2015).

age pension or certain allowances.

The Netherlands is drafting new legislation to better enable relevant authorities to cease payments of all benefits to FTFs within a short timeframe. A version that was recently published for public consultation provides for an independent ground for ceasing payments of benefits, namely a report by the competent law enforcement or intelligence services that the recipient:

- has joined or provides support to an terrorist organisation engaged in armed conflict; and
- therefore resides outside of the Netherlands.

Source: Netherlands

Family and associates have also knowingly or unwittingly transferred their own legitimately obtained funds to persons engaged in conflict. For example, one jurisdiction reported that half of their TF suspicious transaction reports were related to people with some form of employment with only 15% recorded as unemployed (one third did not include a customer business activity or occupation).

As noted in Section III, the proceeds generated from criminal activity remains a source of funding. However, in the case of FTFs, funds raised from criminal activity have generally been petty crimes and relatively unorganised. One emerging trend includes suspected FTFs applying for small short-terms loans from many providers simultaneously with no intention to repay the loans.

In addition to the case study noted below, the Spanish authorities have also detected that members of a terrorist cell will participate as figureheads in value-added tax (VAT) fraud and scams in other EU territories by obtaining funds for covering the costs of their own travel to conflict zones. The proceeds from this activity are often managed in cash outside the formal financial system.

Case study 11: **Non-repayment of a personal loan**

An individual received two personal loans totalling JOD 7 500. After he stopped making repayments, the bank tried to call the individual, and his employer, who mentioned that the individual had been away from work for a long period of time.

After requesting information from its counterpart, the FIU was told that this individual travelled to country (H) and then on to Turkey. The FIU of country (H) referred the case to the competent general prosecutor for a suspicion of conducting terrorist financing. The competent general prosecutor seized his and his family's moveable and immovable assets.

Source: Jordan

Case study 12: **Vishing fraud**

Courier and vishing frauds (a type of telephone scam) have been seen as a TF method. The funds have been used to finance travel to Syria and Iraq and also to sustain individuals who have travelled to these areas to fight with ISIL. UK based extremists have adopted the organised crime group tactic of targeting vulnerable individuals with phones calls purporting to be either police or banking officials. They are informed that their account(s) have been compromised in some way and are persuaded to either transfer money into accounts controlled by the suspects or to physically withdraw the cash. A courier from the criminal network is then dispatched to the victims' home address and picks up the cash.

London-based networks are known to have targeted individuals in Devon, Cornwall, Dorset, Kent, Bedfordshire and London. The method as to how the victims are selected is to date unclear but it may be as simple as online telephone directories filtered to regions for a retirement age demographic.

It is known that such networks have defrauded victims out of hundreds of thousands of pounds. Evidence shows that some money is being transferred overseas using Money Service Businesses (MSBs) to the Middle East by suspects, although the final destination of these funds is still under investigation. The amounts sent are in the low thousands for each transaction or below the GBP 500 limit so suspects do not have to provide further identification.

Source: United Kingdom

Case study 13: **Material support involving returning FTF**

The flat of a Syrian national was searched in January 2013 under an ongoing investigation, conducted by the Frankfurt Public Prosecutors' Office, for suspected preparation of a serious act of violence endangering state security. During the search, police seized computers, several data carriers as well as mobile phones. On this occasion, the individual who was the subject of the investigation received an order prohibiting him to leave the country because it was considered probable that he would again participate in combat activities in Syria. According to information obtained, he had left Germany for Syria via Turkey as early as July 2012 and had handed over EUR 9 500 of donated funds there. Subsequently, he is alleged to have joined the extremists and participated in combat activities. In early August 2012, he returned to Germany following a gunshot injury.

Source: Germany

FTFs returning from conflict zones also need access to funds. While information about the funding sources for returning FTFs is limited, some of the funding techniques to travel to the conflict zone have also been used when returning to their home country. These include fund transfers via MVTS to countries adjacent to conflict zones. Many returning FTFs will request Embassy assistance to travel back to their home country, often due to a lack of documentation.

FTF RECRUITMENT/FACILITATION NETWORKS

Recruitment networks and individuals facilitate FTFs to travel to conflict zones and join terrorist groups. Family, friends or facilitation networks also provide financial support to FTFs once they depart for the conflict zone. It appears that most groups are informal or ad hoc, depending on what assistance is required by the FTF and there are often links between facilitators in the home country and areas bordering the conflict zone.

There also appear to be links between facilitation networks and criminal organisations (some facilitation networks are not based on ideology but on profitability). Many facilitation networks will have specific recruiters (who often exploit social media applications) who sometimes include members or sympathisers of extremist groups or individuals who are loosely affiliated with extremist groups. Some networks include seemingly random individuals who send money to each other, thus forming common counter-parties and becoming a *de facto* facilitation network. FTFs also appear to get logistical support from these facilitation networks, including arranging transportation and purchasing supplies.

Funding for individuals intending to participate in conflicts may also occur through family networks, particularly through funds sent to countries neighbouring conflict zones. It is often difficult to determine the real end use of the transfers, particularly within family groups, as the majority of funding from source countries to countries near conflict zones is likely to be for legitimate family support or humanitarian reasons. Using recently acquired networks of contacts, returnees are likewise involved in facilitating aspiring FTFs transit to conflict areas and in raising money to assist in financing the travel or to support fighting groups.[49] There have also been examples involving family members paying facilitation networks to return FTFs (see Turkish case study below). This issue needs to be explored further.

The issue of indirect funding raises a number of questions about the amount that terrorist organisations expect recruits to expend and costs to the organisation itself. Terrorist organisations generally don't target their recruits personally, but categorise the recruits based on their capability, skill set and willingness.

