Report

Date
18 December, 2015
FHS/CATS

SEDU designation
46/2015

Understanding Terrorist Finance

Modus Operandi and National CTF-Regimes

Magnus Normark and Magnus Ranstorp

Content

"Funding is both the lifeblood of a terrorist organisation and one of its most significant vulnerabilities."[1]

Introduction

The fight against terrorism within the European Union (EU) has taken on a new urgency in the wake of the catastrophic terrorist attacks in Paris on 13 November 2015 when a series of coordinated attacks was launched by Islamic State foreign fighters against restaurants, Stade de France, and Bataclan theatre. 130 were killed and over 360 injured. At a meeting between the EU finance ministers in Brussels on 8 December a broad agreement was made to step up the fight against terrorist financing. Based on a French initiative, the ministers agreed to develop capacity to track and freeze terrorist funding and to make it an immediate top priority.

Building a capability to commit acts of terrorism is contingent on some level of financial means. Without funding, any effort to commit terrorism acts with serious and deadly outcome would be difficult. Past events has shown that while terrorist events can be carried out with limited financial means, fund-generating activities and transfers always leaves footprints for law enforcement and intelligence agencies to track. For this reason, building the capability to prevent, detect and respond to financial activities with the purpose to support terrorism has become a core issue for governments around the world.

This report is the result of a study on Countering Terrorist Financing (CTF) that Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University (SEDU) has conducted during 2015. The study was commissioned by the Swedish Financial Supervisory Authority (FI).

The purpose of this study is to contribute to better insight and knowledge of Terrorist Financing on two essential but different dimensions: (1) contribute to a better understanding of how funds are generated and moved for terrorist purposes, and (2) provide a perspective on key functions of a Countering Terrorist Financing regime, based on an overview of the British and Canadian CTF-regimes.

This report provides an overview of different ways terrorist plots, attacks and terrorist-related activities have been funded and the financial signatures such activities create that may be of relevance for law enforcement, intelligence agencies, regulatory authorities as well as financial institutions. Based on extensive interviews and official documents the report furthermore provide a brief description of existing Counter Terrorist Financing regimes and the key factors that may be of value for Swedish policy makers and the continued efforts to

[1]Quote by: Dennis M. Lormel (former 9/11 Chief of the FBI's Counter-Terrorist Financing Operations Section) from Tom Garry "Would the 9/11 Hijackers' Money Trail Raise Red Flags in Today's System?", *Foreign Policy Association,* September 6, 2013. http://foreignpolicyblogs.com/2013/09/06/would-the-911-hijackers-money-trail-raise-red-flags-in-todays-system/

develop a national capacity to fight terrorist financing in line with the new Swedish counter-terrorism (CT) strategy.

Limitations

This report examines terrorist finance modus operandi and national systems and regimes in order to understand new insights and knowledge as a frame of reference when Sweden develops more effective measures and cooperation when it comes to terrorist finance.

There are a few limitations to the study which are worthwhile to mention. While the focus on modus operandi has been broad-based, it has taken into consideration most but not all terrorist finance literature. There are few studies on foreign terrorist fighter finance so this is an effort to collate the various fragments of information to provide broad insight into the ways and means terrorist groups (with special focus on salafi-jihadist) generate funds and move them across national borders through a wide variety of ways.

This report is also focused on the lessons learned from the national system and regime of countering terrorist finance in the United Kingdom and Canada, which have some of the most developed thinking and experience about these issues. There are other national regimes that can provide valuable insights but due to time and resource constraints this study has limited the perspectives to the experience of the two aforementioned countries. Similarly, this study has not focused specifically on the Swedish CTF experience or context though there were several discussions throughout the process with relevant Swedish agencies and financial institutions.

This study should not be considered an academic report but rather an exploratory report that highlights trends and lessons learned in relation to counter terrorist finance issues. Its main contribution is to raise the knowledge base about terrorist finance modus operandi issues and relevant national systems and regimes.

Method

This report is a qualitative study based on review of available literature on terrorist finance issues and extensive interviews with relevant officials from law enforcement and intelligence communities working specifically with terrorist finance issues; representatives from the finance regulatory authorities and the financial sector. It also involves an interview with non-governmental organizations (NGOs) working with the impact of terrorist finance on nonprofit organisations. The following national agencies, think-tanks, financial institutions and NGO were interviewed for this study:

- National Terrorist Financing Investigation Unit – NTFIU, Metropolitan Police (SO15), London
- Standard Chartered Bank, High Risk Client ID, London
- Royal United Services Institute - RUSI, Financial Crime and Security Studies, London
- National Coordinator for Counterterrorism (NCTV), The Hague

- Israel Money Laundering and Terror Financing Prohibition Authority (IMPA), Tel Aviv
- US Treasury Department
- Financial Crimes Enforcement Network - FinCEN (US FIU)
- US Justice Department
- US State Department Office of Counterterrorism
- Canada Security and Intelligence Service (CSIS)
- Royal Canadian Mounted Police (RCMP)
- Public Safety Canada (PSC)
- Financial Transactions and Reports Analysis Centre of Canada - FINTRAC (CAN FIU)
- Europol, Counter Terrorism and Financial Intelligence, The Hague
- Human Security Collective, The Hague
- Swedish Security Service
- Swedish Finance Police
- Swedish Financial Supervisory Authority
- Handelsbanken
- SEB
- Nordea
- Swedbank
- Danish Broadcast Corporation
- Danish Security & Intelligence Services

This study has taken into consideration the trends of terrorist finance as outlined by the report of the Analytical Support and Sanctions Monitoring Team, prepared pursuant to paragraph 23 of Security Council resolution 2178 (2014), on the threat posed by foreign terrorist fighters (FTFs).[2] It has also examined Financial Action Task Force reports on various terrorist finance issues.

[2] Letter dated 19 May 2015 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning al-Qaeda and associated individuals and entities addressed to the President of the Security Council

Terrorist financing *modus operandi*

Terrorists use multiple methods for moving funds and these are usually either through cash couriers, informal transfer systems (e.g. *hawala*), money service businesses, formal banking, false trade invoicing, and high value commodities. Detecting terrorist financial transactions is a crucial counter-terrorism activity. Through network and transaction analysis it can illuminate the size of a terrorist network, its entire life-support system and the quality of its connections.

The detection of terrorist financial transactions is extremely difficult as there is an entire spectrum of financial flows extending from legitimate businesses (e.g. mobile phone companies, remittances, real estate and donations to charitable businesses) to illegal activities such as counterfeit goods, drug trafficking, financial fraud and even trade in certain precious commodities. Moving terrorist funds covers a broad spectrum from wire transfers to bulk cash transfers, regulated and unregulated alternate remittance systems. The often small amounts involved make it almost impossible to detect.

Understanding terrorist finance sources in Europe

Terrorist groups are all different. Modern terrorist networks are comprised of loosely connected transnational webs of autonomous cells. Some are formed around social circles, friendship or family connections. Some are solo terrorists who emerge for idiosyncratic personal and ideological reasons. Other larger terrorist groups exist that are embedded within larger communities where they emerge from time-to-time to strike against the oppressive state or local enemies. Almost all terrorist groups have significant transnational linkages with dynamic flows of ideas, arms and money.

Terrorist organisations and their activities revolve around five core dimensions: operations; propaganda and recruitment; training; salaries; and provision of social services. Groups differ significantly as to their capabilities and focus. It is, however, clear that terrorist activities do not require substantial funding and is often generated through a combination of legal and illicit means.

Very few studies exist that provides detailed accounts of terrorist finance methods in terrorist operations within Europe. Most of these studies focus on paramilitary groups in Northern Ireland or Euskadi ta Askatasuna (ETA) in the Basque areas. For example, there are several studies on the Provisional Irish Republican Army (PIRA) that have unpacked and outlined their financial operations, extending from kidnapping for ransom, extortion, and armed robbery to drug-dealing.

The PIRA illicit financial schemes are quite sophisticated involving video piracy, counterfeiting tax-exemption certificates, income tax frauds, counterfeiting currency, and extortion, fuel smuggling, protection rackets, Value Added Tax (VAT) fraud and other imaginative schemes. The embedded nature of PIRA working within their constituent community makes accounting for their financial activities very difficult. The Police Service in Northern Ireland (PSNI) estimates that PIRA fund-raising capacity is around $7-10 million which is spent on weapons, munitions, training, salaries, payments to support network material supporters and welfare payments to the families of jailed PIRA members.

Additionally, PIRA finance the activities of its political wing, Sinn Féin which includes salaries, campaigns and general costs.

The Basque ETA group mirrors much of the PIRA financial activity, focusing on racketeering, kidnapping and extortion, looting, subventions to political parties, press, businesses, and relatives of imprisoned ETA members. In total, it is estimated that the network surrounding ETA "managed at least € 28.1 million a year between 1993 and 2002" but it have been reduced to around € 8.8 million per year.[3] ETA's legal and illicit financial flows are incredibly complex and integrated in the rest of the financial system and the local economy.

Terrorist groups operate closely with elements within diaspora communities in the West to generate funding. It is important to recognize that informal transfers of funds through remittances from the diaspora are essential for the survival of e.g. the Somali community. Many Somalis are often dependent on relatives abroad who send home about $1.3bn annually.[4] There is, however, evidence that al-Shabaab has exploited the remittance system, or *hawala*, to generate funding either through cash couriers or appropriation of funds through *hawala* as a tax. While this abuse represents a miniscule proportion of all Somali remittances, it is crucial that there is a possibility for transfer of genuine remittances as they constitute a vital humanitarian lifeline for Somalis.[5]

Closure of genuine possibilities to transfer remittances will drive money transfers underground and will heavily punish the entire Somali community. At the same time, it is important for the banking sector to recognize that it cannot guarantee wire transfers will not reach al-Shabaab as it "is known to steal from local citizens, impose taxes on humanitarian aid, kidnap victims for ransoms, and otherwise terrorize those who live in the territory the group controls across the country."[6] Given that Kenya remains the largest Somali expat and refugee community in the world it becomes important to monitor transfer of remittances, especially Eastleigh is a financial hub for remittances abroad. Al-Shabaab's recent bombing campaign in Kenya resulted in its members being forced underground and its popular support declined in Nairobi and in Eastleigh.[7]

Other terrorist organisations remain actively involved with their diaspora communities where they fund-raise for terrorist-related support. They do so either through coercion or voluntary contributions. The Sri Lankan Liberation Tigers of Tamil Eelam (LTTE) have focused extensively on the Tamil community living in the West as significant source of financial and political support for its struggle to establish an independent state, "Tamil Eelam," for the Tamil minority in North and East Sri Lanka. Human rights organisations have reported that LTTE have

---

[3] Mikel Buesa and Thomas Baumert, *Dismantling Terrorist's Economics: The Case of ETA,* (Madrid: Universidad Complutense de Madrid – Instituto de Análisis Industrial y Financiero, 2012).
[4] "Life after losing remittances: Somalis share their stories", *The Guardian,* June 18, 2015.
[5] Jamila Trindle, "Transfer Denied: The Hidden Costs of Washington's War With al-Shabaab" *Foreign Policy,* February 26, 2015.
[6] Ibid.
[7] Walter Vilkko, Al-Shabaab: From External Support to Internal Extraction A Minor Field Study on the Financial Support from the Somali Diaspora to al-Shabaab (Uppsala University, March 2011).

pursued an extensive campaign of intimidation and violence against the Tamil community in the diaspora to support the LTTE with financial contributions. Through an extensive fundraising campaign, LTTE would force businesses to pay significant contributions to their cause (up to $75,000) and families and individuals would normally pay $2,000-3,700. There is evidence that this practice occurred in the United Kingdom, France and Norway.[8] While the LTTE has been largely inactive since the death of its leader Velupillai Prabhakaran in May of 2009, it highlights the importance of voluntary or coerced fund-raising activities within diaspora communities by terrorist groups.

