Calls to cut off terrorist financing increase

Date Posted: 20-Jul-2016

Author:

Publication: Jane's Intelligence Review

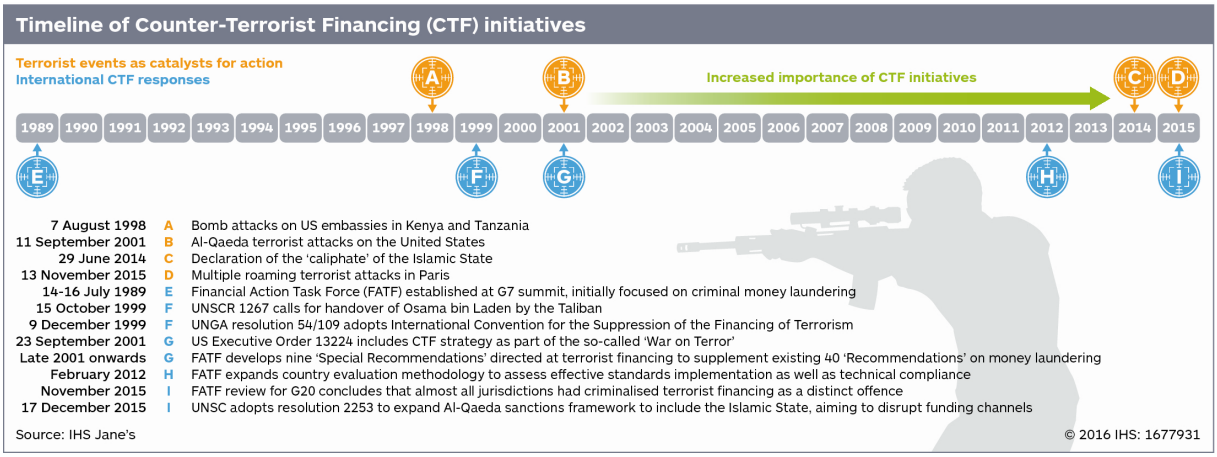
Efforts to counter terrorist financing have increasingly co-opted financial institutions to disrupt the flow of funds. *Tom Keatinge* surveys the evolution of the risk environment.

Key Points
- Counter-terrorist financing (CTF) has featured as a central plank of global counter-terrorism and security efforts since the 11 September 2001 attacks on the United States.
- The evolving terrorist threat, the diversification of available financing tools, and increasing response options all shape CTF initiatives.
- The state-like nature of groups such as the Islamic State has necessitated the use of broader and more varied tools of economic warfare.

Following any terrorist attack, particularly those on Western capitals, there are frequently calls for the financing of terrorists to be identified, targeted, and curtailed. In the immediate aftermath of the 13 November 2015 terrorist attacks in Paris, a communiqué of the scheduled G20 meeting in Turkey expressed a commitment to "tackling the financing channels of terrorism". On 20 November 2015, the European Council urged "increased information-sharing and operational co-operation with regard to the monitoring and investigation of… terrorist financing".

Furthermore, Democratic presidential candidate Hillary Clinton raised the issue of counter-terrorist financing (CTF) following the 22 March 2016 attacks on the airport and metro system in Brussels, urging European banks to cut off the funds that flow to terrorism. Since the 11 September 2001 attacks on the United States, significant effort and resources have been expended in attempting to disrupt terrorist financing.

The end of the Cold War, and the concerted use of UN Security Council resolutions against countries such as Libya and Sudan, led to a dramatic decline in the availability of finance for state-sponsored terrorism. Organisations such as Hizbullah continue to operate with state backing, but terrorist organisations emerging since the Cold War have mostly been unable to rely on state sponsorship and have needed to source their own financing. This presents a vulnerability to be exploited by those seeking to counter their plans and activities.



Timeline of Counter-Terrorist Financing (CTF) initiatives (©2016 IHS)

1677931

A CTF strategy, in the form of Executive Order 13224 signed on 23 September 2001, was the first step in then president George W Bush's so-called 'War on Terror' following the 2001 attacks. He announced, "Today, we have launched a strike on the financial foundation of the global terror network… We will starve the terrorists of funding."

Consequently, although targeting the financing of terrorists was not new - for example, UK authorities directed considerable efforts towards disrupting the funding of the Provisional IRA - the attempt to co-ordinate such an effort systematically and globally certainly was. The 2001 attacks exposed the CTF shortcomings of US domestic and international approaches, the architecture for disrupting terrorist financing, and the lack of an effective, globally co-ordinated response.

Shifting landscape

Several key factors that should determine the shape of CTF responses are continuously evolving. Three in particular are notable: the evolution of the terrorist threat; the diversification of available financing tools; and the broadening of response options.

At the time of the 11 September 2001 attacks, the emerging response to terrorist financing was focused squarely on Al-Qaeda in light of the 1998 US embassy attacks in East Africa. The 2001 attacks confirmed that all efforts to disrupt terrorist financing should be directed at Al-Qaeda, and the strategies that were developed were therefore almost entirely intended to cut off the funding that the group needed to operate and proliferate.