Case study 14: **Example of European network with facilitators**

Four individuals carried out 28 funds remittances through seven different entities located in Germany and France. These transactions had 17 different beneficiaries who withdrew the funds in 16 distinct business entities, located in Egypt, Germany, Greece, Morocco, Portugal and Tunisia.

According to the analysis, the transactions linked to this group occurred between 2006 and 2013, the majority of which were in 2008. The beneficiary in Portugal withdrew the funds in January 2009, in three different entities located in Oporto. He did not have any income or property in Portugal. According to the intelligence collected through international cooperation, in 2014, the beneficiary in Portugal allegedly travelled to Syria, via Turkey, and is suspected of joining ISIL. He was later arrested when returning to Europe.

Source: Portugal

[49] Europol (2015), p.22.

Case study 15: **Paying facilitation networks to get back family members**

The Turkish National Police was approached by liaison officers in two different countries in relation to individuals that had already entered Syria through Turkey. Available information suggests that families of FTFs attempt to buy the freedom of their children who had earlier travelled illegally to Syria through facilitators' networks. There had been a number of FTFs, in particular young adults with single women or women with children, who have been assisted by the families or other individuals to exit from ISIL and were deported from Turkey to their source countries.

Source: Turkey

MOVEMENT OF FUNDS ASSOCIATED WITH FTFS

FTFs have used some of the traditional methods and techniques described in Section III to move and get access to funds. These primarily include the physical movement of cash, use of ATMs to access funds from bank accounts and use of MVTS.

Case study 16: **Use of MVTS from Middle-Eastern countries to finance fighters to join ISIL**

Ceuta and Melilla are home for many of the young Spanish recruits who are fighting in ISIL as FTFs. Although there are a wide variety of sources of revenue to pay travel costs to the conflicts zones to join ISIL as a FTF, it is more difficult for young Spanish recruits in Ceuta and Melilla to purchase plane tickets due to the high long-term unemployment rate in their districts.

Analysis was conducted on 249 transfers that took place from 1 January 2014 to 31 May 2015 via three MVTS totalling EUR 117 000 sent from Syria, Iraq, Turkey and Lebanon to Ceuta and Melilla. Most of those transfers were considered suspicious because of a lack of information regarding their purpose, and no apparent relationship between senders and receivers. In addition, some of the receivers were associated with previously filed suspicious transaction reports associated with TF.

Source: Spain

Case study 17: **Australian-based remitter's registration cancelled due to terrorism financing risks**

On 10 November 2014, AUSTRAC cancelled the registration of Bisotel Rieh Pty Ltd, a remitter based in Sydney. They took this action because of the risk Bisotel Rieh posed in relation to TF. AUSTRAC alleged that Bisotel Rieh failed to accurately report international funds transfer instructions in accordance with Australia's AML/CTF requirements.

Bisotel Rieh was alleged to have sent about AUD 18.8 million to Turkey and Lebanon between January and August 2014 and "routinely" failed to provide "the ultimate beneficiary details as to these transactions".

There was a discrepancy of approximately AUD 9 million between the reports that AUSTRAC received from Bisotel Rieh about their customers and the reports by the financial institutions who

transferred Bisotel Rieh's funds. Bisotel Rieh had also previously admitted to smuggling cash over for militants in Syria.

The owners of Bisotel Rieh acknowledged in a statement that the brother of one of the owners was a member of a proscribed terrorist organisation and had in recent months engaged in shocking behaviour in the Syria/Iraq region which the owner also found "abhorrent."

Source: Australia

CHALLENGES ASSOCIATED WITH COMBATING FTFS

A number of challenges have been identified which may hinder CFT efforts. Information gathered about FTFs is often of a highly confidential nature and its classification makes information sharing challenging. Data held by FIUs needs to be combined with contextual and de-sensitised information from operational and intelligence authorities, and the private sector entities, to provide a full picture of FTF activity. For example, it is often difficult to determine if the nature an isolated transaction (e.g., money transfer) is legitimate (e.g., family remittance) or nefarious (e.g., use to support a terrorist group). To this end, FIUs and operational authorities need the ability to liaise with the intelligence community and specific interagency task forces may need to be established.

There are also a number of gaps in the knowledge of how FTFs operate. These gaps include knowing the sources/use of funds once FTFs are in the conflict zone, the sources of funding for FTFs returning from conflict zones and the role of intermediaries at borders of conflict zones. The multilateral initiatives identified in the Introduction section of this report may address some of these gaps. The FATF is aware of efforts to create a 'financial profile' of FTFs which would articulate the characteristics of financial transactions and activity of FTFs; to include their travel to and from conflict zones.

Despite the number of challenges noted above, there have been many positive examples of how the use of financial intelligence can be used to identify and target FTF facilitators and prevent potential FTFs from traveling abroad. A number of delegations have noted increased domestic outreach to a wide range of authorities which have access to unique data sets which can be exploited for CFT purposes.

