**Royal United Services Institute**
for Defence and Security Studies

Global Research Network on Terrorism and Technology: Paper No. 10

# Social Media and Terrorist Financing

## What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?

Tom Keatinge and Florence Keen

# Recommendations

- Social media companies should recognise the political importance of counterterrorist financing (CTF) by explicitly reflecting the priorities of the UN Security Council and the Financial Action Task Force (FATF) in their policies, strategies and transparency reports.
- Furthermore, social media companies identified as being at high risk of exploitation should update their terms of service and community standards to explicitly reference and outlaw terrorist financing (consistent with universally applicable international law and standards such as those of the FATF) and actions that contravene related UN Security Council resolutions and sanctions.
- Social media companies should clearly demonstrate that they understand and apply appropriate sanctions designations; at the same time, policymakers should ensure that sanctions designations include, where possible, information such as email addresses, IP addresses and social media handles that can support sanctions implementation by social media companies. The more granular the information provided by governments on designated entities, the more efficiently the private sector can comply with sanctions designations.
- Social media companies should more tightly control functionality to ensure that raising terrorist funding through social media videos, such as big-brand advertising and Super Chat payments, is disabled.
- Researchers and policymakers should avoid generalisations and make a clear distinction between forms of social media and the various terrorist-financing vulnerabilities that they pose, recognising the different types of platforms available, and the varied ways in which terrorist financiers could abuse them.
- Policymakers should encourage both inter-agency and cross-border collaboration on the threat of using social media for terrorist financing, ensuring that agencies involved are equipped with necessary social media investigative capabilities.
- International law enforcement agencies such as Interpol and Europol should facilitate the development of new investigation and prosecution standard operating procedures for engaging with operators of servers and cloud services based in overseas jurisdictions to ensure that necessary evidence can be gathered in a timely fashion. This would also encourage an internationally harmonised approach to using social media as financial intelligence.
- Policymakers should encourage the building of new, and leveraging of existing, public–private partnerships to ensure social media company CTF efforts are informed and effective.

## Context and Project Rationale

Social media – as with most digital technologies – enables previously onerous tasks to be undertaken more cheaply at scale and at speed. One such field in which the enabling role of social media is on display is fundraising. As one law enforcement interviewee (from 15 interviews conducted with representatives from law enforcement, international agencies, government stakeholders and social media companies in Israel, Indonesia, Singapore and the UK) observed, the ability of social media to 'industrialise' fundraising campaigns is immense.[1] Shaking an 'electronic tin' to solicit donations is considerably more effective than fundraising on street corners or in places of worship. This has led to growing concerns about the potential abuse of social media for fundraising for criminal purposes – including terrorist financing. The instant reach and wide geographic scope of certain platforms paired with the potential for user anonymity opens opportunities for individuals to anonymously donate funds to terrorist groups without leaving their homes.

In the wake of recent terrorist incidents, including in Christchurch, New Zealand,[2] and the Easter Sunday attacks launched across multiple locations in Sri Lanka,[3] social media companies have attracted further calls from policymakers to do more to block or remove terrorist and extremist-related content from their platforms.[4] Moreover, there is a growing body of existing,[5] forthcoming[6] and proposed[7] domestic and supranational regulation, including the European Commission proposal on preventing the dissemination of terrorist content online, that will introduce financial penalties if content is not taken down within a short, defined time period.[8] In