This particularly included the abuse of charities, the use of cash couriers and 'hawalas' (highly effective, informal money remittance agents), and the use of the formal US banking sector (through which an estimated USD300,000 of the USD500,000 needed to fund the 2001 attacks may have been transferred). Such an approach made sense initially, but the global terrorist threat subsequently evolved, becoming multi-faceted and morphing to include not only Al-Qaeda but also a spectrum of threats ranging from lone actors and small cells to proto-states such as the Islamic State and Harakat al-Mujahideen al-Shabaab.

Connected to this evolving threat picture is a diversification of funding options. The attacks of 2001 led to a focus being placed on the vulnerabilities presented by charities, money service businesses, and other informal mechanisms for raising and moving funding. A number of actors - including the US-based charities Global Relief Foundation and Benevolence International Foundation - quickly found themselves to be the subject of intense scrutiny, ultimately being added

to US and UN terrorist designation and sanctions lists.

Many actors from these sectors continue to be the subject of scrutiny and risk assessment, with many losing access to financial services as banks choose to shed clients that they view as 'outside their risk appetite' in a world of heightened regulatory scrutiny. Consequently, a range of new financing tools has been exploited by the broadening array of terrorist actors.

Since the Islamic State emerged in mid-2014, considerable focus has been placed on disrupting the group's finances. Indeed, one of the core responses arrayed by the international community against the Islamic State is the Counter-ISIL Finance Group, a multi-national gathering of security and finance experts that seeks to degrade the Islamic State's financing capability.

Responses deployed by the international community with the aim of restricting the group's finances have been varied and include the bombing of its oil infrastructure and supplies, restrictions on financial access for those banks and money exchange houses that are operating in or close to Islamic State-controlled territory, and the suspension of salary payments to Iraqi government employees still operating in these regions.

Although less high profile, similar efforts have been made to restrict the financing opportunities of Al-Shabaab in Somalia by applying sanctions to the trade in charcoal, a key source of funding for the group. The state-like nature of these groups has necessitated the use of tools of economic warfare that are broader and more varied than the narrowly-focused responses originally applied by the international community against Al-Qaeda.

At the other end of the spectrum, the limited funding required by lone actors and small cells takes a different form. Although many such plots and attacks are financed with the attackers' own resources, financial sources that were not previously deemed to be vulnerable to abuse by terrorists have at times been exploited.

Key among these are sources that provide access to small amounts of cash sufficient to fund unsophisticated but high-impact attacks. Student loans, payday loans, and other forms of consumer finance have proved popular as, for attackers who do not intend to survive their actions, the problem of repayment is moot.

In addition to loan financing, petty criminality - particularly fraud (for example, credit card and benefit fraud) - is increasingly prevalent, suggesting that the connection between low-level crime and terrorism is not simply a marriage of convenience.

Furthermore, just as cash couriers and money remittance businesses present challenges to the authorities as funding moves outside formal channels, so the advent of 'fintech' (financial technology) solutions that offer fast, secure, and cheap means of moving funds will present further security challenges as they proliferate, taking money transfer business away from the banks. Likewise, the growth of the darknet and access to anonymised cryptocurrencies such as Bitcoin will increasingly provide terrorists and criminals with access to currency transfer outside the formal, regulated system.

Finally, the response set available to the authorities is considerably more powerful and extensive than it was at the time of the 2001 attacks. The financial services sector, stretching from global banks and money service businesses to local and regional foreign exchange bureaux, has been co-opted into the CTF architecture through greater awareness, and has been delegated the responsibility for policing financial borders and money flow by domestic and international

authorities.

Big data capabilities enable these financial institutions to track and monitor financial flows, seeking anomalies within transaction data in an attempt to root out terrorist and criminal activity. The use of 'financial intelligence' to investigate plots and identify malicious actors is increasingly common as law enforcement and security authorities conduct network analysis to connect persons of interest with support networks and facilitators.

This was identified by former UK prime minister Gordon Brown (2007-10) following the disruption of the transatlantic liquid bomb plot in 2006. He claimed that financial intelligence would be to the 21st century what fingerprints were to the 19th century or DNA analysis was to the 20th - one of the "most powerful investigative and intelligence tools available in the fight against crime and terrorism".

Conclusion

Since the 2001 terrorist attacks, CTF has featured as a central plank of global counter-terrorism and security efforts. Regular passing of CTF-related UN Security Council resolutions has reminded member states of the importance of disrupting terrorist financing; the Financial Action Task Force's (FATF's) evaluations have driven up technical compliance and highlighted shortcomings and failures; the EU's anti-money laundering directives, in particular the upcoming 4th Directive, have introduced a growing number of disclosure and reporting measures that seek to close loopholes identified through terrorist attacks; and banks and other designated non-financial businesses and professions have built increasingly substantial systems and processes, and invested substantially in technology and people, in an effort to contribute to CTF efforts.