B. FUNDRAISING THROUGH SOCIAL MEDIA

The widespread access to and anonymity of the Internet and especially the rapid expansion of social media, have been exploited by terrorist groups to raise funds from sympathetic individuals globally and represents a growing TF vulnerability. Social networks are widely used by terrorist organisations to spread their terrorist propaganda and reach out globally to sympathisers. Many European and Western FTFs are actively using social media to document their experience in the conflict zone in real time. Rather than relying on official accounts provided by terrorist groups, most of these FTFs look to and receive information about the conflict from so-called disseminators. These disseminators are officially unaffiliated with a terrorist organisation but are sympathetic to the ideology and significantly invested in the conflict. This has reduced the ability of terrorist groups to

control information, giving private individuals greater influence over how the conflict is perceived by those involved in it.[50]

Social networks are being also used to coordinate fundraising campaigns. Large-scale and well-organised fundraising schemes aimed at TF may involve up to several thousand 'sponsors' and may raise significant amounts of cash. Terrorist organisations are now able to conduct outreach to a large audience through a peer-to-peer horizontal communication, that starts on chats and forums, goes on through social networks (such as Facebook, Twitter and Instagram), and sometimes keeps on going through mobile application for communication (such as WhatsApp and Viber) or more secure communications networks (such as Surespot and VoIP). In addition to targeting would-be FTFs on social media networks, donors are also a priority target group.

Case study 18: **Explicit calls for funds on social networks**

In a Facebook group on recipes for women, one of the users placed a call for funds in 2013. A fighter in Syria was mentioned (no name indicated) who urgently needed "equipment, food and pharmaceuticals". There was time to collect funds until "Thursday", in order to "dispatch" the requested material by "Friday". The user also provided the details of an account held with a German bank where the funds were to be sent. It is unknown if the author of the Facebook call for funds is also the person responsible for this initiative. The owner of the account is a convert, who is suspected of coordinating this advertising campaign.

Source : Germany

The use of organised crowdfunding techniques also represents an emerging TF risk. Crowdfunding is an Internet-enabled way for businesses, organisations, or individuals to raise money, from donations or investments, from multiple individuals. Crowdfunding websites allow people to easily set up a fundraising page and collect donations. Yet, crowdfunding is vulnerable to exploitation for illicit purposes, including instances where the true purpose of the funding campaign is masked. Individuals and organisations seeking to fundraise for terrorism and extremism support may claim to be engaging in legitimate charitable or humanitarian activities and may establish NPOs for these purposes. Several cases indicate that the end-use of funds collected through crowdfunding and social networks was not known to donors.

As well as raising funds for TF purposes, crowdfunding techniques could also be used to transfer funds abroad by avoiding regulated financial entities.

Case study 19: **Crowdfunding**

The FIU of Canada has 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. In one example, a reporting entity received information from law enforcement that an individual left Canada, which prompted an

[50] Carter, J.A., Maher, S. and Neumann, P.R. (2014).

account review and a suspicious transaction report (STR) being sent to FIU Canada. 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, with a known crowdfunding website (web address provided). This merchant is categorised by its merchant bank as "Professional Services". 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: Canada

Individuals and organisations seeking to fundraise for terrorism and extremism support may attempt to disguise their activities by claiming to be engaged in legitimate charitable or humanitarian activities and may establish NPOs for these purposes. Legitimate charities have set up viral campaigns on social networks to gain followers, and encourage donations. This approach is also being used by bogus NPOs. Funds can be raised overtly or under the guise of humanitarian aid. Funds can be raised via social media, or via more formal crowdfunding platforms. The FATF ISIL report addressed this issue in some detail.[51]

Collected funds will pay for material support for FTFs (payment for mobile communication, air tickets, as well as different goods and services ordered via the Internet), or serve as operational funds to undertake a terrorist attack. However, several cases indicate that the donors from crowdfunding and social network did not know the end-use of the collected funds. For example, there are on-going investigations involving the creation of false crowdfunding campaigns by violent extremists as a ruse to obtain funds.

Fundraising advertisements are usually placed in social networks and thematic websites, as well as in specialised media, closed online forums and sent in private messages. In order to conceal the real purposes of fundraising and avoid blocking, such advertisements often do not contain direct references to fundraising for TF but use ambiguous language or the pretext of collecting funds for charitable and humanitarian purposes. Fundraising advertisements and financial details may be placed in different formats rather than in a text (for example, as an image or video), which makes it impossible to detect them through the standard search engines and makes it difficult to identify sites that contain these advertisements, as well as to explore advertisements using known financial details.

The majority of social networks used by terrorists inadvertently provide terrorist groups and their adherents a platform for TF. It should be emphasised that the companies providing these social networks themselves are not participants of such criminal activities, and in many cases cooperate with the competent authorities on providing information, and the closing or blocking of such accounts. In the second half of 2014, social media platforms such as Twitter, stepped up their efforts to suspend accounts that were pivotal for the dissemination of terrorist propaganda.[52]

[51] FATF (2015a), pp.24-26.

[52] Europol (2015), p.13.

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

Case study 20: **Social network fundraising with prepaid card**

Individuals associated with ISIL called for donations via Twitter and asked the donors to contact them through Skype. Once on Skype, those individuals asked donors to buy an international prepaid card (a credit for mobile phone or the purchase of an Apple or other programs or credit for playing on the Internet) and send them the number of this prepaid card via Skype. Then, the fundraiser sent this card number to one of his followers in a neighbouring country from Syria, who would sell this card number at a lower price and give the cash proceeds to ISIL.

Source: Saudi Arabia

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

Case study 21: **Large-scale crowdfunding scheme, with e-wallets**

A group of individuals led by Mr. A (Group A) organised a scheme to raise funds via social networks and the internet. This group of individuals registered numerous e-wallets, credit cards and mobile phone numbers. The financial requisites were placed on the internet (including social networks) under the pretext of collecting donations for Syrian refugees, people in need of medical and financial aid, and for the construction of mosques, schools and kindergartens. The wording contained some indirect indications that the money was intended as financial support for terrorist activities. Indeed, the funds were sent as an aid for terrorists and their families and to support terrorist activities.

