

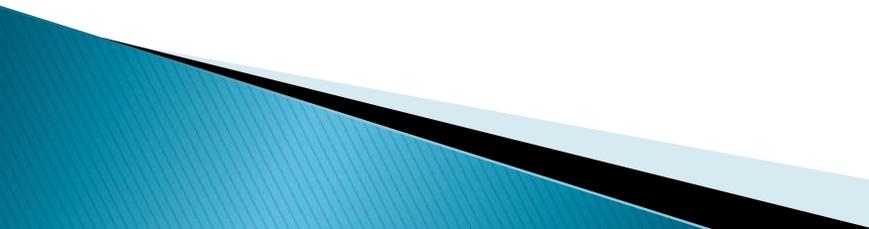
# Terrorism Financing: New Developments in the Area

Robin M. Sykes  
Chief Technical Director, FID  
Jamaica Bankers Association  
AML/CFT Conference 2015

# Terrorism

- ▶ Terrorism stated to be a Tier 2 Threat in Jamaica's National Security Policy 2013;
- ▶ Low probability but High Impact particularly on the tourism sector;
- ▶ Key action points:
  1. Identify threats use of scan assessments, undertake independent critical reviews and use counter-factual reasoning to identify vulnerabilities;
  2. Use of better and more timely intelligence as to the nature and intention of terrorist organizations as regards Jamaica
  3. Training and technology to address a crisis when it occurs;
  4. Improve response capacity (particularly public health infrastructure, with appropriate stockpiles of medical supplies to address the issue)

# The Global Landscape

- ▶ The growing outrageous nature of atrocities committed by terrorist groups such as ISIL and Boko Haram and the ever expanding reach and influence of such groups has refreshed the global community's commitment to address vulnerabilities in the CFT system;
  - ▶ Complicated by the new dynamic where major terrorist organizations (TO) actually occupy and manage clearly defined geographical areas;
  - ▶ FATF has been reviewing the status of implementation of FT measures to assess levels of compliance to report to G20 Leaders.
- 

# Traditional TF means (non-exhaustive)

- ▶ Use of the formal financial sector;
- ▶ Cash Couriers
- ▶ Misuse of NPOs: useful for moving funds in crisis area
  - a) Diversion of legitimate donations;
  - b) Affiliation/exploitation of the NPO with/by a TO;
  - c) Abuse of programme delivery;
  - d) Sham organization
- ▶ Proceeds of Criminal Activity: includes identity theft, smuggling, kidnapping , even tax offences;
- ▶ Extortion of local population;
- ▶ Funding from legitimate enterprises: restaurants, used car dealerships owned by persons originating in the high risk area;
- ▶ Use of nominees/front companies