1. Authors' interview with law enforcement official, Singapore, 9 April 2019.
2. *BBC News*, 'Christchurch Shootings: 49 Dead in New Zealand Mosque Attacks', 15 March 2019.
3. Newley Purnell, 'Sri Lankan Islamist Called for Violence on Facebook Before Easter Attacks', *Wall Street Journal*, 30 April 2019.
4. Kim Willsher, 'Leaders and Tech Firms Pledge to Tackle Extremist Violence Online', *The Guardian*, 15 May 2019; Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, <https://www.christchurchcall.com/>, accessed 22 May 2019; Emily Birnbaum, 'Dems Slam "Vague" Explanations by Tech Firms on Extremist Content', *The Hill*, 5 May 2019.
5. Germany's 'Network Enforcement (NETZDG) Act 2019', German Law Archive, <https://germanlawarchive.iuscomp.org/?p=1245>, accessed 22 July 2019.
6. Australian Government, 'Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019', <https://www.legislation.gov.au/Details/C2019A00038>, accessed 31 May 2019.
7. HM Government, *Online Harms White Paper*, CP 57 (London: The Stationery Office: April 2019).
8. European Commission, 'Proposal for a Regulation Of The European Parliament And Of The Council On Preventing The Dissemination of Terrorist Content Online: A Contribution From the European Commission to the

turn, social media companies themselves are making significant investments in capabilities that take down terrorist and extremist content and remove groups and individuals for violating their terms of service.[9]

The purpose of this paper is not to rehearse discussions around the merits of content removal;[10] rather, it focuses on the narrow issue of terrorist financing enabled by social media and the current, or potential, public–private collaboration for the purposes of CTF. As argued in a previous study conducted by the Global Research Network on Terrorism and Technology (GRNTT),[11] propaganda is not the sole way in which terrorists exploit social media networks; other risks include the raising and transfer of funds, exacerbated by the rise of internet crowdfunding campaigns and the growing integration of financial technology into social media platforms via peer-to-peer transactions.

The move of terrorist operations online (including for terrorist financing) may however present law enforcement with opportunities – from offering greater intelligence to enabling disruption. However, despite the recognised value of social media intelligence (SOCMINT)[12] in counterterrorism efforts, comparatively little attention has been given to its potential role in CTF.[13] This paper explores this gap.

---

Leaders' Meeting in Salzburg on 19-20 September 2018', COM(2018) 640 final, 12 September 2018, <https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF>, accessed 18 July 2019.

9. See, for example, Global Internet Forum to Counter Terrorism (GIFCT), 'Actions to Address the Abuse of Technology to Spread Terrorist and Violent Extremist Content', 15 May 2019, <https://www.gifct.org/press/actions-address-abuse-technology-spread-terrorist-and-violent-extremist-content/>, accessed 20 July 2019.
10. For a recent summary of these merits, see Andrew Glazzard, 'Shooting the Messenger: Do Not Blame the Internet for Terrorism', *RUSI Newsbrief* (Vol. 39, No. 1, January/February 2019).
11. Florence Keen, 'Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes: What can be Learnt from Efforts on Terrorist Financing?' Paper No. 1, Global Research Network on Terrorism and Technology (GRNTT) and RUSI, January 2019.
12. David Omand, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence and National Security* (Vol. 27, No. 6, 2012), pp. 801–23.
13. Examples include Nic Ryder, 'Counter-Terrorist Financing, Cryptoassets, Social Media Platforms and Suspicious Activity Reports: A Step into the Regulatory Unknown', Research Seminar, Centre for Financial and Corporate Integrity, Coventry Law School, 20 March 2019; Scott F Butler, 'Disrupting Terrorist Financing on Social Networks and Video Platforms: A Guide for Non-Traditional

## Methodology

This paper is the output of a three-month research project conducted by RUSI's Centre for Financial Crime and Security Studies, under the umbrella of the GRNTT. The research builds on the Centre's past work on public–private collaboration to counter the use of the internet for terrorist purposes,[14] and on the role of SOCMINT in CTF efforts.[15]

It draws on:

- A review of existing regulation and collaboration as relates to social media and CTF efforts conducted by the authors.
- Fifteen semi-structured, non-attributable interviews conducted between February and May 2019 with representatives from law enforcement, international agencies, government stakeholders and social media companies in Israel, Indonesia, Singapore and the UK.[16]

The team selected Israel and Indonesia as case-study countries for interview fieldwork to provide two perspectives, as both have particular experiences of terrorism and terrorist financing and have demonstrated an interest in exploiting SOCMINT as a disruption tool – with Indonesia specifically discussing its use in CTF efforts in a private white paper.[17]

Both countries are also home to GRNTT partners,[18] with which the authors engaged during the research visits. While findings from each country are specific to that country, the authors have attempted to draw on these lessons to develop policy recommendations that can be applied to a global

---

Financial Institutions and the Banks That Hold Their Accounts', AML White Paper, Association of Certified Anti-Money Laundering Specialists, 2017.