The money was sent either to credit card accounts or to e-wallets. Collected funds were moved through a chain of transfers and were withdrawn in cash to be further transported by couriers. The payment instruments were managed via the internet (using mobile devices as well).

Source: Russian Federation

Some cases show that the money is being moved in several stages: collected funds are moved through a chain of electronic transfers and then withdrawn in cash to be further transported by

couriers. In some cases, the cash is being re-deposited in other accounts. Those schemes aim to break the operational chain and conceal the source of the funds and the final beneficiaries. Funds are also shuttled through multiple jurisdictions or sent through conduit neighbouring countries to reduce suspicion.

Social media companies themselves are not complicit in terrorism financing, but generally cooperate with authorities on providing information, closing and blocking of such accounts. Crowdfunding platforms and payment processors can provide valuable information to an investigation when misconduct is suspected. In most cases, responses to legal processes have included personal identification information, transaction details, IP addresses, and account information.

Case study 22: **Charity prosecuted for terrorist financing thanks to social media**

A charity was created in 2012 to raise funds for humanitarian projects in Palestinian territories and Syria. After a donation campaign, in August 2013, this charity brought two ambulances to Syria with medical material to build a hospital. Pictures were posted on Facebook to attest to the reality of the project and communicate with donors.

A month later, the charity made a new call for funds on social networks, indicating that three members of the association planned to bring funds to Turkey. A customs control at a French airport revealed that each of them carried EUR 9 900, below the declaration threshold, but only EUR 6 000 were to be used for the humanitarian project. The remaining funds were to be given to FTFs.

In January 2014, an administrative order froze the assets of the association and four of its members. In November 2014, the association was dissolved, and two members were arrested for TF and criminal conspiracy in connection with a terrorist enterprise. Law enforcement authorities used Facebook public messages and pictures as evidence.

Source: France

CHALLENGES ASSOCIATED WITH THE USE OF SOCIAL MEDIA

There are a number of interrelated CFT challenges associated with the use of the social media to raise funds. Often, it is not possible to distinguish between the sympathisers, supporters and actual terrorists. Due to false declaration of fundraising purposes, the identification of persons contributing money, either intentionally or unwittingly, is a serious challenge to competent authorities. It is often difficult to get evidence of the use of funds when transferred via the Internet. Social networks are used to show the relationships, but finding proof of TF is still difficult. Some delegations have suggested considering possibilities to monitor, block or remove websites to prevent their use (where law applies and while keeping in mind and respecting privacy and human rights). Further discussion could be considered about the possibilities of referring crowdfunding platforms and other companies as reporting entities and adapting legislation and regulations on new payment methods.

More work remains to be done to better leverage social media information for investigative purposes and including it as court evidence. Competent authorities could share additional strategic

information with reporting entities via clear legal channels. In that regard, the competent authorities should consider further collaboration with the private sector to get access to more data and analysis, including adapting fields in reporting requirements for online information.

C. NEW PAYMENT PRODUCTS AND SERVICES

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

Many evolving methods are similar to money laundering techniques employed by organised crime groups and exploit emerging and increasingly prevalent technologies. Between 2006 and 2010[53], the FATF issued typologies reports which focused on: the potential for NPPS to be misused by criminals; the identification of risk factors which can significantly differ from one new payment product or service to another, depending on functionality; and risk mitigates which can be tailored to a particular new payment product or service to address its specific risk profile. In 2013 the FATF issued guidance on taking a risk-based approach to prepaid cards, mobile payments and internet payment systems.

VIRTUAL CURRENCIES

Virtual currencies have emerged and attracted investment in payment infrastructure built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. At the same time, virtual currency payment products and services (VCPPS) present ML/TF risks. The FATF made a preliminary assessment of these ML/TF risks in the report Virtual Currencies Key Definitions and Potential AML/CFT Risks[54]. As part of a staged approach, the FATF has also developed Guidance[55] focusing on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers.

Virtual currencies such as bitcoin, while representing a great opportunity for financial innovation, have attracted the attention of various criminal groups, and may pose a risk for TF. This technology allows for anonymous transfer of funds internationally. While the original purchase of the currency may be visible (e.g., through the banking system), all following transfers of the virtual currency are difficult to detect. The US Secret Service has observed that criminals are looking for and finding virtual currencies that offer: anonymity for both users and transactions; the ability to move illicit proceeds from one country to another quickly; low volatility, which results in lower exchange risk; widespread adoption in the criminal underground; and reliability.

---

53 FATF (2006, 2008b and 2010).

54 FATF (2014b).

55 FATF (2015b).

Case study 23: **Promotion of virtual currency to fund terrorism**

On 28 August 2015 Ali Shukri Amin was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL.

Amin pleaded guilty on 11 June 2015. He admitted to using Twitter to provide advice and encouragement to ISIL and its supporters. Amin, who used the Twitter handle @Amreekiwitness, provided instructions on how to use bitcoin, a virtual currency, to mask the provision of funds to ISIL, as well as facilitation to ISIL supporters seeking to travel to Syria to fight with ISIL. Additionally, Amin admitted that he facilitated travel for a Virginia teenager, who travelled to Syria to join ISIL in January 2015. This teenager, was charged on 10 June 2015, in the Eastern District of Virginia with conspiring to provide material support to terrorists, conspiring to provide material support to ISIL and conspiring to kill and injure people abroad.

Amin's Twitter account boasted over 4 000 followers and was used as a pro-ISIL platform during the course of over 7 000 tweets. Specifically, Amin used this account to conduct twitter-based conversations on ways to develop financial support for ISIL using on-line currency, such as bitcoin, and ways to establish a secure donation system or fund for ISIL.