# Emerging Trend 1: Financial Management

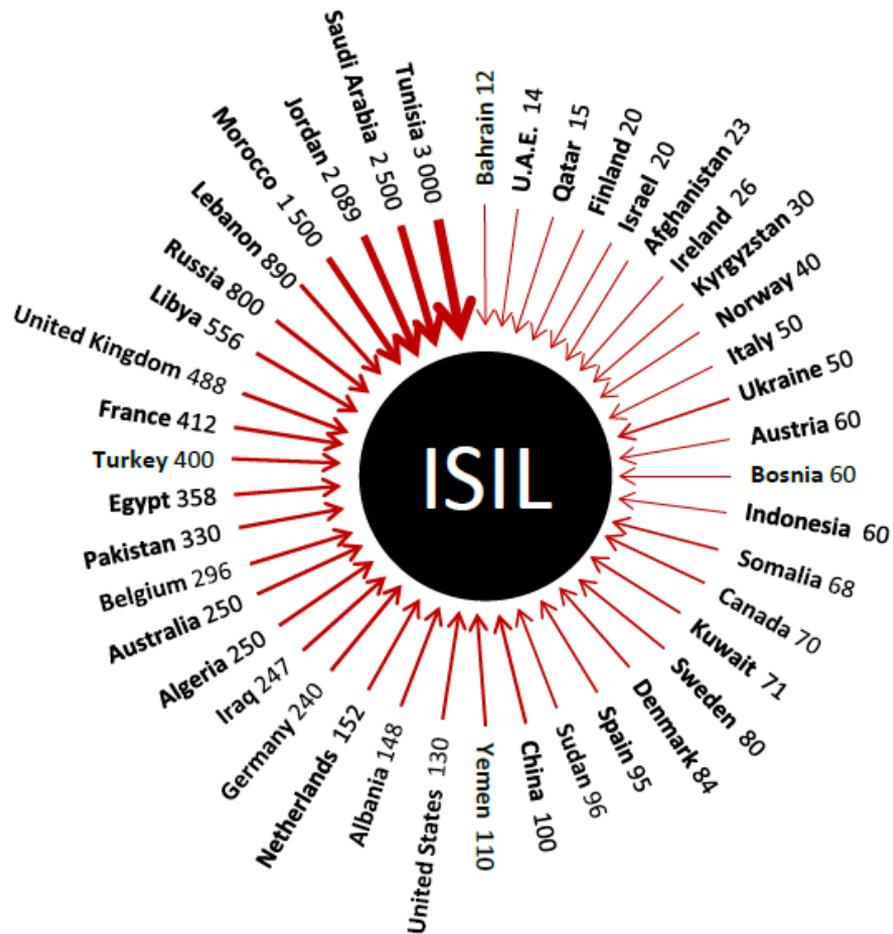
- ▶ TOs vary in size/complexity. Most plots involve less than USD10,000 in resources;
- ▶ Larger, more organized TO requires financial expertise to manage its various ongoing activities (recruitment, training, propaganda, infrastructure, social services).
- ▶ Groups such as ISIL have recruited accountants and other professionals to manage assets and resources, sometimes monitor financial institutions in the domain as well as impose and monitor “taxes”.
- ▶ Captured information from Al Qaida shows meticulous financial recording of the financing of the African operations in Mali;
- ▶ Possible actions: more focus in this area can indicate best disruptive action, identifying targeting these financial managers as well changing focus on destination of funds as opposed to source of funds

# Emerging Trend 2: Foreign Terrorist Fighters

- ▶ It has long been an obligation to prohibit provision of goods and financial services to TOs but how to treat with FTFs?
- ▶ UN Security Council Resolution 2178 of 2014 requires states to prevent the “recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning of, or participation in terrorist acts”.
- ▶ States shall ensure that their legal systems provide for the prosecution, as serious criminal offences, of travel for terrorism or related training, as well as the financing or facilitation of such activities.
- ▶ Likely to be enhanced attention to travel patterns and countries of origin and destination, closer surveillance of social media to ascertain countries/ demographic being targeted as well as those sympathetic to the various causes;
- ▶ Closer ties with immigration authorities, airlines, travel agents to obtain information;
- ▶ In Australia, Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 has minister criminalizing “no go” areas. Person has to prove legitimate purpose for entry.
- ▶ In other cases, jurisdictions are withdrawing welfare benefits of persons suspected of being FTF

# Where are they coming from?

FATF FEBRUARY 2015



# Emerging Trend 3: Use of Internet

- ▶ TO's use of the internet and social media to recruit and radicalize persons is well known. Also the use of sophisticated communications to promote their activities is also well known.
- ▶ However large scale and well organized fundraising schemes aimed at TF can involve up to thousands of sponsors to collect large amounts of cash.
- ▶ Germany: case of persons online requesting urgent donations to meet the needs of a FTF in Syria giving deadlines;
- ▶ Canada: persons under suspicion who tried departing for terrorist purposes was found to have made donations to crowd-funding website (where accounts can be set up by any party) relating to conflict relief in Countries A,B and C.

