Social Media and Terrorist Financing: Time for a Focused Response

Tom Keatinge and Florence Keen

Social media has attracted scrutiny as a tool for promoting extremism. Its power to support terrorist financing requires equal attention.

In recent months, social media companies such as Facebook, Twitter and YouTube have found themselves in the spotlight as global leaders and policymakers have pressured them to do more to combat terrorism. In early August, UK Home Secretary Amber Rudd travelled to California to address the Global Internet Forum to Counter Terrorism and told service providers that '[T]he responsibility for tackling this [terrorism] threat at every level lies with both governments and with [the social media] industry'.

This echoed the 2017 G7 Leaders' Taormina Statement on the fight against terrorism and violent extremism that committed to 'combat the misuse of the Internet by terrorists', urging 'Communication Service Providers and social media companies to substantially increase their efforts to address terrorist content … promoting incitement to violence'.

Social media has grown to be a highly effective tool for those seeking to raise funding for causes they promote, be they positive and socially aware, or extremist. Social media has considerable power to spread awareness of ideas and campaigns, attract followers to a particular cause and solicit their support in the form of material funds.

Activists of all types take advantage of the power of social media. Whether they are charities raising funds for drought relief, individuals soliciting sponsorship for their charitable endeavours or terrorist organisations and their supporters gathering funds, social media has become an integral and indispensable element of fundraising campaigns. In the case of Islamist extremist and terrorist financing, the combination of support for 'the cause', religious messaging and social media have proved to be a powerful means of raising funds. Finance is the lifeblood of any terrorist organisation and thus the combination of social media and the need for finance (however great or small) is a new front in counterterrorist financing (CTF) that deserves greater attention.

Terrorist fundraisers' move online does not represent a threat just for law enforcement and security authorities to counter. It also presents opportunities for identification and disruption for those in both the public and private sectors charged with monitoring for suspicious activity related to terrorist financing. Conversations once held offline and in private are now online and, at least initially, in less private forums.

> *For Islamist extremist and terrorist financing, the combination of support for 'the cause', religious messaging and social media have been a powerful means of raising funds*

As this article will explore, the use of social media as a terrorist financing tool – either overtly or via deception that takes advantage of unwitting charitable support – calls for a dedicated response. This response must recognise the opportunities inherent in exploiting social media intelligence in assisting with the gathering of financial information needed to develop a clearer picture of terrorist fundraising methodologies and developing strategies to disrupt their finances.

Together with law enforcement and security authorities, social media companies must also ensure they are aware of and comply with their obligations as potential tools via which terrorist groups and their followers can source material support.

Social Media: A Powerful Fundraising Tool

The rise of social media has been a boon to the voluntary sector, which has harnessed its promotional power to great effect, contributing to the rapid rise in the use of online means of fundraising by charities. The average size of online donations increased by 20% in the UK between 2010 and 2014. Effectively deployed, social media can significantly enhance the success of any form of fundraising campaign. As demonstrated by their sophisticated use of social media, terrorist groups such as Daesh (also known as the Islamic State of Iraq and Syria, or ISIS) are highly skilled at capitalising on the power of social media.

They follow the strategy that would be recommended for use by any group seeking to promote its cause online, including:

- The importance of identifying the target audience and developing a clear understanding of the social media platforms they use.
- Employing links to websites, photos and videos to engage with potential supporters and create an impact on platforms that often limit space for text (for example, Twitter limits posts to just 140 characters).

A still image taken from a Daesh propaganda video showing militants firing a light machine gun during a firefight in Salaheddin province in Iraq, June 2016. Terrorist groups suchs as Daesh are highly skilled in using social media to promote their ideology and raise funds. *Courtesy of PA Images*

- Conveying urgency by providing real-time updates on the cause being promoted (again, photos and videos can be powerful in this regard), the progress the campaign is making, and the remaining donations needed to meet the fundraising goal.
- Focusing on the impact that each donation will have by linking it to a specific deliverable (for example, every £100 donated will vaccinate a certain number of children).
- Including a 'call to action', exhorting followers to become 'an army' and promote the campaign to their own contacts and followers, undertaking their own fundraising efforts.