The Lebanese Hizballah organisation is also active in the diaspora communities using a global complex web of charities and front organisations to raise funds. Most of these activities are based where wealthy Shiites live in West Africa, sub-Saharan Africa, South America and elsewhere and contribute with fund-raising activities, ranging from diamonds, cigarette-smuggling, counterfeit goods, counterfeit drugs, import-export scams, and other illicit activities.[9]

While most of these activities are mainly outside Europe there are also some suspected front organisations which provide funding for Hizballah. Some have argued that Hizballah developed a "sophisticated, organized, and global crime network"[10] involved in multiple crime schemes and drug-smuggling operations with extensive money-laundering capabilities with a number of Lebanese banks.[11] In parallel in Europe, Hizballah has established a complex web of illicit networks to procure weapons, raise funds, and launder money for the group's activities in Lebanon.[12]

Outside the role of terrorist groups, who exploit remittance systems and fund-raising through their diaspora communities, there are loosely autonomous terrorist networks affiliated with al-Qaeda and other militant Islamist groups. Most of these terrorist groups operate on mission-demand and operational costs, generating funding through a wide variety of financial activities, ranging from charity contributions, donations, credit card fraud, and bank fraud, to more complex self-financing schemes such as document forgery, welfare fraud, robberies, etc.

There is, however, a significant risk of terrorist finance transfer of funds between so-called parent-groups and their affiliated satellites. For example, the Islamic State of Iraq and the Levant (ISIL) and associated pledges of allegiances from terrorist groups in different geographical locations increase the risk of cross-transactions between terrorist groups. This is a major risk as ISIL maintain close

---

[8] Human Rights Watch, "Funding the "Final War" LTTE Intimidation and Extortion in the Tamil Diaspora", Vol.18, No.1.
[9] Matthew Levitt, "Hezbollah Finances: Funding the Party of God", The Washington Institute for Near East Policy, (February 2005). http://www.washingtoninstitute.org/policy-analysis/view/hezbollah-finances-funding-the-party-of-god
[10] Matthew Levitt, "Hezbollah: Party of Fraud", *Foreign Affairs,* July 27, 2011.
[11] *Ibid.* Lebanese-Canada Bank and LCB are mentioned.
[12] Matthew Levitt, *Hezbollah: The Global Footprint of Lebanon's Party of God* (Georgetown University Press, 2013)

interaction with its *wiliyats* (or provinces) established in Libya, Yemen, Sinai, and Khorasan (Afghanistan). There are, already, indications that these satellite affiliated groups are searching for ways to provide financial support to ISIL.[13] It is also difficult to target as ISIL have such diversified portfolio of funding sources, ranging from oil, taxation/extortion, kidnappings, sale of antiquities, Iraqi banks, looted property, real estate, individual contributions from foreign fighters, agriculture, natural resources, human trafficking, etc.[14]

Financing of terrorist attacks and planned attacks in Europe

Few studies exist providing a high-resolution picture of the sources of funding for terrorist plots. One exception is by the Norwegian Defence Research Establishment (FFI) which has analysed the financing of 40 jihadi cells that plotted in Europe between 1993 and 2013.[15] The study revealed some interesting conclusions which challenge some common assumptions about terrorist finance methods. Four main observations stood out from the case-studies:

Firstly, salaries and savings of terrorist members were the most common source of income. At least 73% of the terror cells had acquired part of their financing from legitimate means. There was often a combination of different funding sources, few cases involved single-source funding.

Secondly, 38% of the cases involved criminal activities to raise money. Funding from international terrorist networks only figured in 25% of the cases. Larger cells and cells with foreign fighters were more connected to and supported by international terrorist networks. At least 47% of the cells were entirely self-financed and in 90% of the cases there was a significant portion of self-financing activities. These self-financing cells were more likely to carry out attacks than those provided with external support. This fact could be accounted for partially by the terrorist cell detection rate by the security services.

Thirdly, there was no evidence of *hawahla*-transfers to jihadis. There was also very limited evidence that Islamic charities provided funding for terrorist purposes, only two cases emerged. Most of the financial transfers occurred through cash, money services providers and formal bank transfers.

Fourthly, most of the plots were relatively inexpensive, 76% of the terror plots cost less than $10,000.

The limited amounts involved makes detection difficult. As the study's author concluded: terror financing in these 40 cases show that terrorists' financial activity is "remarkably ordinary." With exception of acquiring weapons and bomb-making ingredients, there is little that stands out in terrorist cells financial activities. There was also little evidence that terrorists used the Internet in any way as a useful

---

[13] Mirwas Adeel, "ISIS affiliates in Afghanistan seeking financial help to rise: Ulomi", June 13, 2015.
[14] Ana Swanson, "How the Islamic State Makes Its Money", *Washington Post,* November 18, 2015.
[15] Emilie Oftedal, *The financing of jihadi terrorist cells in Europe* (Forsvarets Forskningsinstitutt, 2014). FFI-rapport 2014/02234. The discussion in this section is drawn from this study.

fund-raising platform, moving funds around through virtual currencies or fraud schemes. In many ways, the January 2015 Charlie Hebdo and the Kosher store attack in Paris confirm the small amount of money involved in operations: "a 6,000 euro consumer loan, obtained with forged documents and cashed out; the proceeds of the overseas sale of a used car; and cash transfers linked to the sale of counterfeit goods."[16]

As technologies rapidly advance it is probably only a matter of time before terrorists begin to use social media and the Internet as they are using it now in terms of communication with encryption and other creative means.

Financing of Jihadist Plots in Scandinavia

There have been a number of jihadi terrorist plots in Scandinavia since 2001 that provides some insight into the modus operandi of terrorist financing.

Case of Abdullah/Berzengi

In 2006, Ferman Abdullah and Ali Berzengi were convicted for terrorist finance offences in Sweden and sentenced to several years in prison. Abdullah was sentenced to 4 ½ years in prison for preparation of a terrorist crime and for having collected and sent a total of SEK1,3 million to Iraq during seven different occasions. Ali Berzengi was sentenced to 5 years in prison.

Ferman Abdullah owned a falafel stall in Malmö from which he engaged in a hawala or remittance activity to northern Kurdistan. Ali Bergenzi assisted Abdullah in collection of money for suffering Muslims in Afghanistan, Palestina and Chechnya.[17] On 1 February 2004, two suicide-bombers launched attacks against the Kurdish party headquarters in Arbil in which over 100 were killed and 200 injured.

Intelligence services believed that both men were acting as financial bridgehead between the al-Qaeda-related Ansar al-Islam group in Norway and Sweden and Abu Musab al-Zarqawi. Both men engaged in extensive collection activity around mosques in Sweden and spoke in code back to Arbil both in terms of the bomb issue and in discussions of money transfers. Police found a code-book for mujahidin. This remains the only conviction for financing terrorism in Sweden.

Case of Taimour Abdulwahab al-Abdaly

Taimour Abdulwahab al-Abdaly died in a suicide-bomb operation in central Stockholm on December 11, 2010, after he accidentally detonated one of his explosive devices. He carried significant explosives on him in two backpacks on his back and stomach which contained six serially-connected pipe bombs wrapped with nails. Additionally, he had constructed a car bomb which contained gas canisters and pyrotechnics which burnt but did not explode.[18]

---

[16] " Emerging terrorist financing risks", http://www.moneylaunderingbulletin.com/terroristfinancing/emerging-terrorist-financing-risks--1.htm

[17] "Kiosken var en terrorbank", *Sydsvenskan,* February 26, 2006. http://www.sydsvenskan.se/sverige/kiosken-var-en-terrorbank/

[18] Magnus Ranstorp, "Terrorist Awakening in Sweden?", *CTC Sentinel,* January 2011.

While living in Luton in the United Kingdom, Taimour Abdelwahab al-Abdaly, financed his operation from a multitude of sources. It was partially financed through Centrala studiestödsnämnden (CSN) – a Swedish study loan scheme from which Taimour received SEK745,000 for his studies in the United Kingdom.[19] Taimour completed a degree in Sports Therapy in 2004. Later on, between 2008-2010, he managed to forge university documents pretending to study medical science. This enabled him to claim SEK450,000 fraudulently.[20]

Another source of finance for Taimour Abdelwahab al-Abdaly was provided by a financier, Nesserdine Menni, in Scotland. Menni was arrested and convicted for having provided terrorism funds to Taimour and had made bank transfers of just below £5,000.

Case of four Swedes and Jyllands-Posten

On December 29, 2010, four Swedes were arrested in Copenhagen for having plotted an armed attack against the newspaper Jyllands-Posten which published the Muhammed cartoons in 2005. The four Swedes had driven to Copenhagen from Stockholm, and in a joint Swedish-Danish operation they were arrested as they were planning to launch the attack against the newspaper. The plan was to storm Jyllands-Posten and kill as many as possible in a Mumbai-style attack. The terrorists were arrested with a submachine gun, 9 mm cartridges and over 200 plastic strips to be used as handcuffs. They were convicted to 12 years in prison for the terrorist plotting.

The financing of the Jyllands-Posten plot was complex and from multiple sources. As one of the ringleaders, Mounir Dhahri, spent time in a terrorist training camp between 2008 and 2010, there are strands to the financing of this terror cell that is still unknown. What is evident is that most of the funding came from personal sources. When Dharhi left Sweden in 2008 for terrorist training in Waziristan he was given SEK45,000 ($5,850) by Sahbi Zalouti, another cell member. Zalouti would later wire SEK10,000 to Dhahri in Pakistan through Western Union. When the entire terrorist cell was arrested the authorities found $20,000 in 100-dollar notes. It is, however, estimated that the cost of the operation was around $10,000 with Dhrari's Pakistan visit being the most expensive.[21]

Case of Breivik's Financing of Terror

The financial activities of Anders Behring Breivik (ABB) provide interesting insights about fundraising for terrorism. It also shows different pathways for concealment of funds and in the acquisition of the weaponry used in the terrorist attacks.

In parallel to his employment at the advertisement firm Direkte Response (1997-2003), ABB established a number of firms that were largely unsuccessful and went into receivership. In December 2002, ABB established an Internet-based

---

[19] "Självmordsbombaren fick 750.000 från CSN", *Dagens Nyheter,* February 18, 2013.
[20] "Självmordsbombaren fick 450.000 med falska studieintyg" *Dagens Nyheter,* February 19, 2013.
[21] Emilie Oftedal, *The financing of jihadi terrorist cells in Europe* (Forsvarets Forskningsinstitutt, 2014). FFI-rapport 2014/02234.

company called Diplomaservice, which generated fake American university institutional letters for non-U.S. citizens. These forged institutional letters were manufactured by different individuals around the world including an Indonesian student. Each fake institutional letter cost $280-450.[22]

In January 2005, ABB also established the company E-Commerce Group A/S. This company employed two individuals full-time with offices in central Oslo. An elaborate money laundering scheme begun in which ABB, in mid-2004, established another company, Brentwood Solutions Ltd., based in Antigua. The proceeds of sales of credentials were deposited in an account belonging to Brentwood Solutions Ltd. and then transferred to E-Commerce for services rendered. According to the police investigation, ABB received payment of NOK 3,697,588 between the period 2002-2006.[23] After 2006, E-Commerce became inactive and was dissolved in 2008.

ABB generated a significant stock portfolio from some of these proceeds and made 350 trades in his own or in his company's name. Between 2007 and 2009 he sold stocks to a value of NOK1,1 million in over 60 transactions.[24] Significant preparation for acquiring explosives was the reason for establishing, in May 2009, the company ABB called Geofarm, which was reconstituted as A Geofarm in March 2011. As part of this scheme he applied to nine different credit card companies for ten different cards totalling NOK 235,000 which he did not use until April 2011. These cards were used between April and July 2011 and only NOK 27,618 was left.[25]

The amount of purchases provides insight into the operational security of the mission. Police uniform badges were purchased from 11 retailers in five countries; the police uniform from 36 retailers in eight countries and 22 purchases of weapons/ammunition from 14 retailers in four countries. Finally, the 950kg bomb consisted of 43 purchases from 36 retailers in five countries.[26] The total cost of the entire terrorist operation was NOK 389,020. According to the 22 July Commission it is unlikely that ABB would have had enough funds to complete the bomb had it not been for his credit cards.