# Internet Fund Raising issues

- ▶ Payments can be made through a variety of vehicles including crowd funding platforms, paypal, provision of debit and credit card numbers, credit for a mobile phone. These details are not sent by mail but provided over skype. Sometimes the payment chain is broken via cash withdrawal and physical transportation.
- ▶ Advertisements for funding often ambiguous in coded language, use of images or symbols to avoid searches, use of closed online networks;
- ▶ Question as to the role of the platform providers. What is their role and responsibilities regarding the blocking and taking down of websites and what should be the powers of government in this regard? Such sites can have valuable information on identification, details IP addresses and account information.

# Emerging Trend 4: New Payment Methods

- ▶ Virtual currencies represent a new method for transmitting value over the internet. As these grow in popularity, so will TF Risks.
  - ▶ These currencies (such as Bitcoin) allow for anonymous transfers, instantaneously.
  - ▶ Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into a public ledger. This activity is called mining and the miners are rewarded with transaction fees and newly created bitcoins. Besides mining, bitcoins can be obtained in exchange for different currencies, products, and services. Users can send and receive bitcoins for an optional transaction fee. There is no central administrator or repository. Also the supply is limited thus removing possibility of manipulation resulting in devaluation.
  - ▶ The initial purchase of bitcoin (through a Bitcoin exchange) is traceable but the subsequent transactions are not unless you know who owns which account.
- 

# Interest from banks in Bitcoin

- ▶ US has in New York addressed the issue by regulating Bitcoin exchanges.
- ▶ Sunday Times August 30 2015

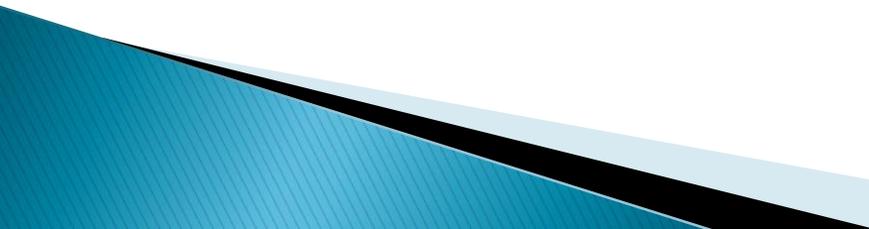
*One of Britain's biggest high-street banks is about to take the first step in bringing bitcoin, the controversial digital currency, into the mainstream, saying it has the "potential to change financial services. Barclays has been conducting experiments into bitcoin in "labs" in London, and working with start-ups. It now plans to test the virtual currency, allowing people to make donations to charities in bitcoin.*

- ▶ Recall of course that bitcoin was the currency of choice in relation to the Dark web and the Silk Road

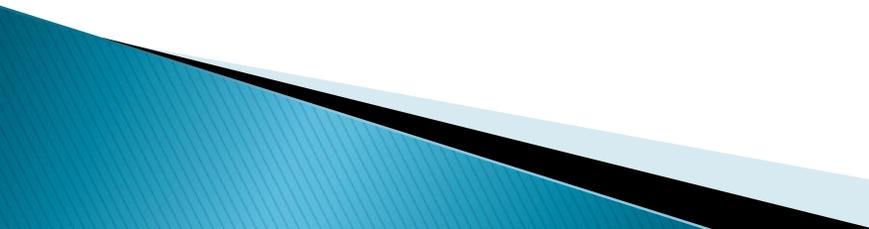
# NPM: Ali Shukri Amin

- ▶ Ali Shukri Amin, a 17-year-old resident of Virginia, pleaded guilty on August 28<sup>th</sup> 2015 to charges of using social media to aid the ISIL terrorist group.
- ▶ On or about July 7, 2014, using the @AmreekiWitness account, the defendant tweeted a link to an article he authored entitled “Bitcoin wa Sadaqat al-Jihad”(Bitcoin and the Charity of Jihad).
- ▶ The link transferred the user to the defendant’s blog, where the article was posted. The article discussed how to use bitcoins and how jihadists could utilize this currency to fund their efforts.
- ▶ The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen.