An October 2015 report from the Financial Action Task Force (FATF, the global anti-money laundering and counterterrorist finance standard-setter), Emerging Terrorist Financing Risks, provides some insight into the unwitting role social media plays in terrorist financing. It notes that:

> *The widespread access to and anonymity of the Internet and especially the rapid expansion of social media, have been exploited by terrorist groups to raise funds from sympathetic individuals globally and represents a growing TF [terrorist finance] vulnerability.*

This vulnerability of social media parallels and supports the extensive use terrorist organisations make of such platforms to promote their propaganda and achievements. As FATF further notes:

> *Social networks are being also used [sic] to coordinate fundraising campaigns. Large-scale and well-organised fundraising schemes aimed at TF may involve up to several thousand 'sponsors' and may raise significant amounts of cash.*

The almost limitless access provided by social media and the population of 'followers' gathered by many leading Daesh supporters in particular, and jihadist preachers more generally, supports this claim. This broad audience provides preachers and financiers with a powerful platform from which to call for material support for terrorist groups, legitimised by Islamic texts that support their call for funding and the 'financing of jihad'.

The concept of '*Tajheez Al-Ghazi*' calls on those such as women, who are less able to join the physical fight, to achieve the reward of waging jihad by funding fighters. The Daesh online magazine *Rumiyah* also exhorts the use of personal wealth to assist with the waging of jihad and using wealth 'in order to prepare equipment and arm the troops'. In contrast to physical fighting, from which some are exempt, there is no excuse 'for anyone whom Allah has enriched from His bounty and who has yet to spend'.

Fundraising campaigns promoted via social media in the early stages of the Syrian conflict employed this approach. For example, a Ramadan Campaign in Kuwait in 2013 intended 'to prepare 12,000 jihadists for the sake of Allah'. Posters for the campaign promised that $2,500 would equip one fighter for battle. Another campaign reported by the *New York Times* was called 'Wage Jihad with Your Money' and promised 'silver status' for those that gave $175 for 50 sniper bullets, or 'gold status' for those generous enough to give $350 for eight mortar rounds. And a further campaign, reported by the *Washington Post,* called for donations of $2,400 to fund the travel, arming and training of foreign fighters.

With social media usage unlikely to decrease, different fundraising tactics will only grow in the coming years

Many more examples exist of social media being employed to promote campaigns that either overtly call for material terrorist support or which, via charities that indicate that donations will be used for humanitarian activity, use funds to support designated terrorist organisations. With social media usage unlikely to decrease, this tactic will only grow in the coming years. This is why it is so important that the platforms themselves increase their understanding of terrorist financing methodologies, and implement processes that specifically target and disrupt bad actors on their networks.

Taking Responsibility

There is no doubting the power of social media to promote causes in support of fundraising campaigns. There is also no doubting the expertise with which those who support terrorist organisations have harnessed the power of social media to encourage supporters to either willingly or unwittingly support their activities with donations, often underpinning their calls for finance with Islamic texts.

However, as mentioned earlier, the move online of terrorist financing operations presents opportunities for law enforcement, security and intelligence services, and private sector actors to develop deeper knowledge of these financing networks. The use of social media by Daesh and other terrorist groups has provided a 'unique window' into the networks of terrorists and their supporters. Such insight can be valuable in the development of disruption strategies; it also allows for the creation and targeting of counter-narrative strategies that are essential in any counterterrorism response. Social media intelligence is proving to be not only practical in terms of insight and counter-narratives, but is beginning to demonstrate tangible disruptive capabilities. For example, the Israel Defense Forces' algorithms monitor the social media accounts of suspects and their networks, looking for terrorist warning signs prior to attacks.

Since the 9/11 attacks, tackling terrorist financing has been a cornerstone of the global effort to combat terrorism. As terrorists' financing strategies evolve, so too should the response of all involved in the disruption effort, including both public and private sectors. One particular element of this initiative is the use of financial intelligence (FININT) to map and connect networks of individuals providing support to terrorist actors. Taking this work online and using the finance-related footprints left by those raising funds for terrorist organisations is an obvious way by which the CTF response should evolve.