14. Keen, 'Public Private Collaboration to Counter the Use of the Internet for Terrorist Purposes'.
15. Tom Keatinge and Florence Keen, 'Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool', *Studies in Conflict and Terrorism* (Vol. 42, No. 1–2, 2018), pp. 178–205.
16. Although Singapore and the UK were not specific case-study countries, transit through Singapore en route to Indonesia and the RUSI office location in London offered opportunities to conduct interviews with additional subject-matter experts. Engaging in semi-structured interviews ensured that the findings were not limited to pre-determined assumptions.
17. A 2017 White Paper produced by Indonesia's anti-money-laundering agency (PPATK) and its national counterterrorism agency (BNPT), although not publicly available, was widely reported on in the regional press, see, for example, Wahyudi Soeriaatmadja, 'Donations Via Social Media Now Main Source of Terrorism Funding in Indonesia', *Straits Times*, 18 October 2017.
18. The International Institute for Counter-Terrorism (ICT) in Israel and the Institute for Policy Analysis of Conflict (IPAC) in Indonesia.

audience. This is particularly important, given the use of social media for terrorist financing purposes is not confined within national boundaries.

This paper focuses on forms of social media that present identified terrorist-finance risks, including networking sites (such as Facebook), content-hosting services (such as YouTube), crowdfunding services (such as GoFundMe), and encrypted communications services (such as Telegram and WhatsApp).

## Social Media and Terrorist Finance: A Varied Picture

Assessing the scale and impact of terrorist financing through social media is challenging for a number of reasons, most notably due to the secretive way in which terrorists and related fundraisers operate, including through their use of encryption. This paper thus does not attempt to quantify the amount of money raised or number of terrorists/sympathisers engaging in this tactic, nor does it assert that it is the most significant tool used by those terrorists to raise and transfer funds.

Nevertheless, an understanding of the terrorist financing vulnerabilities inherent to social media and the identification gaps and deficiencies in the response – within both public and private sectors – is important, particularly as the risk may increase as terrorists innovate in response to the squeezing of their currently favoured methods.[19]

In recent years, discussion around the terrorist financing vulnerabilities of social media has become more focused, disaggregating types of social media and the varying degrees of risk. A joint 2019 report from the Asia/Pacific Group (APG) on Money Laundering and the Middle East and North Africa Financial Action Task Force (MENAFATF)[20] used 27 case studies to outline three types of social media that may be vulnerable to terrorist financing:[21]

- **Social networking and content-hosting services**. These are used to solicit donations and to promote terrorism through propaganda

19. For more on innovation in terrorist finance, see Tom Keatinge and Kerstin Danner, 'Assessing Innovation in Terrorist Financing', *Studies in Conflict & Terrorism*, 14 January 2019, doi:10.1080/1057610X.2018.1559516.
20. The Asia/Pacific Group on Money Laundering (APG) and Middle East and North Africa Financial Action Task Force (MENAFATF) are known as 'FATF-style regional bodies', two of the nine bodies which represent and promote the FATF standards on combatting money laundering, the financing of terrorism and the financing of proliferation of WMD in countries that are not members of the FATF itself. The FATF is the global standard setter for anti-money laundering and counterterror financing and currently comprises 37 member jurisdictions and 2 regional organisations.
21. APG and MENAFATF, 'Social Media and Terrorism Financing', January 2019.

and radicalisation. Due to limited integration of payment methods in these services, the report reveals that donated funds are moved using traditional payment methods such as banks.