For example, Amin tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen.

Source: United States

Law enforcement agencies are also concerned about the use of virtual currencies (VC) by terrorist organisations. They have seen the use of websites affiliated with terrorist organisations to promote the collection bitcoin donations (see above case study). In addition, law enforcement has identified internet discussions among extremists regarding the use of VC to purchase arms and education of less technical extremists on use of VC. For example, a posting on a blog linked to ISIL proposed using bitcoin to fund global extremist efforts.

PREPAID CARDS

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

Prepaid cards are replacing travellers' cheques as a method of moving money offshore In terms of TF risk, these cards can be loaded domestically via cash or non-reportable electronic methods and carried offshore inconspicuously with no requirement to declare their movement across the border. On arrival in a high-risk country or transit country for TF, the funds are then converted back to cash through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Once a loaded card has been carried offshore, funds are accessible with minimal chance of detection.

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

Many of the large, reputable companies will capture relevant data and have records similar to credit cards or debit records. In such cases, the companies can provide this data to competent authorities via compulsory measures such as a court order. This can include information about the card itself including:

- activation date,
- card holder information such as phone and e-mail address,
- transaction activity,
- transaction time and location and
- IP addresses used when logging in.

Case study 24: **Example of prepaid card marketed for travel**

One Australian product allows the online self-transfer of AUD 5 000 onto the card over a 24-hour period and an overall maximum of AUD 20 000 to be stored on the card over a 21 day period. Ongoing storage of AUD 5 000 per day via domestic electronic funds transfers removes visibility of these funds and allows for easier cross-border movement of the funds with less scrutiny than the same cash amount on exit from the country. These cards are chip and PIN protected and funds can be withdrawn from any location where MasterCard is accepted.

Source: Australia

INTERNET-BASED PAYMENT SERVICES

Internet-based payment services provide mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider. Pre-funded accounts that consumers use for online auction payments are among the most dominant Internet-based payment services. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Some TF cases involving low-value transactions via

online payment systems such as PayPal have also been linked to a number of terrorism suspects. The extent to which these transactions have been used to finance terrorism is unclear.

Terrorism suspects have been observed using multiple online payment accounts, combining both verified and guest accounts. Payments appear to be linked to online purchases of equipment and clothing prior to the departure of individuals travelling to conflict zones rather than direct payments to associates to fund terrorist activities.

The use of online payment systems for these purchases is unremarkable given the ages of most terrorism suspects and their familiarity with online purchasing. Approximately half of all terrorism financing suspicious transaction reports concern customers aged between 21 and 35 years. The use of an online payment system to assist in financing terrorism is more a reflection of the prevalence of this payment system in the wider financial system rather than any indication that online payment systems are more vulnerable to terrorism financing.

Case study 25: **PayPal accounts used for fundraising**

A charity, set up in 2010, whose chairman is specialised in e-marketing, offers on its website several options to make donations by credit card, PayPal, cash transfers, checks.

Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. Of the EUR 2 million collected, EUR 600 000 came from a few PayPal transactions from another country.

Personal PayPal accounts were also used to collects funds, then to be withdrawn by cash, or transferred to other accounts.

Source: France

Case study 26: **CashU**

Law enforcement identified the use of CashU accounts to anonymously engage in transactions for illicit purposes. CashU is a prepaid online and mobile payment method available in the Middle East and North Africa, a region with a large and young population with very limited access to credit cards. Because of this, CashU has become one of the most popular alternative payment options for young Arabic online gamers and e-commerce buyers. CashU was established in 2003 by Maktoob in Amman, Jordan but when Yahoo! acquired Maktoob in November 2009, the ownership of CashU was transferred to Jabbar Internet Group. Today, CashU has established offices in Dubai, Amman and Cyprus. CashU uses courier companies in the UAE to collect cash from customers. CashU is mainly used for paying for online games, VoIP, matrimonial, IT services, FX trading and download of music and software. They have a strict policy to not accept merchants providing gambling and sexual content. CashU also provides a parental control feature allowing parents to limit and control where their kids spend money online.

Source: United States

CHALLENGES ASSOCIATED WITH NEW PAYMENT PRODUCTS AND SERVICES

The rapid development, increased functionality, and growing use of new payment products and services (NPPS) globally have created AML challenges for countries and private sector. Notwithstanding the known vulnerabilities, the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear at this time and remains an ongoing information gap to be explored.

D. EXPLOITATION OF NATURAL RESOURCES

The exploitation of natural resources is considered a subset of how terrorist organisations control and occupy territory (see ISIL Report[56]). This issue is also linked to how terrorist organisations fund themselves through criminal activity and through potential links to organised crime groups. Criminal activity related to this sector includes extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes.

In countries where the government lacks effective control of territory and its resources, the natural resource sector may be vulnerable to exploitation for TF. Terrorist organisations could use these resources as a means to raise funds by controlling or exploiting a wide variety of vulnerable resources to include gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g., ivory trading) and charcoal (e.g., in Somalia). These sectors represent a profitable source of revenue and may also be appealing because of weak regulation in the sector. Also relevant is the low level of detection, prosecution and lower penalties associated with criminal activity involving these sectors. There is also a higher TF risk in regions with a history of weak institutions, political instability, conflict areas and those regions rich in untapped natural resources. This is particularly relevant in West Africa and parts of South America.