The Norwegian Police Security Service (PST) issued a report stating that they would not have managed to detect ABB following their routines as he planned the operation over several years and was exceptionally security conscious knowing how to avoid detection.[27]

---

[22] *Rapport fra 22. Juli-kommisjonen* (Norges offentlige utredninger, 2012:4).
[23] "Her er hele dommen mot Anders Behring Breivik", *Aftenposten,* August 24, 2012. http://www.aftenposten.no/nyheter/iriks/Her-er-hele-dommen-mot-Anders-Behring-Breivik-6973988.html
[24] *Rapport fra 22. Juli-kommisjonen* (Norges offentlige utredninger, 2012:4).
[25] Ibid.
[26] Ibid.
[27] Randi Johannessen, Vibeke Buan, Andreas Bakke Foss, "PST: - Vi kunne ikke avslørt Breivik før 22. Juli", *Aftenposten,* March 16, 2012.

Support to Terrorist Groups and Related Activities

Generating funds

Legal fund-raising activities

Humanitarian
Charitable contributions are an integral part of Muslim solidarity and a core pillar of the Muslim faith. There are different types of charities and humanitarian aid organisations operating which sometimes come into contact with terrorist finance issues. This charity sector is sometimes abused by terrorists in order to fund-raise – often from unsuspecting communities who do not know where their contributions end up.

The complexity of the crisis in Syria and the huge need for humanitarian assistance makes the issue of detection of terrorist finance extremely sensitive and difficult. The physical absence of international aid agencies (the United Nations (UN), the International Committee of the Red Cross (ICRC) and international NGOs) inside Syria have meant that the vacuum has been filled by 600-700 local groups in the region since 2011.[28] About a fifth of them are active inside Syria.

Access to ISIL territory is perilous, dangerous and negotiated. ISIL seem to operate under the principle that distribution of aid can serve its cause as it seeks to consolidate its state-building and control of the almost 4 million people living under "Caliphate" rule. A limited number of aid agencies operate under strict ISIL supervision as long as the aid is distributed under ISIL credit (IS Department of Relief) and no international staff is present.[29]

A 2014 Financial Action Task Force (FATF) report found that NPOs (non-profit organisations) most at risk being "those engaged in 'service' activities which are operating in close proximity to an active terrorist threat" and those "that send funds to counterpart or 'correspondent' NPOs located in or close to where terrorists operate".[30]

There are several examples of terrorist abuse of humanitarian NPOs. For example, in the United Kingdom there have been multiple cases of connections between terrorists and charities.[31] In one of these cases, three men were "convicted of terrorism offences in the UK fraudulently posed as volunteers for Muslim Aid, one of the largest British Muslim NGOs, collecting up to £14,000 from the public."[32] In the Netherlands authorities have not found concrete proof of

---

[28] Nicholas Crawford, *Engaging with Syrian CSOs* (30 April 2015).
[29] The IRIN/HPG Crisis Brief, "Aid and the Islamic State" December 2014.
[30] Financial Action Task Force, *Emerging Terrorist Financing Risks* (October 2015): p.14.
[31] For multiple examples, see: Andrew Gilligian, "'Terror link' charities get British millions in Gift Aid", *Daily Telegraph,* November 29, 2014. For example, UK authorities have frozen £117,000 across 80 accounts of those designated under the UK's domestic TAFA regime, the UN AQ regime and the EU CP931 regime (as of 31 Dec 2014) See: HM Treasury/HM Home Office, *UK national risk assessment of money laundering and terrorist financing* (October 2015) .
[32] "Banks block charity donations over terrorism funding fears", *The Guardian,* March 5, 2015.

charities being abused but they have found that FTFs operate in the periphery of these charities and have transferred large bulks of cash to Syria.[33] In France, authorities recently charged two individuals for collecting €60,000-100,000 for terrorists in Syria and Iraq with the charity Pearl of Hope.[34] Their social media accounts provided pictures that provided the clues that they were diverting funds to terrorists.

As the UK Charity Commission's chairman William Shawcross has stressed "terrorist abuse is one of the greatest risks facing the charitable sector today"[35] as it seriously undermine public confidence in providing humanitarian aid. However, as noted recently by UK authorities, de-risking by withdrawing bank services to charities may mean "charitable funds may go underground, increasingly transacted in cash, or moved off-shore via cash couriers or alternative remittance systems."[36]

Private donations

Among the most common methods of Muslim individual contribution is *'Tajheez Al-Ghazi,'* which means "preparation" *(Tajheez)* and "warrior" *(al-ghazi).* Essentially, it is a mechanism for those that cannot or will not join jihad physically in which they can achieve personal honour and reward by contributing to jihad by proxy. This is a very common method of "sponsorship" for jihadi FTFs around the world. Research has shown that *tajheez* cost $300-400 per jihadi during the Bosnian conflict and $200 per jihadi travelling to Afghanistan, whereas the Chechnya conflict with few foreign jihadis cost as much as $15,000 per jihadi.[37]

This principle of *tahjeez* have created a complex web of sponsorship stretching everywhere without a central hub or connector which makes it difficult to pinpoint and counter. Funds can be distributed via humanitarian channels or be as simple as buying someone's airline ticket or sponsor a piece of equipment.

Some of the most important donors for ISIL are *sadaqa* (voluntary donations) from Arab donors in the Gulf. These private funders come from Saudi Arabia, Qatar, fundraisers from Kuwait, United Arab Emirates (UAE) and donations from ISIL theatres abroad (Indonesia, Afghanistan etc.).[38] Often Saudi funding is channelled through Kuwaiti facilitators to avoid "blowback." These donations are both from very wealthy benefactors as well as private citizens.

---

[33] Financial Action Task Force, Emerging Terrorist Financing Risks (October 2015): p.15.
[34] Dan Bilefsky, "Charity in France Is Accused of Being a Front for Financing Terrorism in Syria", *New York Times,* December 4, 2014.
[35] Andrew Gilligan, ""'Terror link' charities get British millions in Gift Aid", Daily Telegraph, November 29, 2014.
[36] HM Treasury/HM Home Office, UK national risk assessment of money laundering and terrorist financing (October 2015)
[37] Aimen Dean, Edwina Thompson, & Tom Keatinge, "Draining the Ocean to Catch one Type of Fish: Evaluating the Effectiveness of the Global Counter-Terrorism Financing Regime", *Perspectives on Terrorism,* Vol 7, No 4 (2013).
http://www.terrorismanalysts.com/pt/index.php/pot/article/view/282/html
[38] "Islamist Insurgency Fueled by Global Finance Web", *VOA,* July 7, 2014.

Another way to receive individual donations is through fund-raising websites where one can individually contribute to different charities. For example, the Hizballah provides an array of fund-raising pathways on the Internet to its charitable activities around the world.[39]

Student loans

As demonstrated by the case of Taimour Abdelwahab al-Abdaly, the suicide-bomber in Stockholm in 2010, student loans can be used for terrorist finance purposes. These types of student loans are easily obtained both legitimately and fraudulently. Often they originate with fake certificates. They have also proven a convenient way to finance FTFs travel to Syria. In the United Kingdom, it is possible to get up to £8,000 loan to cover living expenses while at university.

In February 2015, a 19-year old British man used a forged Business and Technology Education Council (BTEC) certificate to gain a university place at Middlesex University for which he received student loans and educational grants. These student loans were then used to purchase five flights for himself and four friends to Morocco costing £906.[40] They then continued on separate flights to Turkey and Gaziantep where the four friends continued into Syria while the 19-year old was persuaded by his father to travel to British consulate in Istanbul instead where he was arrested by British police. He was subsequently convicted and sentenced to five years in a youth offenders' institution for the terrorism offences and four months for an offence of fraud by deception.[41]

Loans

Many FTFs have borrowed money from banks (or via Internet applications) and many of these loans are made without any intentions of paying them back. In Sweden there are several cases where FTFs take out unsecured bank loans in combination with other types such as quick loans (SMS-loans) and/or leasing of SUVs and other cars.[42]

In the United Kingdom, there are so-called payday loans which offer deposit of £2,500 in applicants account within 15-20 min. As pointed out by financial experts, payday loans were involved in the fund-raising scheme for a large-scale suicide-attack in the United Kingdom in 2012 when four men unsuccessfully tried to borrow money from payday loan institutions and banks. One applied online for £20,000 from Yes Loans, pretending to be self-employed, as well as for a £18,000

---

[39] http://www.shariahfinancewatch.org/blog/2008/05/29/funding-terrorism-hezbollah-uses-its-websites-to-collect-donations-for-itself/

[40] Sophie Hane Evans, "London teenager used his student loan to fly himself and four friends to join ISIS in Syria and duped airport police by claiming they were travelling to find love", *Daily Mail,* November 13, 2015.
Read more: http://www.dailymail.co.uk/news/article-3317389/London-teenager-used-student-loan-fly-four-friends-join-ISIS-Syria-duped-airport-police-claiming-travelling-love.html#ixzz3twbSNiQC
Follow us: @MailOnline on Twitter | DailyMail on Facebook

[41] "Teenager who used student loan to join Isis in Syria gets youth custody", *The Guardian,* November 18, 2015.

[42] "Lån och bedrägerier finansierar terrorresor", *Sveriges Radio,* June 22, 2015.

loan from Barclays, while another cell member applied for a £15,000 from another branch of the same bank.[43]

The head of the Royal United Services Institute's (RUSI) Centre for Financial Crime and Security Studies have suggested that a solution to these payday loans and student loans is the idea that "funds could be provided via prepaid cards with restrictions attached that allow them only to be used in certain shops, to pay for pre-agreed services, or settle registered bills."[44]

There are also other types of bank frauds. In the United Kingdom, the Metropolitan Police unravelled a large-scale fraud by British FTFs in March 2015 who pretended to be police officers targeting elderly people to hand over their bank details as they were told their bank accounts had been compromised. Instead they were instructed to transfer money to an account under the control of the fraudsters.[45]

Illicit activities

VAT- and business-fraud

The issue of withholding VAT-payment is a very common and lucrative method for terrorist financing. Very large sums can be generated specifically in consumer goods that are easily resold. In Sweden, a thirty-year-old salafi preacher, influential with FTFs, was charged with VAT-fraud amounting to SEK 6 million in a scheme lasting four months in the first quarter of 2013. Having purchased mobile phones and tablets for SEK 29,7 million in the United Kingdom, the shipment went via his company in Finland and was resold to a 23-year-old Swedish FTF and his company in Bergsjön.[46] SEK 5 million is either believed to be missing, believed to be in the Middle East or North Africa. These kinds of VAT-carousels where phones are sold and resold to different companies create profitable margins of criminal proceeds. In business jargon, these so-called "missing traders" receive a VAT-number and then trade before dissolving their companies.[47]

Another case of VAT-fraud occurred in Denmark with Abdessamad Fateh, also known as Abu Hamzah, who was officially designated by the U.S. as a foreign terrorist fighter and "a member of a Scandinavia-based network of extremists allegedly linked to al-Qa'ida, and has travelled to Syria."[48] Abu Hamza had been previously arrested as a suspect in a terror plot against the cartoonist Kurt Westergaard at Jyllands-Posten in 2008. He owned a company importing large

---

[43] "Would be suicide bombers tried to fund terror plot with payday loans", *Evening Standard,* October 24, 2012.
[44] Tom Keatinge, "Terror on the Cheap: Financing Lone Actor and Small Cell Attacks" August 18, 2015. http://www.cfcs.london/the-41st-recommendation/terror-on-the-cheap-financing-lone-actor-and-small-cell-attacks/
[45] Jonathan Owen, "British pensioners targeted in scam by extremists raising funds for Isis", *The Independent,* March 5, 2015.
[46] "Momsfiffel finansierade jihadister I Syrien", November 28, 2004.
[47] "Julhandeln högtid för kriminellas momsfiffel", *Dagens Nyheter,* December 3, 2014.
[48] http://www.state.gov/r/pa/prs/ps/2014/09/232067.htm

quantities of chicken breast and cheese from Germany to Denmark and failed to pay DKK 3 million VAT in a scheme where accountants acted as facilitators through a series of shell-companies, including a travel agency, which were created and dissolved.[49]

VAT-fraud can also assume massive proportions. In 2014, Italian authorities discovered that so-called carbon-credit and VAT-fraud occurred between 38 middlemen who sold carbon-credit between Italian SF Energy and a series of companies in Denmark, Germany, the Netherlands, and the United Kingdom. This €1.15 billion tax scam, involving the trade of carbon credits, diverted to fund the Taliban via bank transactions in Cyprus, Hong Kong, and UAE.[50]

Often these VAT-fraud schemes involve fake addresses or designated 'fall-guys' who takes the legal and financial costs. This enables the real culprits to continue the scheme elsewhere.