- **Internet communication services**. These are used to privately communicate with campaigners or terrorist groups. The vulnerabilities of these services, in particular encrypted communication and the number of active users, are factors driving their abuse for terrorist financing.
- **Crowdfunding services**. These can be abused by campaigns disguising the use of funds for humanitarian causes and are often integrated with new payment services, which may hinder terrorist financing detection and investigation by competent authorities.[22]

This is a useful lens through which to investigate the problem, making the important distinction between different forms of social media and the different vulnerabilities that they pose. One expert interviewee noted that 'overt' calls to donate funds via social media were often perceived to be a law enforcement trap, resulting in greater caution from terrorist sympathisers.[23]

According to officials from the Canadian Financial Intelligence Unit (FINTRAC), crowdfunding services pose a 'significant challenge' when trying to identify suspected terrorist transactions, due to the lack of information available in electronic transfer reports.[24] The confluence of social media, crowdfunding and charitable giving thus presents a significant challenge. In Indonesia, there are several examples of charitable social media campaigns to raise funds to support the families of convicted terrorists, such as 'ADC' and 'Infaq Dahwar', which, despite being a legitimate cause, raises concerns regarding who monitors the end use of the funds and the extent to which they may be diverted to support further terrorist activity.[25]

## Social Media and Charitable Giving

Charitable giving has been repeatedly abused in order to finance terrorism,[26] with recent cases associated with the conflicts in Iraq and Syria. In 2016, Adeel Ul-Haq was convicted in the UK of a terrorist-financing offence involving the solicitation of donations via Twitter in support of humanitarian aid convoys.[27] The abuse of charities to promote extremism and terrorism has long been

22. *Ibid*., p. 1.
23. Authors' interview with counterterrorism researcher, Jakarta, 12 April 2019.
24. Alexandra Posadzki, 'Detecting Terrorism Financing in Crowdfunds Poses "Significant Challenge": Fintrac Report', *Global News,* 18 May 2017.
25. Authors' interview with counterterrorism researcher, Jakarta, 10 April 2019.
26. Tom Keatinge and Florence Keen, *Humanitarian Action and Non-State Armed Groups: The Impact of Banking Restrictions on UK NGOs*, Chatham House Research Paper (London: Royal Institute of International Affairs, 2017).
27. UK Government, 'Charity Commission Today Welcomes Conviction of Individual for Terrorist Offences', press release, 10 February 2018, <https://

recognised by actors including the FATF through its Recommendation 8, which requires that the laws and regulations that govern non-profit organisations be reviewed so that these organisations cannot be abused for the financing of terrorism.[28] In the UK, the Charity Commission provides specific guidance on protecting charities from abuse for extremist purposes.[29] This kind of guidance may also lend itself to social media companies attempting to tackle the vulnerabilities posed by charitable giving on their platforms.

In addition, there are a number of examples of crowdfunding via social media in which supporters are encouraged to donate using cryptocurrency. While this paper does not deal with the terrorist-financing risks of cryptocurrency,[30] as the authors have previously judged this risk as low, it is important to recognise the potential for abuse as it was mentioned by a number of interviewees in Israel and Indonesia. Former intelligence officers in Israel stated that, as Daesh (also known as the Islamic State of Iraq and Syria, ISIS) has become more decentralised, its reliance on cryptocurrency may grow, given it lacks the resources it had when it controlled territory.[31] This remains somewhat speculative with the potential threat evolving. One government official in Israel emphasised that they were not yet seeing the popular take-up of fundraising via cryptocurrency on social media,[32] while in Southeast Asia there appears to be greater evidence of the use of cryptocurrency.[33] In light of Facebook's recent announcement of plans to launch its own cryptocurrency 'Libra',[34] the convergence of social media and cryptocurrency is inevitably attracting considerable scrutiny and remains an area to watch regarding the potential for terrorist-financing abuse.[35]

---

www.gov.uk/government/news/charity-commission-today-welcomes-conviction-of-individual-for-terrorist-offences>, accessed 4 July 2019.