Companies that extract and/or exploit natural resources can be vulnerable to extortion, kidnaping of their employees for ransom or by being extorted by terrorist groups in order to operate in certain regions. The FATF ISIL report also notes funding sources which included extorting farmers and crop producers, and other resource extraction and production facilities.[57] Across Africa, criminals, militias and terrorists illicitly "tax" charcoal, commonly up to 30% of the value. The illegal trading and taxation at roadblock checkpoints and ports from charcoal traffic is considered to be Al-Shabaab's primary source of income which is valued at 38-56 million USD.[58]

OIL AND GAS SECTOR

The FATF ISIL report notes that ISIL seeks to operate local oil infrastructure, to extract and refine oil for its own use, and for onward sale or swap to local and regional markets, at a lower market price. ISIL benefits mostly from using the petroleum and petroleum products it controls or by earning revenue from sales of these resources to local customers. The remaining portion of ISIL's oil revenue stems from sales routed through middlemen and smugglers who trade and transport the

[56] FATF (2015a).

[57] FATF (2015a).

[58] UNEP (2014).

illicit petroleum and petroleum products for sale to end-users. According to press reports, ISIL is paid mostly in cash for the oil it sells, making the transactions underlying its oil trade difficult to track and disrupt.

The exploitation of oil and gas also takes place in other regions of the world. For example, about 10% of Nigeria's oil production of 2 million barrels per day is stolen through highly organised transnational criminal operations involving networks of criminals, corrupt politicians and military officials. Locals call the practice "bunkering". Thieves use hacksaws and blades to cut into the pipes. When the companies see the pressure drop on their lines, they dial back the pressure just long enough for thieves to attach spigots to the lines. As the pressure rises back up, the thieves simply divert some of the oil out of the line to their own uses.[59] There is a high risk that the proceeds of such operations go to extremist groups such as Movement for the Emancipation of the Niger Delta.

Case study 27: **TF cases in Columbia involving oil**

The Attorney General Office investigated senior executives of SICIM, a multinational oil company, on the grounds of linkages with Colombian groups that commit acts of terrorism (National Liberation Army - the ELN- and the Revolutionary Armed Forces of Colombia - FARC). SICIM is an Italian-Argentinian company that provides services of infrastructure of pipeline installations and facilities for gas, oil and water transportation, with a presence in 20 countries. The company was hired in 2011 to build one of the most important oil infrastructure projects of the country: the Bicentennial Pipeline. Previous records of the company in Colombia linked SICIM to a German oil company, Mannesmann, involved in a scandal regarding extortion payments to ELN group.

At the beginning of the Colombian authorities' criminal investigation, the Attorney General's Office identified focal points of the Domingo Lain Front of ELN in charge of the finances of the organisation. Through traditional investigative techniques, including interception of communications, the Attorney General's Office discovered that two SICIM employees who served as senior executives, manager and legal representative, had links with the financial focal points of the Domingo Lain Front of ELN, and provided financial support to the terrorist organisation to continue building the oil infrastructure. Although those payments at the beginning were reported by SICIM as victims of extortion, the Attorney General's Office could collect enough evidences that showed a level of collaboration between the two senior executives of SICIM and ELN. Indeed, payments made by these two employees strengthened the finances of the Eastern Fronts of FARC and ELN. Among them, one of the payments involved USD 6 million, which was divided equally between both terrorist groups.

Nevertheless, the links between SICIM employees and ELN was far beyond the multimillion dollar extortion payments, as it also implied requests from SICIM senior executives to ELN to threaten other companies of the same oil sector with presence in the area, by conducting violent acts such as extortion and destroying machinery. Thus, SICIM employees participated in bribing local police and military officers, as well as prosecutors and judges. In November 2014, ELN murdered its contact points in charge of relations with SICIM, as well as the undercover agent of the Attorney General's

[59] Gambrell, John and Associated Press (2013).

Office. Afterwards, the Attorney General's Office issued arrest warrants against the two senior executives of SICIM and three members of ELN.

Source: UNODC

MINING SECTOR

Mining companies often operate in areas that are ungoverned or under the control of corrupt officials. Sometimes, these same areas have a significant presence of terrorist groups. For example, in West Africa, groups such as AQIM and MUJAO use protection and extortion rackets to exploit resources. There are often low barriers of entry into the mining sector. Operators of mining operations may be sympathisers of terrorist organisations and may seek to contribute financially to the cause of terrorist organisations. There is a risk that the donations from legal and illegal mining operators could be sent directly or indirectly to terrorist groups.

Case study 28: **TF cases in Colombia involving the mining sector**

"Anostomus" Operation was a joint, interagency and coordinated operation conducted by troops of the Army, Navy, Air Force, National Police, members of the Technical Investigation Corps - CTI (by its acronym in Spanish) and the Attorney General's Office in Colombia, involving 600 police and military officers. The operation was carried out in the Amazon region against the financial sources of the Revolutionary Armed Forces of Colombia - FARC (by its acronym in Spanish) from the gold mines and industrial black sands as tungsten and coltan. Indeed FARC collects funds from extortion of different actors of the chain of exploitation of mines, including entry fee and use of machinery, work authorisation, charges to traditional miners and to gold mines, as well as incomes from allowing transportation and commercialisation of precious metals.

As a result of the tactical intervention, "Anostomus" Operation successfully prevented USD 8 010 000 from the mining sector to enter into the treasury of the Revolutionary Armed Forces of Colombia - FARC. Thus, the network of illegal finance and support from FARC, including the "Acacio Medina" and "Jose Antonio Paez XVI" fronts, and the moving company "Urias Rondon", were dismantled. In addition, the investigation involved 63 mines where 59 persons were arrested, including 12 members of FARC; 8 dredges and 50 mining machines were confiscated and destroyed; 9 camps of FARC and 8 laboratories were destroyed; 6 weapons were confiscated, and 4 tons of food was seized.