Lease/Loans of SUVs and cars

One of the most common practices is to secure a car loan or leasing options with no intention of paying back the loan. Often these cars are larger SUVs. For example, Toyota Hilux pickups and Toyota Land Cruisers have become permanent fixtures in videos of the ISIL campaign in Iraq, Syria and Libya. In fact, a majority of the vehicles paraded in Raqqa are white Toyotas with the black emblems. Toyota Hilux pickups have a reputation for being indestructible and have become ubiquitous with insurgents in conflict zones. It is rear wheel drive, manoeuvrable and light-weight, desert-friendly, and requires basically no maintenance. Often they choose twin-cab model as it provides storage possibilities while it allows retrofitting heavy calibre weapons on the back of the pickup.[51] There are also a small number of other brands including Mitsubishi, Hyundai and Isuzu being used by ISIL.

Toyota Hilux models are being stolen, bought and shipped from around the world to Turkey. There are numerous reported cases as far away as Canada and Australia. In Canada, fraudsters approach dealerships with stolen identities, invoices and credit cards. Then they lease the SUV and make a first month and last month down payment before disappearing.[52] In Europe they are often driven through Europe into Turkey and then into Syria. Turkish border authorities require coupling a driver with a foreign-registered vehicle for each entry/exit into Turkey.

Besides ISIL, the Hizballah has dispatched agents to buy used vehicles from Canada and ship them in containers to Lebanon. There have also been more large-scale schemes. In 2011, a Tulsa-based used car dealership was one of about 30 U.S. car buyers that were part of a money-laundering scheme. In this scheme it

---

[49] Discussions at DR with journalist Troels Kingo Larsen, May 2015.
[50] "Milliardsvindel med dansk kvoteregister er mistænkt for at finansiere terror", *DR,* October 1, 2014. http://www.dr.dk/nyheder/indland/milliardsvindel-med-dansk-kvoteregister-er-mistaenkt-finansiere-terror "Italy tax scam 'may have funded terrorism'", *The Local,* September 24, 2014. http://www.thelocal.it/20140924/1bn-italy-tax-scam-may-have-funded-terrorism
[51] Ravi Somaiya, " Why Rebel Groups Love the Toyota Hilux", *Newsweek,* October 14, 2010.
[52] http://news.nationalpost.com/news/canada/ontario-extortion-racket-has-ties-to-hezbollah

involved sending funds from Lebanon to the U.S. to buy used cars, which were then transported to West Africa. These car sales were orchestrated to mask the proceeds of illegal drug trade. At the centre of this scheme was a Lebanese-Canadian bank which diverted funds to the Hizballah.[53]

Social Insurance Fraud

The issue of social insurance or benefit fraud has been flagged as a method exploited by FTFs in Syria and Iraq. These problems stem from inadequate control systems that are not requiring unemployed individuals to report regularly to authorities. In some EU states the problem has been exposed by inquiries by authorities. For example, an investigation in Denmark revealed that 32 FTFs had collectively received DKK 378.999 in social insurance benefits while they were in Syria fighting for ISIL.[54]

In Britain, a probe has been launched to examine the extent of which British FTFs are abusing the taxpayer social insurance system through false claims, online fraud and student loans. Assistant Commissioner Terri Nicholson, from the Metropolitan Police's counter-terrorism command unit SO15, confirmed that women were being used to smuggle cash derived from benefit fraud as they arouse less suspicion.[55] In July 2015, the Department of Work and Pensions (DWP) Fraud and Error Service launched a wide probe into the extent of these benefit frauds. This was prioritised after three women from Bradford with nine children claimed benefits and had allegedly left for Syria.

In Belgium, the two cities of Antwerp and Vilvoorde decided in August 2013 to stop welfare payments to 29 FTFs as they did not live at their registered address. These FTFs had managed to access their bank accounts via ATMs across the border in Turkey to withdraw their money.[56] The Dutch authorities have decided to freeze the payment of social benefits of 85 FTFs.[57] Meanwhile in France, authorities decided to cut welfare benefits last year for 290 persons identified as jihadists.[58]

Thirteen FTFs were arrested in Austria in November 2014 for collecting welfare payments to fund their trips to Syria.[59] In Spain, five men were arrested for pocketing the welfare payments of a Moroccan immigrant living in the Basque areas who had been killed in Syria in March 2015.[60]

---

[53] " Money Laundering at Lebanese Bank", *The New York Times,* December 13, 2011.
[54] "Syrienkrigere har fået 378.000 kroner i velfærdsydelser", *Ritzau,* May 18, 2015.
[55] Peter Dominiczak, Tom Whitehead and Christopher Hope, "Jihadists funded by welfare benefits, senior police officer warns", *Daily Telegraph,* November 26, 2014.
[56] "Belgian jihadists in Syria stripped of welfare benefits", *France 24,* August 19, 2013.
[57] FATF Report, *Emerging Terrorist Financing Risks* (October 2015).
[58] "France cut welfare benefits for 290 jihadists last year", *France 24*, March 18, 2015.
[59] http://www.oe24.at/oesterreich/chronik/Austro-Jihadisten-kassierten-Sozialhilfe/167065672
[60] "Dos detenidos por el cobro ilegal de ayudas sociales de un yihadista muerto" *ABC.es,* July 4, 2014. http://www.abc.es/espana/20140704/abci-detenido-subvencion-yihadista-201407032148.html

Counterfeit goods

The global counterfeit market is a $500 billion yearly global industry in which terrorist groups operate and make profits. Extensive links have been made between trade in counterfeit goods and terrorist groups such as al-Qaeda, Hizballah, the IRA, ETA and major criminal syndicates. For example, the role of Ciudad del Este in Paraguay as a trading zone among these groups is one example of the globalized nature of this lucrative business. Even Hizballah has been found to trade in counterfeit medicine.[61]

In 2014, Spanish authorities broke up Spain's largest counterfeit clothing ring, leading to the arrest of 99 people, including two imams, for having sold over 235 tonnes of fake designer clothes and shoes. Generating revenues of 5.5 million euros, the counterfeit ring had regional affiliates all over the country.[62] The trade of counterfeit items is lucrative and low-risk compared to other illegal means such as drug-trafficking or drug-dealing which carry with it long prison-sentences.

The counterfeit industry can also be seen as important at the individual terrorist level. Allegedly sales of counterfeit goods by Charlie Hebdo attacker Cherif Kouachi helped partially fund the purchase of weapons.[63]

Transaction methods

The issue of transaction or access to moving funds is important. ISIL relies on access to banking services in Syria and Iraq and in neighbouring areas contested by ISIL. According to one report, "in Iraq alone, approximately ninety such international bank branches continue to operate in contested areas of Ninawa, Salah al-Din, Anbar, and Kirkuk provinces."[64] ISIL is also accessing the government funding of workers which is provided every month in Mosul. However, one of its most important access points to the international financial system is the border region between Turkey and Syria.

Money Service Businesses (MSB)

Money remittance and currency exchange providers have been exploited for money laundering purposes and terrorist finance. Like money-laundering, terrorists use 'sequencing', breaking down amounts into multiple/sequential transactions below the threshold which would require mandatory reporting. They also may employ smurfing or proxy techniques to avoid detection.

MSBs are widely used in Turkey to transfer FTF funds coming from Europe to recipients using MSB offices and ATMs along border towns straddling the Syrian/Turkish border. For example, these can be found in Gaziantep, Akcakale,

---

[61] "Hezbollah and the traffic in counterfeit Captagon", *Jerusalem Post,* June 29, 2015.
[62] "Two imams held as Spain police smash counterfeit clothing ring", *AFP,* January 3, 2014. https://moneyjihad.wordpress.com/2014/01/03/two-imams-arrested-in-bust-of-organized-counterfeit-clothing-ring/
[63] "French police identify potential fourth terror cell member after Paris attacks", *The Guardian,* January 15, 2015.
[64] Matthew Levitt, "Here's how ISIS still has access to the global financial system", *Business Insider,* March 24, 2015.

Adiaman, Hacipasa, Reyhanli, and Sanliurfa where arriving and departing FTF access financial services. The travel is often facilitated and FTFs arrive in pre-determined destinations where they take out funds from MSBs through their home country bank accounts or in cash that is wired. The sources of this funding vary. Some is received by travelling FTFs en route to ISIL; others receive it as a bonus for recruitment of FTFs (usually receiving $600 for each recruit) as well as facilitators who smuggle both prospective FTFs and are cash-couriers for ISIL.[65]

Regular withdrawals of smaller amounts along the border are common. As noted by UK Authorities in a 2015 report: "Funds are typically broken down in to smaller amounts to avoid the need to provide identification and to avoid detection. Intelligence also indicates that employees have been known to facilitate funds to terrorists through their position within MSBs."[66]

It is also important to recognise that FTF facilitators use the MSBs for a variety of purposes. They receive payment for facilitation into ISIL or in the service of ISIL. At times, these facilitators have raised funds through MSBs, even in cases of extraction as they receive funds from worried parents to FTFs.

There have also been large scale transfers of funds to Islamic State FTFs. A major hub for Australian Muslims sending money overseas is the Sydney-based Bisotel Rieh money transfer company which sent $18.8 million to Turkey and Lebanon in 2014 and "routinely failed to provide the ultimate beneficiary details as to these transactions."[67] More importantly, Bisotel Rieh sent more than $200,000 via Dubai to ISIL commander Mohamed Elomar in Syria.[68]

A recent change in ISIL instructions on how to transfer money to MSBs safely was revealed when donations were instructed to be sent via Western Union or MoneyGram, to Turkey or Bosnia. The ISIL instructions further instructed that €5,000 was appropriate for donation and that transferring to Bosnia is safer and provided important contact details for recipients in the Brcko district. This area is a well-known jihadi hotspot as the village of Gornja Maoca contains a concentration of jihadists.[69]

Informal Money Transfer Systems (Hawala)

The traditional system of using *hawala* is in operation around the world. In many cases ISIL financial transactions are conducted through a web of *hawaladar* underground network established throughout Iraq, Syria and beyond. As ISIL is

---

[65] Tom Porter, "Isis commander in Pakistan 'claims Islamic State funding routed through the US'", *International Business Times,* January 28, 2015.
[66] HM Treasury/HM Home Office, UK national risk assessment of money laundering and terrorist financing (October 2015)
[67] Sean Rubinsztein-Dunlop, Bisotel Rieh, money transfer company owned by Khaled Sharrouf's family, may have sent more than $200,000 to Islamic State", *ABC,* October 15, 2014. http://www.abc.net.au/news/2014-10-14/company-owned-by-sharrouf-family-may-have-sent-200000/5813374
[68] Ibid.
[69] Gordon N. Bardos, "Jihad in the Balkans: The Next Generation", *World Affairs,* September/October 2014.

consolidating its reach through its provinces such as in Libya it is clear they are increasingly relying on *hawala* networks for transferring funds. This mechanism will increase in importance as ISIL expands in operational areas with infrequent or no access to international financial institutions.