28. See Financial Action Task Force (FATF), 'Combating the Abuse of Non-Profit Organisations (Recommendation 8)', Best Practices report, June 2015.
29. UK Charity Commission, 'Guidance, Chapter 5: Protecting Charities from Abuse for Extremist Purposes', 19 November 2018, <https://www.gov.uk/government/publications/protecting-charities-from-abuse-for-extremist-purposes/chapter-5-protecting-charities-from-abuse-for-extremist-purposes>, accessed 18 July 2019.
30. See Tom Keatinge, David Carlisle and Florence Keen, 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses: Counter-Terrorism', European Parliament TERR Committee Study, 2018.
31. Authors' interview with former Israeli intelligence officers, Tel Aviv, 27 February 2019.
32. Authors' interview with Israeli government official, Jerusalem, 26 February 2019.
33. Authors' interview with leading counterterrorism academic, Singapore, 11 July 2019.
34. Josh Constine, 'Facebook Announces Libra Cryptocurrency: All You Need to Know', *Tech Crunch*, 20 June 2019.
35. See, for example, the recent US Senate Banking Committee hearing, 'Examining Facebook's Proposed Digital Currency and Data Privacy Considerations', 16 July 2019, <https://www.banking.senate.gov/hearings/

A further concern is that of the money terrorists may earn through big-brand advertising under their popular videos. As a *Times* newspaper investigation revealed in 2017, companies including Mercedes Benz, Waitrose and Marie Curie appeared on posts by Daesh and UK extreme right-wing group Combat 18 – which, according to the investigation, could generate 'thousands per month', due to the revenue earned per 1,000 views.[36] Furthermore YouTube's 'Super Chat' feature enables users to raise funds through subscribers paying money to have their questions answered. According to a 2018 *BuzzFeed* investigation, this has proved a lucrative model for prominent far-right and white-nationalist figures.[37] While this is not terrorist financing, it nevertheless constitutes a vulnerability that could be exploited by bad actors.

**Supporting the Syrian Conflict**

There is a growing body of open-source evidence of terrorist abuse of social media for fundraising. In its early stages, this form of terrorist financing manifested in overt calls (including the provision of bank account details) on social media to donate funds, as seen in 2013, a year before Daesh announced its caliphate in Syria and Iraq. Private donors were reported to have used sites including Twitter to solicit funds and provide payment instructions, in what officials described as 'crucial backing for Islamist militias in northern and eastern Syria', with campaigns asking for pledges to pay for weapons or finance specific operations.[38]

In 2014, former US Under Secretary for Terrorism and Financial Intelligence David Cohen noted that charitable fundraising networks in the Gulf collected 'hundreds of millions of dollars through regular fundraising events held at homes or mosques and through social media pleas'.[39] In 2015, FATF identified social media as an emerging terrorist-financing risk, citing the use of networks in 'coordinating fundraising campaigns' with schemes that involve 'up to several thousand "sponsors" and may raise significant amounts of cash'.[40]

---

examining-facebooks-proposed-digital-currency-and-data-privacy-considerations>, accessed 20 July 2019.

36. Alexi Mostrous, 'Big Brands Fund Terror Through Online Adverts', *The Times*, 9 February 2017.
37. Ishmael N Daro and Craig Silverman, 'How YouTube's "Super Chat" System is Pushing Video Creators Toward More Extreme Content', *BuzzFeed*, 17 May 2018.
38. Joby Warrick, 'Private Donations Give Edge to Islamists in Syria, Officials Say', *Washington Post,* 21 September 2013.
39. US Department of the Treasury, 'Remarks of Under Secretary for Terrorism and Financial Intelligence, David Cohen, Before the Center for a New American Security on "Confronting New Threats in Terrorist Financing"', 4 March 2014, <https://www.treasury.gov/press-center/press-releases/pages/jl2308.aspx>, accessed 18 July 2019.
40. FATF, 'Emerging Terrorist Financing Risks', October 2015.