The idea of exploiting social media intelligence as a source of information to support the integrity of the financial system is not new. In 2013, FATF identified social media as a means of financial institutions verifying the accuracy of customers' declarations regarding their sources of wealth. A discrepancy, for example, between declared wealth and online evidence, could be evidence of criminality. The Canadian financial intelligence unit, FINTRAC, also reportedly scrutinises Facebook and other social media platforms in order to enhance their financial intelligence picture. FINTRAC's spokesperson Renée Bercier stated:

> *It is important to remember that the perpetrators of these crimes [money laundering and terrorist financing] have an online presence and actively use the web, including social media to connect with associates, facilitate their activities, and in the case of terrorism financing, even raise funds.*

FinTech companies are also demonstrating innovation with regard to social media intelligence; it is clear that social media screening forms a core part of these platforms' financial crime risk management, monitoring sites such as Facebook, LinkedIn and Twitter to gather information on customers and conducting necessary due diligence checks to ensure the platform is not being used for financial crime purposes.

Law enforcement agencies increasingly use social media intelligence when conducting investigations. Digital policing is on the rise, in particular when investigating missing persons and cases of child sexual exploitation. However, the validity and reliability of social media activity has deterred both banks and government authorities such as financial intelligence units (FIUs) from incorporating social media intelligence (SOCMINT) fully into investigations; the resources required to analysis and assess SOCMINT are also considerable and thus deter extensive use of this tool.

As with the offline world, where partnerships between financial institutions and governments are flourishing in an attempt to create a more effective approach to tackling financial crime, so too is partnership critical if law enforcement and security authorities are effectively going to disrupt the use of the online world for criminal and terrorist activity.

Social media platforms are being unwittingly exploited by terrorists in planning, communicating or equipping their activities, yet they are seemingly immune from the level of responsibility placed on FATF-obliged entities, such as banks. This lack of enforced obligation presents security vulnerabilities.

It would be unfair to suggest that social media companies take no action. For example, from July to December 2016, Twitter suspended 376,890 accounts for violations related to the promotion of terrorism, identified primarily by its own filtering systems. Facebook has a team removing and investigating terrorist content. Furthermore, the online payments services provided by social media companies employ financial crime compliance specialists to ensure sanctions and counterterrorist legislation are not being contravened and like banks, file suspicious activity reports with national FIUs.

From July to December 2016, Twitter suspended 376,890 accounts for violations related to the promotion of terrorism

Despite this, these service providers do not seem to be as alert to the risks of providing material support as the financial services industry, which has learnt from experience as a result of significant enforcement action for failing to comply with sanctions issued by the UN or national bodies, such as the US Treasury Department's Office of Foreign Assets Control.

Bypassing a Risk Rendezvous

David Cohen, then deputy head of the CIA and Assistant Secretary for Terrorist Financing in the US Treasury Department, noted in March 2014 that 'fundraisers can now use social media handles instead of face-to-face solicitations, and sympathetic donors can bypass a risky rendezvous in favor of a simple and remote hashtag search'. Social media has significantly changed the terrorist financing landscape, necessitating an updating of the status quo. Facebook and Twitter were not created until 2004 and 2006 respectively, well after the 9/11 attacks established the current approach to CTF.

Combatting terrorist financing is a collaborative and joint responsibility of the public and private sectors. To date, the private sector contribution to this effort has been dominated by the banking and remittance industries, but as social media is increasingly revealed as playing a valuable role in the provision of material support to terrorists and their supporters, it is clear that more needs to be done by both governments and social media companies to adapt CTF strategies to the online environment.

The role of social media as a tool through which terrorist groups have promoted their extremist narratives has been intensely scrutinised over the past twelve to eighteen months. Similar scrutiny has not been applied to the role social media has played in supporting the fundraising ambitions of terrorist groups. This oversight needs to be addressed as intelligence gleaned from the finance-related social media activity of terrorists and their supporters could prove invaluable in the investigation and disruption of those planning terrorist activity.

However, for this to happen, urgent steps must be taken to establish partnerships between government authorities and social media companies that focus not just on addressing the high-profile role social media plays in promoting extremist messaging, but also the valuable CTF opportunity inherent in combining financial and social media intelligence.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI

Florence Keen
Research Analyst, Centre for Financial Crime and Security Studies, RUSI