In Europe, it has been easier to detect and disrupt *hawala* business to terrorists. The most prominent case is the roll up of a massive secret *hawala* network in Spain that was composed of 300 *hawaladars* with clandestine offices around Spanish cities through 250 butcher shops, grocery stores and telephone call centres. They managed "the savings of over 150,000 Muslims, many of whom are believed to be receiving social welfare payments from the Spanish state, without any legal oversight. The network allegedly paid the salaries of Spanish jihadists in Syria: They received about $800 if they were single and $1,200 if they were married."[70]

It is Somali *hawala* networks that have received most attention. These exist through the Horn of Africa and are the lifeline for most Somalis and their diaspora communities around the world. Since the series of terrorist attacks in Nairobi and specifically the 2015 attack against Garissa University College, Kenyan authorities have suspended licences of 13 major remittance firms alongside focused efforts against al-Shabaab sympathizers and operatives. Dahabshiil, which is the remittance service used by 95 percent of international agencies and charities in Somalia, was suspended alongside others such as "Kendy, UAE Exchange, Amal, Iftin, Kaah Express and Amana. Others include Juba Express, Tawakal, Bakaal, Hodan, Continental and Flex."[71]

Cash couriers

The existence of ISIL cash couriers is not surprising given the global coalition against it. These cash couriers provide essential services for ISIL inside Syria and Iraq as well as across the border into Turkey where it is distributed to trusted networks and used to buy essential equipment.

The system of cash couriers also works the opposite direction in which European FTFs and support networks conceal and transport cash to ISIL and their fighters. In one such case Amal El Wahabi, a British mother-of-two, was arrested and convicted in the UK for trying to arrange to smuggle €20,000 (£16,000) to her husband in Syria.[72]

Social Media Transactions

According to the head of Australia's financial intelligence agency, crowdfunding is an emerging source of funding for ISIL and its terrorist activity.[73]

---

[70] http://politica.elpais.com/politica/2015/01/30/actualidad/1422641735_380266.html
[71] http://www.unhcr.org/cgi-bin/texis/vtx/refdaily?pass=52fc6fbd5&id=55260d235
[72] "Two unlikely jihadis: the 'weed-smoking kaffir' and the ignorant dupe", *The Guardian,* August 13, 2015. http://www.theguardian.com/uk-news/2014/aug/13/amal-el-wahabi-nawal-msaad-trial-syria-terrorism
[73] "Islamic State using social media as crowdfunding platform for terrorist activities, expert warns", *ABC,* November 17, 2015.

Crowdfunding for specific projects combines clever social media and emotional telethons with fund-raising power of multiple individuals. Establishing charitable NPOs for this purpose can attract funding through diverse social media sites. According to FATF reports there are plenty of cases where the appeals for supply and equipment was quickly matched with specific instructions to which bank accounts or MSBs funds were to be sent.[74] This is likely to become a major emerging modus operandi across multiple social media platforms.

Crowdsourcing is also evident in *Jahed Bimalak* (Make Jihad with Your Money) which is a fundraising campaign for Jabhat al-Nusra (JN or Nusra Front), the official al-Qaeda branch in Syria, under the supervision of the Saudi JN-affiliated scholar Abdallah al-Muhaysni and his JN-affiliated civil organization, The Jihad's Callers Center.[75] The campaign has been running since 2014 and the mobile applications used by Jahed Bimalak are the mobile messenger application Telegram and WhatsApp. Like Kik, Telegram is considered to be secure and this application is popular among fighters and terror group supporters in Syria and Iraq. The campaign is candid that the donations are used to purchase arms for JN, and it showcases weapons bought with donations received via the Jahed Bimalak campaign.

Jahed Bimalak's fundraiser refers potential donors to the mobile app Telegram. There, he asks the donor to join a Secret Chat – a service provided by Telegram whereby conversations are not saved on Telegram's servers and the application provides its users with the option to delete messages after a certain period of time, predefined by the user. Moreover, the app does not allow you to resend messages from a secret chat to other media platforms. To start such conversations, both users must accept the secret chat option.

Following one case over the Internet provides interesting insights into modus operandi. During a secret chat conversation, the fundraiser points out that the transfer should be affected via any branch or company that accepts Western Union's services in Turkey. Notably, the recommended amount for a donation should range between $500 and $9,500 allowing, according to fundraiser, repeat transfers and hampering the discovery of the money trails by the authorities. The donor is requested to advise the amount of the donation as soon as possible. The fundraiser provides contact details for the transfer and asks the donor to send him the "secret code" after executing the transfer, in order to withdraw the money in Antakya (on the Turkish border with Syria). The details of recipients could be traced to Hayat humanitarian foundation.

Another example of crowdfunding is an effort by the Chechen Salafist-jihadist group fighting in the Aleppo area, Jaish alMuhajireen wal-Ansar. This group operates a fundraising campaign called "7sanaabil" using WhatsApp and Telegram for transfer instructions of funds.

---

[74] FATF Report, *Emerging Terrorist Financing Risks October,* 2015.
[75] This information was provided by a private consultancy firm in the Middle East.

Another new emerging trend among ISIL and other groups is using the wide variety of digital cryptocurrencies such as Bitcoin or accessing the Dark Web as a subversive, hidden market area for arms sales as well as document forgery.[76] As a European Union Institute for Security Studies report starkly show that mastery of the Dark Web unlocks infinite possibilities for terror finance.[77]

ISIL have been skilful in exploiting social media sites to advance its global mobilisation campaign. It has also developed a presence on most social media sites providing extremely targeted and well-choreographed and appealing propaganda. As ISIL have become more security conscious it has increasingly moved towards encryption solutions in its use of social media.

Over time ISIL have learnt that new available technologies offer safer social media communication solutions. It is also in response to protect ISIL from Anonymous hacking efforts. ISIL advise that the safest social media communication apps are: SilentCircle, Redphone, OsTel, ChatSecure, Signal, Telegram, Wickr, Threema and Surespot.[78] The use of these is increasing in frequency and it is expected that new digital currencies and social media methods will increase in frequency in the future.

Foreign Terrorist Fighters and Travelling to Syria

The scale and scope of the European FTF travels to Syria and Iraq to join ISIL is unprecedented. It is estimated that around 5,000 EU nationals have joined ISIL and to a lesser extent Jabhat al-Nusra since the onset of the Syrian civil war. While there are significant numbers of FTFs departing from France (1,700): Germany (750); United Kingdom (700-1,000) there are other smaller states with proportionately higher ratio of the Muslim population leaving for Syria.[79]

From Belgium 470 have joined ISIL (50 are women); from the Netherlands 210 have joined; from Denmark 130 have joined, and from Sweden 286 have joined out of which at least 45 are women. In Scandinavia, there is a total of 500 FTFs of which almost 200 have returned. From Austria over 300 FTFs (with a high proportion of former Chechens) have left, which probably is a spill-over effect of its vicinity to the Western Balkans from which several hundred FTFs have departed.[80]

The funding mechanisms for FTFs departing from Europe for Syria and Iraq via Turkey are multi-varied as recruits often are asked to provide pre-departure financial contributions from a range of different sources in their home countries. These financial contributions vary according to the recruit's individual financial position and situation. While the average age of male recruits is 26, it is lower for the females who are often between 17-21 years old.

---

[76] Ian McKendry, "ISIL May Be Using Bitcoin, Fincen's Calvery Says", *American Banker,*
[77] Beatrice Berton, "The dark side of the web: ISIL's one-stop shop?", *Issue Alert* 30 (2015).
[78] Don Reisinger, "This is How ISIS Communicates Online", *Fortune,* November 19, 2015.
[79] This information has been gathered by Linus Gustafsson at SEDU throughout 2015.
[80] Ibid.

Often male recruits come from a difficult past with dysfunctional families and a multi-criminal background having past convictions for e.g. drug-offences, theft or violence. Many have operated together with territorial criminal gangs and acquired useful criminal skillsets. Acquiring available funding provides FTFs with enhanced status and position within ISIL on arrival in Syria.

There are several possible indicators before travel. FTFs often make sudden asset sales before departure. They often quit their jobs if they have one. It is often common that they make unusually large withdrawals from their accounts. A red flag is unusual high activity in combination with many different loans and cash withdrawals. In terms of company financial activity, recruits often generate very large revenue in short periods. Credit is accumulated and business purchases are at high levels to maximize credit limits and orders are placed within a short period, often IT or mobile phone related purchases. Bills are never paid. This means that by the time the recruit has travelled unpaid invoices keep arriving in large numbers.

FTFs travel to and from the principal conflict regions in Syria or Iraq through direct or indirect air travel routes (often they break up travel patterns to disguise destination) or through various land routes to Turkey, Jordan, and Lebanon. Turkey is a key hub for flows of FTFs and funding sources with a long and porous land border to Syria. Often FTFs fly into Istanbul and then proceed to fly to Hatay or other airports closer to the Turkish-Syrian border. Some are denied entry in Istanbul but travel with boats through the Greek archipelago to gain entry to Turkey. Many travellers now avoid Istanbul because they are turned away. Instead they travel to charter destinations close to Syria. There are cases with sponsorship of travel through several detour destinations.

When they arrive in Turkey at an airport they proceed through different routes to the border areas where there are safe houses. ISIL have issued pre-travel instructions which are combined with other facilitation advice. For example, FTFs are given phone numbers to safe houses on the Turkish-Syrian border. They are also instructed to contact the Office of the Border of *Dawlah* (Islamic State). They are told to use Android phones as Iphones have geolocation and to buy Turkcell pre-paid telephone cards at the airport. Women should also be escorted by a *mahram* (male companion) when travelling through Turkey and it is mandatory inside of Syria.[81]

Turkey is a key hub for the flow of funds to Syria for terrorist use, especially along border towns in Syria. Intelligence suggests that cash is withdrawn from ATMs on the border of Turkey and Syria by foreign fighters engaged in fighting in Syria. Periodic withdrawals occur over prolonged periods along the border areas through MSBs. Small amounts (€ 500 –€ 1,000) are usual levels of withdrawal to avoid suspicions. This is the principal assignment of the facilitator.

[81] This information is derived from various ISIL manuals available on social media platforms.

Funding methods

There are a number of methods used by FTFs to acquire the necessary funding. Many are identical to the multiple ways described in earlier sections. They acquire unsecured loans in banks through the Internet (at times with falsified employment records or salary slips) and through SMS-loans which they can secure quickly and from many different financial institutions. Common for loans is that FTFs intends to default on them. Often loans are multiple, combining larger and smaller amounts, and they occur in a short time period. A fall-guy, who absorbs the blow when the loan defaults, is sometimes used for larger schemes, and it is often the case that these volunteers are themselves FTFs in Syria.

Another method is to secure vehicle loans or lease of vehicles; they will default on payments and often report the vehicle stolen to claim insurance. The vehicles are often larger SUVs and transport vans. Sometimes the FTFs sell the vehicle in another country to pocket profits. It has become more difficult for FTFs to transport vehicles in or out of Turkey as authorities 'couple' entry and exit visas of persons with specific vehicles.

Some try social insurance fraud even though the reporting requirement and control stations makes is more difficult to collect from afar. Pre-advance student loans, often to study at a foreign university, are another method. Some FTFs receive contributions from specific funding drives at religious meetings. *Tajheez* sources of funding are extended in some cases. These are given on case-by-case basis.

Indicators and Red Flags (awareness raising)

Single indicators are difficult to develop and use as FTFs financial activity often is low and designed to appear routine. It is, however, the combined account activity that provides a fuller picture and the possibility to detect anomalies. For example, the combined account activity using "ATMs in known jihadi-gathering locations, has taken a consumer loan that is in arrears or in default, has received an unusual number of typically small payments that might be from supporters or donors, or has received a student loan but is not attending classes, a different picture begins to emerge."[82] There is no 'one-size-fits all' typologies that will solve the issue of detection of terrorist finance. Yet it is important to combine many different indicators in different scenarios.

It is possible to develop several indicator sets of FTFs behaviour that needs to be combined to provide meaning and utility. Here are some useful indicators and advice[83]:

- Multiple loan applications to several financial institutions combined with SMS-loans in short period of time, combined with large cash withdrawals and airline ticket purchases to destinations near FTF destinations.
- Geographically map ATMs and MSBs along the (Turkey) border area.

---

[82] http://www.bbc.com/news/business-32722318

[83] Some of these indicators were drawn from: http://www.moneylaunderingbulletin.com; http://2www.acams.org/webinars; and unclassified law enforcement papers.