# NPM: Open Payment Cards

- ▶ Where funds can be preloaded and withdrawn at global ABMs.
  - ▶ Once the card is carried offshore, funds are accessible with minimal chance of being detected.
  - ▶ Stored value cards in some jurisdictions are not subject to CDD.
  - ▶ Some allow for multiple cards to draw from a common pool;
  - ▶ Portability of the card allows for undetected crossing of borders.
  - ▶ Critical balance has to be sought as regards the prospective benefits of financial inclusion and the risks of anonymity posed by these products.
  - ▶ Recall TF does not require large amounts.
- 

# UK Canada Joint Operation: Crevice

- ▶ UK Target suspected of a plot to detonate a 66kg IED in London.
  - ▶ Covert search of UK targets 's luggage whilst at the Stansted Airport revealed a Canadian issued bank card in unrelated female name.
  - ▶ RCMP checks showed wire transfers and account holder was closely linked with an Canadian IT Specialist with high security clearance, who was in the process of obtaining tickets to go to UK.
  - ▶ Technical surveillance showed he had developed a detonator and was planning to carry same to UK with cash for the UK target.
  - ▶ Both and co-conspirators were arrested and subsequently tried, with life sentences being handed down.
  - ▶ The key was the bank card. If it had been issued anonymously as a open payment card, the case would have failed.
- 

# Emerging Trends 5: Geographical Control

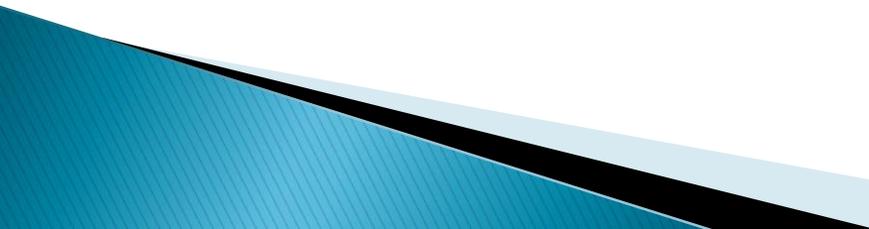
- ▶ ISIL\* presents a key challenge insofar as they control huge geographic regions and a key emphasis is the expansion of their territory.
- ▶ Proceeds to fund ISIL are generally raised by illicit proceeds from occupation (extortion, looting, kidnapping, control of oil fields, cash smuggling);
- ▶ ISIL claims (in addition to Syria and Iraq) new provinces, in Libya (Wilayat al-Barqah, Wilayat al-Tarabulus, and Wilayat al-Fizan), Algeria (Wilayat al-Jazair), Egypt (Wilayat Sinai), Yemen (Wilayat Sanaa), and Saudi Arabia (Wilayat al-Haramayn. In January 2015, a new province was announced in Afghanistan–Pakistan (Wilayat Khorasan), in March 2015 a new province was announced in and around Northern Nigeria (Wilayat Gharb Afriqiya), and in June 2015 a North Caucasus province (Wilayat al-Qawqaz) was announced.
- ▶ So potentially funds to that area (even for legitimate purpose) have a strong potential; to fall into ISIL hands.