However, as the Australian Transactions, Reports, and Analysis Centre (AUSTRAC) observed in its 2014 terrorist financing report, terrorist financing is dynamic - unlike money laundering with which it is often erroneously conflated - and requires entities seeking to identify and disrupt related financial flows to update their processes and procedures regularly in response to evolving global and domestic events. Yet banks cannot do this alone.

As the 9/11 Commission's Monograph on Terrorist Financing acknowledged in 2004, "Although financial institutions lack information that can enable them to identify terrorists, they have information that can be absolutely vital in finding terrorists." Similarly, as underlined by Richard Barrett, former co-ordinator of the UN Al-Qaeda and Taliban Monitoring Team, "States cannot expect the private sector to have a better idea of what terrorist financing looks like than the states themselves," particularly when modern technology is increasingly moving money flows out of traditional banking channels.

In the face of an evolving threat and a widening array of terrorist financing opportunities, the integrity of the financial system and its ability to disrupt terrorist financing will only be maintained by institutional co-operation, information-sharing, and the development of effective partnerships.

GENESIS OF CTF Following the 1998 terrorist attacks on the US embassies in Kenya and Tanzania, the United Nations took two important steps: first, in October 1999 it adopted UN Security Council Resolution 1267, which called upon the Taliban to hand over then Al-Qaeda leader Osama bin Laden for indictment in the US for the embassy bombings; second, it introduced the International Convention for the Suppression of the Financing of Terrorism.The convention stated, "Any person commits an offense within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out [terrorist acts]...". However, the low priority given to CTF by the global community before the 11 September 2001 attacks was illustrated by the fact that, at the time the attacks happened, only four states - Botswana, Sri Lanka, the UK, and Uzbekistan - had actually adopted this convention.This lack of focus changed rapidly after the 2001 attacks as the FATF, hitherto the leader of the global effort to tackle money laundering, developed an extensive architecture of 'Recommendations' aimed at obliging nations to take steps against terrorist financing. The FATF was established at the 1989 G7 summit to lead efforts against criminal money laundering, most notably related to international drug production and trafficking.Its original mandate had been to highlight money-laundering risks, review national and international disruption efforts, and propose improvements at a national and international level. However, after the 2001 terrorist attacks on the US, the international community turned to the FATF as the logical body for co-ordinating and implementing a global effort to raise standards for combating terrorist financing.Adding to its existing 40 Recommendations aimed at tackling money laundering, the FATF's nine Special Recommendations for CTF demanded the ratification and implementation of relevant UN conventions and resolutions, the criminalising of terrorist financing, the application of asset-freezing measures, and greater monitoring for possible terrorist financing abuse of charities, cash couriers, and wire transfers. Fifteen years after the terrorist attacks in 2001, even though some states still lag, this effort has led to a considerable raising of standards as technical compliance with the FATF's Recommendations has advanced across the globe.The FATF's Recommendations, guidance, and evaluations have led countries to establish financial intelligence units (FIUs). Moreover, almost all countries have criminalised terrorist financing, and co-opted banks and other so-called 'designated non-financial businesses and professions' into the security architecture by imposing a requirement on them to report suspicious activity and transactions related not only to money laundering, but also to terrorist financing.The regular evaluation by the FATF of countries' compliance with its Recommendations ensures that failures and omissions are publicly exposed. Ahead of the November 2015 G20 Leaders summit, the FATF conducted a review of the CTF regimes in place in 194 countries, concluding that, "Almost all jurisdictions - particularly the systemically important jurisdictions - have criminalised terrorist financing as a distinct offence."However, although standards and technical compliance have been raised, financing appears as central as ever to terrorists' operations. This applies to large groups such as the Islamic State that, controlling territory, operate state-like financing models including tax-raising and resource exploitation, as well as to lone actors and small cells that use fraud and draw on financing provided by consumer finance products such as payday loans.As the FATF noted in its study for the G20 Leaders meeting, "relatively few jurisdictions have obtained convictions for terrorist financing" and although states have legal instruments in place to implement targeted financial sanctions, use of these tools by most jurisdictions is rare. In its 'unprecedented session' of ministers of finance in December 2015, held in the shadow of the attacks in Paris a month earlier, the UN Security Council expressed concern at the lack of implementation of previous, key CTF Security Council resolutions as it passed resolution 2253. In sum, although technical compliance has improved, the implementation of CTF disruption measures appears far from effective.To address this gap between technical compliance and effective implementation, the FATF has expanded its evaluation methodology. Since 2012, it has assessed countries not only for compliance with its Recommendations, but also for the effective implementation of its standards.Evaluations of effectiveness only began in 2014, but it already appears that there are material gaps in many countries between technical compliance and effective implementation, challenging countries to develop a genuinely disruptive response to terrorist financing that goes beyond the superficial passing of laws.

Related Articles
EU combats dirty money with new directive Russian money-laundering put under pressure **Author** Tom Keatinge is Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute, London.