- High account activities and frequent withdrawal of funds from international destinations near FTF destinations.
- Multiple airline tickets and broken up travel arrangements with Turkey emerging as final destination combined with travel costs.
- VAT-fraud is detected when companies trading in IT- or mobile phone sales make quick and huge profits in short periods of time.
- Individuals with low or no income apply for multiple loans (bank, SMS, etc.) using false employment papers/payslips.
- Travelling to places near FTF destinations in combination with purchases of outdoor equipment or military supplies.
- Loans with no security or leasing arrangements to purchase specific SUVs (Toyota Hillux or equivalent (often in white/black). Often buyers have not pre-owned vehicle.
- Unexpected sale of personal belongings and assets combined with travel to areas near FTF destinations.
- Receiving multiple funds to same FTF account from multiple senders.
- Flurry of activity in account and then dormant with withdrawals from areas near FTF destinations.
- Receipt of donor funds into FTF account in Turkey and flipping these to other conflict zones through many-to-one; one-to-many; many-from-one.
- Identifying areas along border, border towns and associated ATMs and known crossings into Syria.
- Upgrade of credit limit combined with questions about ATM withdrawal in Turkey, Jordan and Lebanon.
- Complete clean out of account combined with airline ticket purchase to areas close to FTF destinations.
- Use of family accounts transferred to FTF near Syrian border.
- Social media profiles (open) reveal often sympathy for FTF causes.

It is important to better understand FTF financing issues and to combine different typologies together with an in-depth understanding of the geography of FTF border areas and processes of transferring funds through legal and illicit means. Additionally, simple searches on social media profiles of FTFs can be useful as auxiliary information tool.

Terrorists are increasingly using new innovative ways with new technologies that provide infinite possibilities to generate and transfer financial funds. It is crucial to recognize that any typologies will be in constant flux. They need to account for monitoring of new terror finance techniques, combined with new the evolution of new technologies that enable terrorist groups to evade detection.

Countering terrorist financing – National models

This section describes other countries national framework and structures to prevent, detect and counter financing activities in support for terrorism. The information is drawn from openly available documents as well as interviews with both state officials engaged in CTF activities and researchers studying CTF-regimes and their effects.

Due to this study's limited resources this section is narrowed down to the national CTF regimes of United Kingdom and Canada. These two countries are singled out for this study due to their active and long term efforts in this area on both national and international level and as representatives of two rather different regime settings. Studying these two national regimes provides some useful insights from which Sweden can benefit in the continued work to strengthening its CTF structures and processes.

Financial intelligence in national regimes

A national regime designed to prevent, detect and respond to financial activities with links to terrorism or terrorist entities is heavily depended on financial information. Any regime with a CTF purpose must be designed in order to promote and facilitate sharing of relevant financial information between actors involved in any of the above purposes of the CTF regime.

Financial information of relevance for and analysed by agencies and state functions within the regime results in "financial intelligence" (FININT) and may have several purposes. It may provide useful knowledge for intelligence, law enforcement and regulatory authorities to reconstruct or piece together how a criminal act was conducted after an event has occurred, identify or confirm relationships between individuals and activities as well as looking forward by identifying signals and behaviour patterns of relevance to detect and predict future terrorist activities.

Furthermore, financial intelligence serves a vital function in an analysed and aggregated form of providing knowledge and insights from which all potential nodes for collecting new financial information to the regime can develop their methods and focus. Thereby, this function becomes a potential force multiplier by enhancing the capacity to generate new financial information and intelligence of quality and relevance to the regime as a whole.

Financial intelligence has to a larger degree come to serve a key function in the overall work against terrorism and criminal occurrences, both in terms of understanding past events, identifying and investigating current activities as well as a tool to understand possible future activities of concern.

National Counter Terrorist Financing Regimes

Learning from other countries perspectives, experiences and knowledge is one way to assist in identifying own capabilities, weaknesses and possible ways forward. CTF is portrayed to be "a room in many buildings" and hence need a national framework of leadership (regulatory framework and strategic direction) and a robust structure for inter-agency coordination and communication. The

national CTF regime is furthermore heavily dependent on the relationship with sectors in society that may become abused (direct or indirect) by terrorists and criminals or their supporters.

This section, exploring other countries CTF regimes, is therefore structured by brief descriptions of national framework, structures for inter-agency coordination and information sharing and finally the public-private partnership of CTF relevance. The final section discusses what this study considers to be part of key factors in national CTF regimes and its possible implications for Sweden.

Canada

The framework

The Canadian governments stated objectives are to create a hostile environment towards terrorist financing, to respect international obligations and to be vigilant in dealing with terrorist financing (TF).[84] The minister of Finance is accountable and has the lead responsibility for the national regime in fulfilling the objectives. The efforts to counter terrorist financing are conducted within the wider framework known as the anti-money laundering and anti-terrorist financing regime. The regime is based on three pillars: Coordinating policy; prevent money laundering (ML)/TF; and disrupting ML/TF.

The first pillar constitutes the regimes framework. A primary component of this framework is the national legislation. The Canadian legislation dates back to the Proceeds of Crime (Money Laundering) Act (AML) from 2000. The AML act established the Canadian Financial Intelligence Unit (FINTRAC), and compulsory reporting of large and otherwise suspicious transactions by financial institutions. The AML act was amended in December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), bringing the counter terrorist finance aspect into the legislation.

The PCMLTFA together with the Criminal Code constitutes the foremost regulatory tools to combat terrorist financing in Canada today. While the Criminal Code addresses a variety of TF-related offences, the PCMLTFA creates the mandatory reporting system, regulates cross-border movements of currency and the mandate of the agency that administers the act. Furthermore, the PCMLTFA requires the financial institutions and intermediaries to identify their clients, keep records and have an internal compliance system in place

The second pillar creates the prevention of terrorist-linked linked funds or criminal abuse of the financial system. The foundation for this capability rests on the financial institutions and their intermediaries who are the gatekeepers to the financial system on which the regulators depend. FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) are the regulators ensuring the compliance for this regulated business.

---

[84] Testimony of Diane Lafleur to Air India Commission reported in "Air India Flight 182 – A Canadian tradegy", Vol.5, p.14, 2010

The final pillar of the Canadian AML/ATF-regime represents the detection and disruption of transactions linked to money laundering, terrorist financing and other financial crimes. Key agencies to disrupt TF are the Canadian intelligence and law enforcement agencies together with the Canadian Revenue agency and the public prosecutors service.

Furthermore, the regime has a terrorist listing process to freeze terrorist assets. The terrorist listing process is established pursuant to the national Criminal Code, led by Public Safety Canada (PSC), and UN regulations administrated by the Canadian Foreign Affairs. In June 2015, Canada had in total 90 terrorist entities listed under these two listing regimes. In September, more than 50 entities was listed based on TF-related activities.[85]

In its 6th follow-up report of the mutual evaluation report (MER), February 2014, FATF concluded that Canada had made significant progress in addressing the deficiencies identified in the 2008 MER and could be removed from the regular follow-up process.[86]

The Canadian CTF-regime

The Canadian AML/ATF-regime is a comprehensive, horizontal initiative, led by the department of Finance and comprises of 11 federal departments and agencies. The goal is to detect, deter and facilitate the investigation and prosecution of ML/TF-crimes as outlined by the three pillars of the regime.

Responsible authorities are the Department of Finance which has the primary responsibility for the government initiatives to counter TF together with FINTRAC, Department of Justice, The Public Prosecution Service, The Royal Canadian Mounted Police (RCMP), Canadian Security and Intelligence Service (CSIS), the Canada Border Service Agency (CBSA) and the Canada Revenue Agency. These authorities have specific government funding for countering terrorist finance amounting to $70 million annually.[87] Other authorities in the regime are OSFI, Public Safety Canada and the Department of Foreign Affairs, Trade and Development.

In addition to this governmental regime structure approximately 31 000 financial institutions and businesses across the country have a shared responsibility to counter TF.[88]

The Canadian Financial Intelligence Unit (FIU) – Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

The Canadian FIU serve a key function within the Canadian AML/ATF-regime with the mandate to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.

---

[85] Interview with Canadian officials in Ottawa on 23 of September 2015.
[86] Mutual Evaluation of Canada, 6th Follow-up Report, FATF, 14 February 2014.
[87] ”Terrorist Financing in Canada and Abroad: Needed Federal Actions”, Report of the Standing Committee on Finance, June 2015, page 9.
[88] Discussions with FINTRAC officials in Ottawa, 23 September 2015.

FINTRAC have three main functions: To serve as a central repository for financial information; to analyze that information; and to facilitate dissemination of the results. FINTRAC can also monitor compliance to FATF recommendations, block transactions, freeze bank accounts and engage in financial sector training, research and public education. The Canadian FIU is established as a stand-alone administrative and regulatory agency under the Ministry of Finance and not an entity within the law enforcement and intelligence services. FINTRAC hence constitutes as an intermediary between the reporting financial business sector and the law enforcers, a model designed to enhance the likelihood of winning the private sectors trust.

FINTRAC receives approximately 20 million financial transaction reports from a broad range of financial business institutions annually. These reports provide FINTRAC with a wealth of data from which FINTRAC can produce actionable FININT for both tactical and strategic purposes. During 2014, FINTRAC produced 1,143 FININT disclosures to regime partners, of which 234 were related to TF activities.

The type of financial reports provided to FINTRAC includes:

- Cross-border currency reports and seizure reports from CBSA
- Casino Disbursement reports
- Electronic Funds Transfer reports ($10,000 and above)
- Large Cash Transaction Reports
- Suspicious Transactions Reports (STR)
- Terrorist Property Reports

The reports are received through FINTRAC's database which contains more than 250 million transaction reports in total. Approximately 90,000 STRs is received from financial institutions annually, mainly from the bank sector. The criterion of $10,000 for electronic transaction reports is under evaluation since terrorist financing often includes transactions far below that amount. There is however a technical obstacle to reduce or remove an amount criterion as the number of reports is likely to increase from $20 million up to $60 million or even $80 million annually.[89]

The FINTRAC database as well as access to other databases provides a very powerful capacity to analyse the reports, together with other information, in order to produce FININT products to other regime partners. The intelligence products are to a large degree disseminated to CSIS, RCMP and the local police forces. Other entities receiving FINTRAC intelligence are CBSA, provincial/territorial securities commissions and the Canada Revenue Agency (on suspected illicit transactions involving charities). Recently FINTRAC has produced information on money laundering and terrorist finance trends and typologies within specific financial business sectors as an effort to provide feed-back to reporting financial

[89] Gérald Cossette, statement for the House of Commons Committees – FINA (41-2), number 073, March 24, 2015.

institutions.[90] Finally, the FIU provides intelligence to the federal policy makers to inform them about the dynamics and emerging trends within the TF environment.

FINTRAC is a very active partner within the international efforts to counter TF. Intelligence is shared with other countries FIUs which also provides FINTRAC access to their FININT. Canada has signed a memorandum of understanding with 90 of the 147 different FIUs within the Egmont Group. As a result of the tactical and strategic financial intelligence work, FINTRAC plays a significant role in international efforts including at the Financial Action Task Force, within Egmont Group of financial intelligence units and in other international organizations.

Canada Revenue Agency (CRA)
As the federal regulator of charities in Canada, CRA have three main responsibilities in relation to TF: protecting the charity system from abuse by terrorists, sharing information of relevance to departments and agencies to detect and supress terrorist financing activities and assisting Canada in meeting international obligations.[91]

CRA can decide on specific monitoring or investigation of charities if provided information that an entity may have ties to terrorism. CRA receives information from law enforcement and security intelligence agencies if there is intelligence regarding suspected illicit activities amongst charities. FINTRAC can disseminate FININT to CRA on the condition that it may have links to money laundering or tax evasion. CRA do not have the reciprocal obligation to report information to FINTRAC on information related to TF activities. CRA reports to intelligence and law enforcement agencies regarding charities engaged in suspected ML or TF activities may however be shared through the partnership the agencies have with FINTRAC.