Source: UNODC

Illegal activities related to gold mining occur all over South America, but in Colombia there are suspected links between drug trafficking and the armed actions of the FARC. The Colombian government recognises that 87% of metal production units operate outside the law and that this activity has displaced cocaine trafficking in some regions taken by the rebel group, such as Choco, Caqueta and Amazonas.

CHALLENGES ASSOCIATED WITH EXPLOITATION OF NATURAL RESOURCES

The investigation of crimes associated with the natural resources sector, including TF-related investigations, are often complex and requires extensive financial analysis. It is often difficult to identify the entire criminal network and specific actors (including facilitators) who are committing these crimes. This also leads to challenges in the prosecution of these crimes. It is important to identify all the operators in the sector, both legal and illegal, in order to take steps to deal with the illegal operators through law enforcement measures. Additionally, targeting smugglers and smuggling networks, which often extend beyond the source country of the natural resources in addition to the area in the immediate control of the group, will assist in combating this method of raising funds.

In order to overcome these challenges it will be necessary to consider how the public and private sectors can collaborate and include actors outside of the traditional scope of the AML/CFT regime. Strengthening legislative and regulatory frameworks within these sectors is also critical. This is especially true given the vast sums that terrorist groups can generate through the exploitation of natural resources. To adequately tackle these issues, the public and private sectors need to be aware of the vulnerabilities of this sector as the possible links of TF to corruption and organised crime.

OVERALL CONCLUSIONS

While terrorist organisations are continuing to adapt and counter law enforcement responses, it is clear that they continue to require resources to meet their destructive goals. Following the financial trail, and **understanding how all types of terrorist organisations, whether large territorially-based or small cells operating autonomously, need, use and manage funds is critical in detecting, preventing and sanctioning terrorist and terrorist financing activity**. Understanding and exchanging information on the financial management of terrorist organisations is important in order to implement CFT measures effectively.

While the emerging risks identified in this document require monitoring by law enforcement agencies, it is important to note that the **traditional terrorist financing methods and techniques described in Section III of this report continue to present significant TF risks**. These risks evolve. For example, the proceeds of criminal activity are an important source of funds for terrorists; however, jurisdictions have noted an increase in self-funding through legitimate means such as personal and business income.

The prevalence of reliable and efficient mechanisms to move funds internationally, such as banks, money value transfers systems or internet-based payment services, make them attractive vehicles to move funds for terrorism. While there are characteristics of new payment products and services that make them vulnerable to abuse, the actual prevalence and level of exploitation of these products is not clear at this time. Like criminals, terrorists and their sympathisers are interested in using technologies which maximise anonymity and are relatively cost-effective.

This report has explored some of the emerging risks that the members of the FATF's global network have identified, but further work is required. For example, further input is required on how FTFs operate their finances in the conflict zone, how FTFs source the funds to return home and the role of intermediaries which facilitate FTF activities at the borders of conflict zones. Further information is also required on the risks posed by fundraising through social media, especially where donors are unwittingly providing funds to terrorist organisations. Additionally, jurisdictions should ensure that their implementation of the FATF standards applicable to new payment methods and providers sufficiently address any new TF vulnerabilities.

There is also a lack of concrete data regarding the financial flows related to illicit exploitation and smuggling of natural resources, especially in relation to terrorist organisations. Further work could be undertaken to ensure that international standards allow for the detection and blocking of such sources of TF and jurisdictions should ensure that their CFT regimes comply with its requirements of UNSCR 2199.

This report is intended to assist jurisdictions and the private sector to implement robust CFT systems which take into account changing TF risks, trends and methods. **The FATF Recommendations provide the necessary AML/CFT framework to address the TF risks identified in this report but effective implementation of these standards is key.** For instance, developing national, or specific, terrorist financing risk assessments will provide a basis for implementing a risk-based response to addressing TF. The use of these risk assessments to conduct

strategic analysis of current TF risks will help inform policy makers implement the necessary legal and operational measures.

In conducting this study, jurisdictions noted **the importance of genuine private/public partnerships to enhance awareness of, and responses to, emerging TF risks**. Providing accurate and forward-looking guidance to the private sector improves their monitoring and screening processes and reporting-time on sensitive transactions which may relate to TF. This close collaboration could develop various mechanisms to both identify and communicate TF risk, from the elaboration stage of a national risk assessment, up to giving precise feedback to reporting entities. As information gathered by domestic authorities is often of a highly confidential nature and its classification makes information sharing challenging, a common solution that was proposed was the use of specialised, secure and non-public advisories to communicate the latest TF risks. Furthermore, there should be an increased focus on developing public-private sector forums that enable legal exchanges of operationally-relevant information on terrorist financing characteristics.

Financial intelligence is a necessary component for all counter terrorism activities, and use of relevant and appropriate non-financial information is essential for TF investigations. National CT authorities should continue to leverage financial intelligence, and also promote international financial intelligence-sharing on priority CT issues through organisations such as the Egmont Group or Interpol and bilateral and multilateral information exchange through FIUs. In order to capitalise on the benefits of financial intelligence, FIUs, operational authorities and intelligence agencies must continue to improve mechanisms to share information on emerging risks. An area of focus could include identifying and targeting financial collection/aggregation/accounting points within a terrorist organisation. This would increase law enforcement agencies' ability to increase their investigative focus on the ultimate recipients of the funds, rather than just the source of the funds.