\*Islamic State in Iraq and the Levant

# Some Key Findings from the FATF

- ▶ Some countries have not criminalized assisting a terrorist when the terrorist is not engaged in a criminal act (only one of our offences seems to cover this (section 7 deal with property owned or controlled)
- ▶ Some countries are not clear whether their laws will be sufficient to cover foreign terrorist fighter (who operate abroad);
- ▶ There is not sufficient supervision/enforcement to ensure that financial firms meet their obligations under the law
- ▶ Countries are only now trying to criminalize travelling for Terrorist purposes.
- ▶ Some countries have major delays in implementing UNSCRs into domestic laws for targeted financial sanctions (freezing);
- ▶ There are very low levels of cross border requests for freezing terrorist assets (in last 5 years only 4 FATF countries requested over 50 requests)

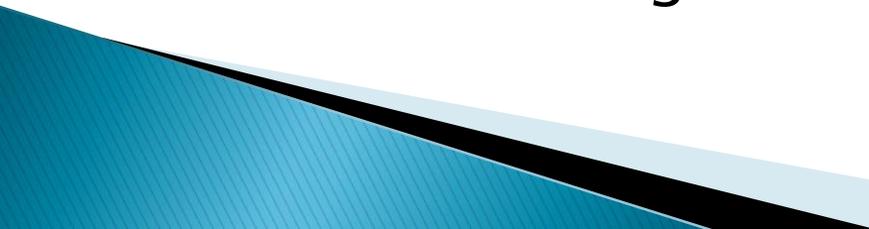
# FATF Commitment

- ▶ Review of findings with countries indicating reforms;
  - ▶ Amendments of standards to deal with foreign fighters;
  - ▶ Guidance on effective supervision and enforcement of financial sanctions;
  - ▶ Clarifying how AML/CFT measures should be applied to charities;
  - ▶ Preparing a handbook to facilitate foreign freezing requests
- 

# Some other possible directions

- ▶ FATF will reform its standards on TF by incorporating new requirements on foreign terrorist fighters (ensuring that the offence is wide enough to include cases where no terrorist offence is involved);
- ▶ Jurisdictions are now looking at greater access powers with respect to travel agencies and airlines;
- ▶ Perhaps use of the powers proposed under Australian Bill to designate “no go” zones;
- ▶ Regulatory Geographical Targeting Order: FIs in high risk areas have to do more EDD
- ▶ Expanding the guidance available as to how CFT measures should apply to NPOs;
- ▶ Obligations on companies registries to report suspicious transactions;
- ▶ Bringing payment services providers/platforms under the AML/CFT framework

# What are we seeing?

- ▶ Passengers transit Jamaica from unusual destinations going to unusual destinations, sometimes carrying out financial transactions whilst in Jamaica to garner funds before travelling out;
  - ▶ Foreigners from high risk zones conducting large financial transactions (whilst “on vacation”), providing evasive information (i.e. a phone number through which he can be reached).
  - ▶ Persons receiving wires from high risk zones, requesting different persons to collect them, some wires indicating NPO in the high risk jurisdiction
- 

# What are we doing?

- ▶ Acknowledged that we are at an early stage and our framework does not encompass these emerging trends;
- ▶ Training both for senior FIU analysts and investigators. These include RCMP/Canadian Department of Justice/FINTRAC training as well as UK National Terrorist FIU (Scotland Yard) training;
- ▶ Training has and will include ODPP, CTOC, RPD, MOCA, JDF, CUSTOMS
- ▶ Engagement with Charities Authority about outreach and a RBA to AML/CFT
- ▶ Discussions with BOJ and FSC on MOUs to lead to discussions on designating high risk jurisdictions;
- ▶ Discussions with BOJ/World Bank on balancing inclusion concerns with TF issues;
- ▶ Discussions with CTOC on MOU to facilitate better co-ordination relating to TF cases
- ▶ Building on regional MOUs and working with regional bodies in increasing regional vigilance and co-operation on FT issues;
- ▶ Ongoing revision to the TF laws particularly coming out of the CFATF Mutual Evaluation (including naming of DNFBPs as reporting entities)

# The End

## ▶ Sources:

- I. FATF Global Money Laundering and Terrorist Financing Threat Assessment (July 2010)
- II. FATF International Best Practices Targeted Financial Sanctions relating to terrorism and the Financing of terrorism (June 2013)
- III. Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL) (February 2015)

## ▶ QUESTIONS?