The CRA assess that approximately 1% of the reviewed charity registration applications in Canada are deemed to be of high risk and thereby undergoes a more detailed review.[92]

Identified weaknesses and recommended measures
During 2015, the Canadian AML/ATF-regime underwent a comprehensive review, led by the Standing Committee on Finance, assigned by the then acting Minister of Finance, Joe Oliver. The review was initiated as a response to recent terrorist incidents with connections to Canada and the agreement amongst G-20 Finance Ministers to deepen the cooperation in efforts to combat terrorist financing.

The review resulted in some critique against vital aspects of the regime, both in terms of effectiveness and privacy concerns. The Canadian Privacy Commissioner

---

[90] See FINTRAC webpage, Guidence, Guideline 2 “Suspicious transactions”, 20151124 http://www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp
[91] Rick Steward, CRA Assistant Commissioner, Presentation to the Finance Committee on Terrorism, March 26, 2015
[92] Gérald Cossette, statement for the House of Commons Committees – FINA (41-2), number 073, March 24, 2015

has previously stated that there is a risk of over-reporting and retention of data in violation of the right to privacy.[93]

The review resulted in 15 recommendations that the Committee of Finance deemed necessary in order to increase the effectiveness of the regime. The recommendations covered a broad range of measures including efforts to bring increased transparency to the charitable sector, enhanced public-private partnership, increased review mechanisms of FINTRAC:s efficiency, objectives and capabilities, training and education regarding TF-risks to the private sector, law enforcement and legislators as well as providing better guidelines and guidance to reporting entities within the financial sector.[94]

In particular the report highlights the necessity for all federal activities in the domain of countering terrorism to consider the financing angle and develop a deeper knowledge of the connection between financial transactions and terrorist activities.

United Kingdom

The framework

The United Kingdom's early undertakings to counter terrorist financing were disclosed in a joint HM Treasury and Home Office report in October 2002.[95] In the report the UK is stated to be a leading world participant in efforts to counter the financing of terrorism. Furthermore, the acting ministries Gordon Brown and David Blunkett expressed in the foreword of the report: "*Our response to the funding of terrorist acts must be every bit as clear, as unequivocal and as united as our response to the terrorist acts themselves*." The document specifically conveys a firm commitment to establish a powerful CTF-regime in the UK by providing new regulatory regimes, more resources to key agencies, a structure for coordination and cooperation and promote a strong partnership with the financial sector.

The UK Government concludes that as finance is the lifeblood of criminals and terrorist, it is also one of their greatest vulnerabilities. Three key organising principles guiding the UK regime against financial crimes set out in the 2004 Anti-Money Laundering Strategy are:

- Effectiveness – making maximum impact on the criminal and terrorist threat;
- Proportionality – so that the benefits of intervention are justified and that they outweigh the costs;

---

[93] "Privacy concerns with FINTRAC remain following two separate audits", News release by the Office of privacy Commissioner of Canada, October 24, 2013

[94] "Terrorist Financing in Canada and Abroad: Needed Federal Actions", Report of the Standing Committee of Finance, June 2015

[95] "Combating the financing of terrorism: a report on UK action, HM Treasury and Home Office, October 2002.

- Engagement – so that all stakeholders in government and the private sector, at home and abroad, work collaboratively in partnership.

A UK Government strategic document from February 2007 states that UK operates within a comprehensive international framework that deters financial crime and terrorism in the first place; detects it when it happens and disrupts the activities of those responsible.[96]

The basic principles for the UK CTF-regime is furthermore stated to bring about an increased understanding of the threats which will guide mitigating actions, inhibit institutional barriers and ensure a development toward maximum practical impact, an impact which will be assessed in order to ensure the effectiveness of the regime.

The UK CTF-system applies a risk-based approach, similar to the Canadian system and many other national CTF-models. This principle implies that all parties in the national system focus their resources on the areas where the likelihood and impact of abuse of the financial system is greatest.

According to the latest HM Treasury risk assessment on money laundering and terrorist financing, released in October 2015, the UK approach focuses on three main areas: reducing terrorist fundraising in the UK; reducing the movement of terrorist finance into/out of the UK; and reducing the fundraising and movement of terrorist finance overseas.

Furthermore, the UK strategic documents highlight the financial business sectors "*immense value in delivering high-grade financial intelligence and effective audit trails*" in support of government insights and measures regarding terrorist financing. It also brings the asset freezing tool to the forefront of the UK counter terrorist efforts in general. Asset freezing provides the capacity to deny terrorists ability to raise and move funds through the international financial system; deal with funds already in the financial system and provides lead intelligence components in support of investigations and regulatory measures.

The UK CTF Legislation
The UK regulatory framework for countering terrorist finance consists of a range of legislations providing the key instruments for law enforcement and regulatory authorities.

The legal regulations of terrorist property are covered by the Terrorism Act 2000 (TACT). Terrorist property is defined as: money or other property which is likely to be used for the purposes of terrorism, commission of acts of terrorism and acts carried out for the purpose of terrorism.[97] Offences covered by TACT include:

- inviting, providing, or receiving money or other property with the intention or reasonable suspicion that it will be used for the purposes of terrorism,

[96] "The financial challenge to crime and terrorism", HM Treasury, February 2007
[97] Terrorism Act 2000, Part III, Section 14

- using or intending to use money or other property for the purposes of terrorism,
- being involved in an arrangement which makes money or other property available for the purposes of terrorism,
- being involved in an arrangement which facilitates the retention or control of terrorist property by concealment; removal from the jurisdiction; transfer to nominees, or in any other way.

The Anti-Terrorism, Crime and Security Act 2001 was introduced to the Parliament two months after the 9/11 terrorist attacks in the United States and went into force in December 2001. The act strengthened the powers to counter terrorist financing in the Terrorism Act 2000 and provides the police with powers to seize terrorists' funds anywhere in the UK, freeze funds in the outset of any investigation, the ability to monitor accounts which may be used to facilitate terrorism as well as imposing obligations on people to report suspicions that funds are destined for terrorism. The act also allows the Treasury to freeze assets of foreign individuals, groups and countries where there are reasonable grounds to suspect that they pose a threat to the UK. This act has since then been developed through the Prevention of Terrorism Act 2005 and Terrorism Prevention and Investigation Measures Act 2011.

The Proceeds of Crime Act 2002 (POCA) establish the regulatory foundation for anti-money laundering. POCA targets not only traditional money laundering measures but all proceeds and properties generated through crime. The Money Laundering Act regulates the requirements on the financial sector entities which include capacities to verify the customers' identities, keep financial records for five years and a reporting system ensuring that suspicious activities are reported. The regulation also requires that staff is well trained to identify signs of illegal activities and have the capability to respond in accordance with the key legal requirements.

The Money Laundering Regulation 2007, place requirements on entities to have systems and controls in place to identify, assess, manage and mitigate risks with the purposes of preventing and detecting money laundering and terrorist financing. The regulations include requirements to conduct customer due diligence (CDD) and identify risk clients, have a nominated officer for ML/TF, ensure awareness and training of staff etc.

The Terrorist Asset-Freezing Act 2010 (TAFA) was introduced as a response to the obligations set out in United Nations resolutions and European Commission regulations and establishes the UK terrorist asset freezing regime. To designate a person under TAFA two criteria has to be met: (1) there has to be evidence to support a reasonable belief that the person has been involved in terrorism activity and (2) that it is considered necessary for purposes connected to protecting the

public from terrorism that financial restrictions should be applied.[98] Offences under the TAFA include:

- dealing with funds or economic resources owned, held or controlled by a designated person,
- making funds, economic resources or financial services available to or for the benefit of a designated person,
- circumventing the restrictions imposed by those restrictions.

TACT, TAFA and related national legislations[99] bring UK in line with international requirements and agreements to counter terrorist financing and money laundering.

The UK CTF-regime

Countering terrorist financing constitute a key part of the UK long-term strategy against terrorism (CONTEST). Measures to detect and tackle financial transactions are an integral aspect of the Pursue-strand of CONTEST. The Home Office, Office for Security and Counter-Terrorism (OSCT), is responsible for all CT-policy in the UK. Other departments with a key role within the UK regime are the HM Treasury and the Foreign and Commonwealth Office (FCO). HM Treasury appoints supervisors reviewing the AML/CTF measures on a regular basis and is also responsible for financial sanctions within the UK and freezing terrorist assets under the TAFA, manly on requests from the police and intelligence agencies. HM Treasury also leads the UK delegation to FATF. FCO is responsible for UK obligations to international agreements, UN resolutions etc.

The main cross government coordinating committee for CTF-policy in the UK is the Terrorist Finance Action Group[100] , which convenes four times a year, brings policy, operational and supervisory experts together. The committee's foremost function is to set policy and direction for the UK CTF-regime and to drive continuous improvements in tackling the terrorist finance threats. In HM Treasury strategic document from 2007 the committee presented four prioritized issues for developing the CTF-regime work including building a better understanding of the TF-threat, identify knowledge gaps and how to address them, policy interventions to strengthen the wider environment for CTF-actions and to promote more effective financial tools to disrupt terrorist targets.[101]

A key function within the UK CTF regime is the National Terrorist Finance Investigation Unit (NTFIU), located within the Counter-terrorism Command of the Metropolitan Police (SO15). NTFIU has the strategic lead of law enforcement for countering terrorist financing in the UK and is responsible for all investigations of financial matters with possible links to terrorism activities or

---

[98] Terrorist Asset-Freezing etc. Act 2010, chapter 1, Section 2, Treasury's power to make final designation

[99] For example the Terrorism Order 2006 and the Al-Qaida and Taliban Order 2006 established to meet the obligations under United Nations resolutions.

[100] Now changed into the Terrorist Finance Board, interview at RUSI, 14 of April 2015.

[101] The financial challenge to crime and terrorism, HM Treasury, February 2007, page 39.

entities. NTFIU also supports mainstream police CT-investigations with financial intelligence and financial disruption options.

NTFIU is also located within ten additional Counter-terrorism Units situated in various cities throughout England, Scotland and Northern Ireland. NTFIU is the main receiver and investigator of financial intelligence from the UK Suspicious Activity Report (SAR) regime and received 10-11 000 reports of suspected transactions of CT relevance during 2014. Of these reports 856 (approximately 8%) where investigated by the NTFIU with possible connections to terrorist activities.[102] NTFIU is furthermore active in outreach activities to the financial business sector. The outreach programme is stated by NTFIU representative to be a vital part of gathering financial information from the private sector. This investigative capability within the Metropolitan police have developed and established FININT as a key component in all CT-related police investigations in the UK.

The UK SARs regime is led by the national Financial Investigation Unit (FIU), located within the National Crime Agency (NCA). The FIU constitutes the gateway to reporters of SARs submitted under both TACT and POCA. The Terrorism Finance Team (TFT) within the FIU identifies and acts upon submitted reports relating to terrorist financing. Terrorism related SARs are disseminated to NTFIU and other CT-related agencies. During the period October 2013 to September 2014 the number of CT-related SARs increased with over 56% compared to the same period the preceding year.[103]

The increase of terrorist-related SARs is likely due to the general increase of reports from the financial sector. The total number of SARs submitted during this time period was over 350 000 and are registered in the ELMER database. A modern and effective database-tool for receiving and analysing SARs is crucial to all FIU and the whole SARs regime. ELMER is stated to be reaching the end of its lifetime and hence constitutes a risk for the efficiency of the UK SARs regime.[104] There are approximately 1.5 million SARs registered in ELMER and all SARs are retained in the database for six years or until proven not to be linked to a crime.[105]

The TFT conducts analysis of SARs and other financial intelligence with the purpose of identifying terrorist finance typologies. These typologies are produced in order to inform the financial business sector for awareness raising and discussions on relevant indicators of TF activities. The typologies are also used for cross-Whitehall assessments for both domestic use and to international bodies in relation to strategic policy and standard setting. Furthermore, the FTF is

---

[102] Interview with NTFIU representative, London, 14 of April 2015.
[103] Suspicious Activity Reports (SARs) Annual Report 2014, National Crime Agency,
[104] UK national risk assessment of money laundering and terrorist financing, HM Treasury, October 2015, p 10.
[105] The SARs regime, National Crime Agency website, 20151211 http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/the-sars-regime

engaged in CTF-training both abroad and for national programs and is the UK representative in the Egmont Group.

