The term “terrorist financing” became prominent in international banking after the September 11, 2001 attacks in the United States. Since then, the term has permeated the world of financial sector compliance, financial intelligence and national security.

The rationale behind generating anti-terrorist financing compliance regimes within financial institutions is to deny individuals and groups the funds necessary to carry out acts of terrorism.

Yet attacking the purely financial aspect of a terrorist group limits the potential impact of a financial institution’s AML/ATF compliance regime upon terrorist activity.

An act of terror depends not just upon the available liquid assets of the day, but the support networks, institutions, affiliate groups and infrastructure that surrounds the terrorist group.

For some terrorist operations, the necessary levels of resourcing are complex. For others, particularly so-called “lone wolf” operations, the necessary resourcing is more spontaneous and immediate. The larger the terrorist event, the more likely significant resourcing by members, supporters and others was expended in the lead time to the event.

By placing focus on “terrorist resourcing”, a financial institution can turn its financial intelligence capabilities towards the support and architecture behind terrorist groups, not just bank account balances and wire payments.

In a chaotic world, financial institutions placing emphasis on terrorist resourcing will yield more accurate financial intelligence. Greater accuracy within reporting entities will lead to more concise disclosures by national financial intelligence units. The intelligence community and law enforcement will benefit greatly from more refined indicators distributed by the national financial intelligence unit.

With more accurate information, the war waged against terrorist groups inflicting horrendous damage upon a civilian population will hopefully slant in favour of civilised nations and away from barbaric violence.

During the month of November 2015, numerous terrorist attacks caused grave concern amongst civilised people and nations.

On Friday November 13th 2015, the capital of France was attacked by gunmen and suicide bombers, violence not seen in Paris since the Nazi occupation of the Second World War. Few intelligence community professionals believe the momentum of terrorist activity will subside in the short term.

In October, the Financial Action Task Force (FATF) released a report outlining emerging terrorist financing risks. Financial institutions were then expected by banking regulators and financial intelligence units to incorporate the information
discussed in this report into their compliance regimes.

The FATF report states the following on jurisdictions who criminalise the financing of a terrorist organisation:

In 71% of all jurisdictions (and 94% of FATF members) the terrorist financing offence applies to financing a terrorist organisation even for a purpose unrelated to committing a terrorist act. This is important, as the majority of terrorist financing is not used to meet the direct costs of mounting attacks but for broad organisational support (including recruitment, training, subsistence, travel, and maintaining a veil of legitimate activities), particularly in the case of foreign terrorist fighters.

The “broad organisational support” mentioned by the FATF report describes activities that are not directly associated with an act of terrorism that either maims or kills innocent civilians to spread fear amongst a population.

The support can be quite bland in nature, as even terrorists need to eat, stay warm, move about and sleep. Without efficient supply lines, logistics, finances or management, major acts of terrorism are difficult, if not impossible.

In volume 5 of the Canadian government’s 2010 report into the terrorist bombing of Air India Flight 182, John Schmidt, then of Canada’s Integrated Threat Assessment Centre (ITAC), spoke of a shift in mind-set from financing to resourcing:

Schmidt named his model the “Terrorist Resourcing Model” rather than the “Terrorist Financing Model” because, in his view, TF does not necessarily involve money. It can consist of an exchange of goods and, even if money is used, it may not reach the operating cell if it is exchanged before then for goods.

The terrorist resourcing model identifies five stages which may not necessarily appear in each case, nor occur in the order listed below.

**Stage 1 - Acquisition**
Includes both the acquisition of funds and of goods or services to be consumed by the terrorist group, including munitions, transportation, food or shelter.

**Stage 2 - Aggregation**
The pooling of resources into manageable clusters for administration or accumulation.

**Stage 3 - Transmission to a Terrorist Organisation**
Finances, goods or services are moved from one location to another, often across an international border.

**Stage 4 - Transmission to a Terrorist Cell**
Assets are allocated to a specific terrorist cell to perform a specific task, which may include a terrorist act or an activity that furthers the cause of the terrorist group.

**Stage 5 - Conversion**
The exchange of assets, financial or otherwise, for end-use goods.

There are a variety of sequences and possibilities for all the above stages, many of whom are outlined in the Air India report. In certain cases, some stages are skipped and others are re-arranged.

Acts of terrorism that involve few actors and depend on assets that are easily at hand will create a straightforward flow in the terrorist resourcing model. More sophisticated combinations of assets over longer periods of time will generate more elaborate flows through the model and, unfortunately, terrorist events with larger impacts upon a civilian population.

For financial institutions, whether monitoring transactional activity or conducting on-going due diligence, reporting suspicious activity remains the top priority. The July 7, 2005 terrorist attacks in London were generated by a group that relied...
partially on petty theft and credit card fraud to fund their daily routines prior to the attack.

Numerous sources have stated that had certain suspicions been reported regarding individuals involved in the September 11, 2001 attacks, counter-terrorism divisions of the FBI and CIA may have been able to piece together the possibility of a major attack.

Hindsight is always 20/20, yet the evidence clearly states that the reporting of suspicious criminal and money laundering activity can lead directly to a greater understanding of terrorist activity.

Suspicious activity reported by an employee or generated from transaction monitoring or analytics software could be, at first glance, to be possible indicators of money laundering activity. Yet it may form a piece of a terrorist resourcing investigation by an intelligence agency or branch of law enforcement.

The modern international financial institution understands the need to incorporate terrorist resourcing into its compliance regime. It also understands the discreet role it plays within a nation’s defences against organised crime and terrorist groups. Those who seek loud pronouncements of gratitude and waves of publicity from their AML/ATF efforts are in the wrong line of work.

At first glance, the most valuable piece of financial intelligence it may ever report could appear to be a simple transaction or association between persons or entities.

Yet this seemingly innocuous piece of information could be of enormous benefit to a team of intelligence professionals during an investigation. Intelligence agencies are well aware that to reveal their tradecraft by thanking staff at a financial institution may damage their ability to conduct future investigations. It’s simply not worth the risk.

As a result of this level of operational security, a financial institution may never know whether a piece of financial intelligence perceived to be money laundering was ever employed in a terrorist resourcing investigation.

Professionals in the public sector understand this is a thankless job where the impact of one’s efforts may have a direct or indirect bearing upon a nation’s money laundering and/or terrorist financing defences. Compliance professionals at financial institutions face a similar fate.

Financial institutions who fully engage their responsibilities for creating and maintaining a vibrant compliance regime that truly implements the FATF’s risk-based approach are aware that they are part of the solution towards terrorism.

Financial institutions who adopt a lackadaisical approach to terrorist resourcing can do more harm than good. They are easily manipulated by those who seek to resource terrorist groups, the consequences of which can be damning.

In 2016, combatting terrorist resourcing will be more than scrubbing names through a purchased database. As recent events have proven, the stakes are simply too high to tolerate inaction.

Terrorist resourcing is examined in-depth in ManchesterCF’s FINTEL (Terrorist Financing & Resourcing) training program for supervised financial institutions and public-sector agencies.

For further information, visit: www.manchestercf.com