BIBLIOGRAPHY AND REFERENCES

AUSTRAC (2014), *Terrorism financing in Australia 2014,* Commonwealth of Australia, West Chatswood, Australia, www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf, accessed September 2015

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

CGTF (nd), Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists, CGTF, https://www.thegctf.org/documents/10162/159874/Algiers+Memorandum-English.pdf

Europol (2015), *EU Terrorism Situtation & Trend Report (TE-SAT) 2015*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015

Europol (2014), *TE-SAT 2014 : European Union Terrorism Situtation and Trend Report 2014*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

Europol (2013), *TE-SAT 2013 - EU Terrorism Situtation and Trend Report 2014*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/te-sat-2013-eu-terrorism-situation-and-trend-report

FATF (2015a), *Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL),* (the 'FATF ISIL report'), FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015b), *Guidance to a Risk-Based Approach to Virtual Currencies*, FATF, Paris, France, www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF (2014a), *Risk of terrorist abuse in non-profit organisations* (the "NPO report'), FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

FATF (2014b), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

FATF (2013a), FATF Guidance, *National Money Laundering and Terrorist Financing Risk* Assessment, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2013b), *Financial flows linked to the production and trafficking of Afghan opiates,* (the "Afghan Opiates report"), FATF Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financial-flows-afghan-opiates.html

FATF (2013c), Terrorist Financing in West Africa "TF in West Africa report", FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/tf-west-africa.html

FATF (2013d), *The role of Hawala and other similar service providers in money laundering and terrorist financing*, Hawala report, p 41, www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2012), *Illicit Tobacco Trade, FATF, Paris, France* www.fatf-gafi.org/publications/methodsandtrends/documents/illicittobaccotrade.html

FATF (2011), *Organised Maritime Piracy and Related Kidnapping for Ransom,* FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/organisedmaritimepiracyandrelatedkidnappingforransom.html

FATF (2010), *Money Laundering Using New Payment Methods*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html

FATF (2008a), *FATF Terrorist Financing Typologies Report*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html

FATF (2008b), Money Laundering & Terrorist Financing Vulnerabilities of Commercial Website and Internet Payment Systems, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html

FATF (2006), Report on New Payment Methods, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/reportonnewpaymentmethods.html

Gambrell, John and Associated Press (2013), "Oil bunkering threatens Nigeria's economy, environment", *Washington Post,* Washington, United States, July 20, 2013, https://www.washingtonpost.com/national/oil-bunkering-threatens-nigerias-economy-environment/2013/07/18/e38cb4a0-e273-11e2-aef3-339619eab080_story.html, accessed September 2015.

Human Rights Watch (2006), "*Funding the Final War: LTTE Intimidation and Extortion in the Tamil Diaspora*", Volume 18, No.1 (2006), www.hrw.org/reports/2006/ltte0306/ltte0306webwcover.pdf, accessed September 2015

Keatinge, Tom (2014), "The Role of Finance in Defeating Al-Shabaab", *Whitehall Report 2-14*, Royal United Services Institute (RUSI), United Kingdom, December 2014, www.rusi.org/downloads/assets/201412_WHR_2-14_Keatinge_Web.pdf, accessed September 2015

Keatinge, Tom (2015), *Identifying Foreign Terrorist Fighters : the role of public-private partnership, information sharing and financial intelligence*, Royal United Services Institute (RUSI), United Kingdom, July 2015, www.rusi.org/downloads/assets/201506_OP_Identifying_Foreign_Terrorist_Fighters.pdf , accessed September 2015

Telegraph (2014), "How ISIL is funded, trained and operating in Iraq and Syria" (Harriet Alexander and Alistair Beach), August 23, 2014, www.telegraph.co.uk/news/worldnews/middleeast/iraq/11052919/How-Isil-is-funded-trained-and-operating-in-Iraq-and-Syria.html, accessed September 2015.

Oftedal, Emilie (2015), *The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI), Norway, 6 January, 2015, www.ffi.no/no/Rapporter/14-02234.pdf

Ottawa Citizen (2014), "ISIL using social media to lure young teenagers, accountants, engineers to its cause" (David Pugliese), Ottawa Citizen, Ottawa, December 16, 2014 http://ottawacitizen.com/news/national/defence-watch/isil-using-social-media-to-lure-young-teenagers-accountants-engineers-to-its-cause, accessed September 2015

United Nations Al-Qaeda & Taliban Sanctions Monitoring Team, First report of the Analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2012_683.pdf, accessed 18 October 2015

UNEP (2014), The Environmental Crime Crisis – Threats to Sustainable Development from Illegal Exploitation and Trade in Wildlife and Forest Resources. A UNEP Rapid Response Assessment, United Nations Environment Programme, Nairobi, Kenya, www.unep.org/unea/docs/RRAcrimecrisis.pdf, accessed September 2015

United Nations Security Council (2012), *First report of the analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities*, S/2012/683, 5 September 2012, United Nations Security Council, New York, United States, www.un.org/Docs/journal/asp/ws.asp?m=S/2012/683

US Department of Treasury (2015), *United States National Terrorist financing risk assessment*, US Department of Treasury, Washington, United States, www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf, accessed September 2015

US Department of State (2015), *Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*, US Department of State, Washington, www.state.gov/e/eb/rls/othr/2015/242414.htm, accessed September 2015

www.fatf-gafi.org

October 2015

Emerging Terrorist Financing Risks

This report, the result of the call for further research into terrorist financing, provides an overview of the various financing mechanisms and financial management practices used by terrorists and terrorist organisations. It explores the emerging terrorist financing threats and vulnerabilities posed by foreign terrorist fighters (FTFs), fundraising through social media, new payment products and services, and the exploitation of natural resources.