Other UK agencies engaged in CTF-work is the security and intelligence agencies including the Security Service (MI5), Government Communications Headquarters (GCHQ), Ministry of Defence and the Secret Intelligence Service (SIS). The UK intelligence fusion centre Joint Terrorism Assessment Centre (JTAC), based in MI5-headquarters, is the lead function to analyse intelligence on international terrorism threats at home and abroad. JTAC sets the threat levels and issues specific warnings to concerned sectors in government departments and agencies. The intelligence community serves an important function in providing CT-related intelligence and as a capacity to identify subjects of interest as well as a key entity using financial intelligence disseminated by the FIU and NTFIU for terrorism threat assessments.

Cross-agency cooperation
The core UK structure for cross-agency cooperation and information sharing is based on secondment of personnel between government agencies and departments. The SO15 have personnel placed at agencies such as MI5, GCHQ, MoD, SIS and NCA (UKFIU). At NTFIU other agencies have seconded personnel such as the Charity Commission, Department for Work and Pensions and HM Revenue and Customs.[106] This model of secondment for interagency cooperation provides the foundation for fruitful cross-pollination and shared expertise between agencies that is crucial for identifying and assessing complex linkages between different criminal activities.

Private-public partnership on terrorist financing
Information sharing and partnership between government agencies and the private sector has been identified as a vital part in developing a robust system for preventing, detecting, and respond to finance activities with links to terrorism. However, the relationship between government agencies and the private sector in the UK has been recognised as plagued by mistrust resulting in poor information sharing where vital information possessed by each party has been kept in silos.[107]

This observed and acknowledged weakness in the UK regime spurred the creation of new set of initiatives to develop this partnership in relation to AML/CTF. In 2014 the Financial Sector Forum (FSF) was set up by the Home Office together with the Bank of England and the Financial Conduct Authority. FSF purpose is to establish a joint effort between government and financial institutions to collectively understand the threat, disrupt criminal activities and protect UK institutions from damage. FSF convened three times during 2014 to discuss joint measures to "stamp out illicit activity and ensure the UK retains its pre-eminent position in financial services worldwide."[108]

---

[106] Interview with NTFIU representative in London, 14 April 2015.
[107] Speech by Hon Theresa May, Home Secretary on the work of the Financial Sector Forum, GOV.UK, 24 February 2015.
[108] Speech by Hon Theresa May, 24 February 2015.

As a result of the FSF the Joint Money Laundering Intelligence Taskforce (JMLIT) was launched in February 2015. JMLIT is a one year pilot initiative where representatives from NCA:s Economic Crime Command and National Intelligence Hub, HM Revenue and Customs, City of London Police (NTFIU) meets and share information with financial institutions including the non-profit company CIFAS and vetted staff from Barclays, Santander, Standard Chartered, RBS, HSBC, BNP Paribas, Citigroup, Nationwide, Lloyds and Post Office. The taskforce is led by the head of NCA Economic Crime Command. The initial task for JMLIT was to combat Money Laundering but its key priorities has been complemented with "understanding key terrorist financing methodologies" in the autumn of 2015.[109] The efforts within JMLIT to develop a better understanding of TF are led by the NTFIU.

Another initiative to increase the partnership between public and private sectors to fight economic crimes is the launch of the Financial Crime Alert Service (FCAS) which developed by the British Bankers Association. FCAS went operational in April 2015 and is a system developed to provide British banks with alerts regarding trends observed by 12 different government and law enforcement agencies in the UK.

[109] NCA homepage, Joint Money Laundering Intelligence Taskforce (JMLIT), 20151201, http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

Key Factors for a CTF-regime and Implications for Sweden

A holistic and risk-based approach

Any national regime construction treating terrorist financing as a separate discipline, relevant only for the security service, is destined to be ineffective and of minimal use. Both the UK and Canadian regimes includes a holistic approach – one regime for all financial crimes within which FININT are shared across the spectrum of law enforcement, regulating authorities and intelligence. As financial transactions constitute a key activity in all form of crimes and hence can be utilized by government agencies to detect and respond to illicit activities, sharing and analysing FININT must become one of the centre pieces in the everyday work by all regime partners.

There are many references to the fact that most terrorist investigations include other illicit proceeds making signatures of other crimes a potential lead for disrupting terrorism-related activities. Conversely, investigations of suspected terrorist entities can provide useful information of other crimes committed by the suspects that may constitute a more robust case for success in future convictions in court proceedings, disrupting any plans of terrorist activities.

Hence, all FININT related to money laundering, other financial crimes and terrorist financing represents possible avenues for investigations for all law enforcement, intelligence agencies as well as regulatory authorities. The key success factor for any regime is therefore to develop information sharing and dialogue mechanisms which provides a holistic and cross government approach, avoiding silos between money laundering, terrorist financing and other financial crimes creating possible avenues to utilize the interconnections between terrorism and other criminal offences that more often than not exists.

Furthermore, making the most effective use of the limited regime resources rest on a shared perspective of where the risks in the national financial system are of highest concerns. A risk-based approach requires that both government and industry has good knowledge of where the risks of financial abuse are of particular concern and that the national regime has a flexibility to adapt to changed circumstances and events. A process of identifying and sharing risk perspectives needs to be guided by a national strategy but the flexibility in the regime is heavily dependent on effective dialogue and information sharing cross government and in close partnership with the industry.

Government and industry; partnership through balance and systematic dialogue

Throughout this study the relationship between the government regime and the financial sector has been raised by most interviewed representatives in visited countries as a key success factor for effectively combating any financial crime. The financial sector constitutes the foremost information-nodes for data on illicit proceeds conducted or in the making.

The international obligations to set in place regulations and measures on the national level in order to fight money laundering and terrorist financing has

developed considerably during the last decade as an effect of the increasing costs to society by financial crimes and the alarming trend of increased threat from terrorism against the west.

Most notably the obligations for the financial business industry has grown rapidly to include the capacity to have better knowledge of clients, screening transactions and reporting suspicious activities in real time to the FIU. Reaching proportionality with the growing burden for the financial institutions requires that the government establishes a balanced capability to make the most use of the business sectors efforts end engagement.

It furthermore creates a pressing need for guidance and directions from government to the industry as of what to be aware of and how to report information in a way that results in the best outcome. This means that the relationship between government and the industry must be perceived as a vital part of the cross-government regime. The quality and relevance of reported financial data from the industry can only be developed and improved through a continuous, long term and systematic dialogue, where feed-back, guidance and guidelines are developed and disseminated by the government agencies.

Capabilities to produce useful Financial Intelligence

There is a wide pool of sources to information of relevance for investigating terrorism activities. A traditional form of information for law enforcement and intelligence agencies rests upon the capacity to collect information from special sources and through special methods. This is the art of the intelligence community within the country and partners abroad.

A second category of sources for CT- relevant information is represented by open sources and the increasing stream of information through social media applications.

A third category and specifically related to the terrorist financing challenges is access to data from the financial industry sector. Any function with the task to play a key role producing useful FININT within the government CTF-regime needs access to a wide plethora of relevant information streams from different sources and of varying format and character. This puts a heavy challenge to any agency and requires both skilled human resources (investigators and analysts) and tools designed for the purpose to merge information, analyse the information through different methods and to produce intelligence products for different end-users and purposes.

Contingent of any law enforcement business is to use detailed data of individuals, activities and transactions related to a specific crime for investigative purposes. Investigations of specific entities of concern require tools to identify and examine financial footprints and assets but also for revealing links to other individuals, suspicious purchases, transfers or withdrawals linked to specific dates or locations. These investigative measures will produce intelligence of potential high operative value for other law enforcement and intelligence agencies but may also

be relevant for regulatory authorities who may possess additional data related to the specific entities or activities under investigation.

For the purpose of identifying trends, potential future modus operandi and threats the detailed data of entities, activities and transactions needs to be put in a larger context. Analysing activities in relation specific geographic locations, entities and specific illicit proceeds or using statistics to analyse deviations or dominating aspects of financial activities may be of outmost importance for the law enforcement and intelligence agencies to assess future events and behaviour.

This type of strategic relevant FININT are furthermore very useful for policy-makers at government offices but can also serve the purpose for informing relevant sectors within the financial industry regarding trends and behaviour of highest concern.

It may also have a force multiplier effect as an informed and aware compliance officer at a financial institution will be more likely to report relevant financial data to the FIU than one that do not know what to screen for. Strategic FININT-based information produced in support for industry-specific sectors (i.e. banks, insurance companies, money service business, security dealers, real estate, casinos etc.) could become a corner stone for industry outreach and dialog. Furthermore, it could provide the industry with the critical insight and awareness that enhances the financial institution to report suspicious transactions into the CTF-regime.

The capacity to merge all types of information and to conduct analysis in order to produce useful FININT, both on the investigative operational level as well as trend analysis on a strategic level is of outmost importance for a comprehensive approach within a CTF-regime. Limited ability for strategic analysis will in the long term have a negative impact on the capacity to access high quality information and the ability to produce useful FININT for law enforcement operational purposes.

FATF has produced useful effectiveness assessment methodologies in relation to "immediate outcome 6" which should be considered by all countries with an ambition to establish an effective CTF-regime where FININT is appropriately used by competent authorities.[110]

An active international engagement

FATF and the Egmont group of Financial Intelligence Units represents two examples of lively international structures where threat perspectives, methodologies and framework for combating terrorist finance are shared between countries and institutions. Actively contributing to this cross-pollination of experiences and perspectives is yet another avenue for building the capacity both nationally and supporting the international community in general to prevent, detect and respond to terrorism and financial crime. Putting resources from the

[110] Methodology for assessing compliance with the FATF recommendations and the effectiveness of AML/CTF systems, FATF, February 2013, http://www.fatf-gafi.org/media/fatf/content/images/FATF%20Methodology%2022%20Feb%202013%20.pdf

national regime for the purpose of international collaboration can thus become a very potent force multiplier, more beneficiaries for the national CTF-effort in the long run than the burden on resources dedicated to the engagement at the time of the event.

Implications for Sweden

One of the main conclusions in this study is the necessity to have a national hub that simultaneously investigates operational cases and analyze strategic aspects to terrorist finance. It will be very difficult to forge closer cooperation between the finance sector and national authorities without the existence of a national hub with adequate resources, tools and production output of useful FININT. Similarly, such a hub would strengthen law enforcement/intelligence cooperation with the financial regulatory system.

The study has recognized four areas with regards to Sweden where improvements could be considered in order to detect and prevent terrorist financing:

- The first area is about strengthening the role and function of the national FIU by providing the unit the resources, tools and organizational leverage to collect, analyze and disseminate FININT to support the national regime as well as policy makers with useful output. Strengthening the FIU is furthermore vital in order to provide feedback, guidance and guidelines for the financial sector.

- The second area concerns the lack of a common operational picture due to inertias and ”bottlenecks” when it comes to information sharing between the three key actors – the Swedish Security Service, the Finance Police (who also acts as the Swedish FIU) within the National Police Authority and the informal group of the four major banks. One recommendation here would be to instigate regular trustful information sharing forum, where the UK-model might give some inspiration.

- The third area is about the need for concrete examples (”cases”) and scenarios to develop a grounded understanding and context where these kind of unwanted financial transactions takes place. Focusing in on FTF financial transactions provide a narrow scope for focus of financial institutions (major banks). Even if ways and means of the transactions are fluid and the modus operandi could change fast, there is still a need to develop a common knowledge base in order to with new perspectives be able to detect suspected transactions in the overwhelming flow of totally legal and harmless transactions.

- The fourth and final conclusion is the necessity for further studies on terrorist finance risk areas within the financial sector. As recognized by UK National Risk Assessment of Money-Laundering and Terrorist Financing there are certain sectors such as MSBs, cash- and banking-sector that can be exploited. Studies need to provide in-depth analysis on changing modus operandi and the role of social media in this process.

Another priority area is to examine charities and foundations and their potential exploitation for terror finance purposes. There also needs to be thematic studies on, for example, terrorist finance modus operandi in the Nordic areas to look for similarities, differences and trends in order to identify risk areas and counter-measures.