Both the 2015 and updated 2018 US National Terrorist Financing Risk Assessment reports draw attention to this risk, noting respectively that social media is used to reach potential donors[41] and that terrorist groups and their supporters 'aggressively use social media to identify followers … and solicit financial or other forms of material support'.[42] A 2016 Camstoll Group report collated additional case studies of individuals operating on multiple social media platforms who were designated as terrorists by the US and the UN and therefore subject to sanctions. These included Salafi Sheikh Hajjaj bin Fahd Al-Ajmi and Sheikh Abdullah Muhammad Al-Muhaysini, who both raised funds to support the Al-Nusrah Front, a Syrian jihadist group aligned to Al-Qa'ida.[43] Unlike financial institutions and others in the regulated sector, it is apparent that screening for sanctioned entities as part of compliance procedures is not consistent practice across the social media sector, as is further discussed in this paper.

## The Picture in Indonesia and Israel

### Indonesia

The role of social media in terrorist financing in Indonesia has attracted intense scrutiny, with the threat of social media-enabled terrorist financing considered to be high. In 2017, a private white paper produced by Indonesian government counterterrorism agencies noted a changing trend in fundraising methods for terrorist activities, terrorists and terrorist organisations, from the use of non-profit organisations in 2013–2015 to the use of social media.[44] The white paper credits this change to two primary factors: the convenience in opening a social media account that allows people to use a false identity or the identity of others, creating problems in identification and tracking; and wider coverage of the distribution of information, resulting in a potentially substantial amount of funds received. According to the white paper, the impact of social media has been considerable as it has caused the trend in terrorist financing to move from illicit activity (especially motorbike theft) to non-criminal fundraising methods, including the payment of dues by members of terrorist organisations, donations through social media, and self-funding.

41. US Department of the Treasury, 'National Terrorist Financing Risk Assessment', 2015, p. 16, <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf>, accessed 18 July 2019.
42. US Department of the Treasury, 'National Terrorist Financing Risk Assessment 2018', p. 2, <https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf>, accessed 18 July 2019.
43. Mark Nakhla, 'Terrorist Financing and Social Media', The Camstoll Group, December 2016, <https://www.un.org/sc/ctc/wp-content/uploads/2016/12/TCG_Social-Media-TF_11DEC161.pdf>, accessed 31 May 2019.
44. Author interview with law enforcement officer, Jakarta, 10 April 2019.

This threat was underlined by the recently published APG Mutual Evaluation Report (MER) on Indonesia which stated that: 'the use of social media to call for and facilitate donations has increased';[45] that the authorities in Indonesia view the 'use of social media to solicit funds as high risk for TF [terrorist financing]';[46] and that '[r]ecent investigations have also involved funds linked to social media'.[47] In response to this threat, Indonesia's National Strategy 2017–2019 for Anti-Money Laundering and Countering the Financing of Terrorism (STRANAS) has introduced a new action plan on increasing the effectiveness of supervision related to the misuse of social media for terrorist financing.[48] The MER also reveals that the authorities in Indonesia have gathered information from social media in support of terrorist-financing investigations that were not connected to terrorist attacks.[49]

## Israel

Although the authors encountered numerous general references to the use of social media by terrorists and counterterrorism authorities in Israel,[50] in contrast to the extensive reference made to social media and terrorist financing in Indonesia's MER, the December 2018 MER on Israel produced jointly by FATF and MONEYVAL[51] contains not a single reference. Indeed, references to the risks (of money laundering or terrorist financing) posed by modern technology are also limited.

This is not to say that the risks posed by new technologies are ignored by the Israeli authorities. A 2017 report, 'Promoting Use of Advanced Means of Payment in Israel', published by the Bank of Israel, emphasises the role that new technologies can play in reducing the size of the Israeli shadow/cash economy and thus reducing the risk of money laundering while at the same time recognising that these technologies may be abused for

45. APG, 'Anti-Money Laundering and Counter-Terrorist Financing Measures – Indonesia: Mutual Evaluation Report', October 2018, p. 16.
46. *Ibid*., p. 28.
47. *Ibid*., p. 61.
48. *Ibid*., p. 29.
49. *Ibid*., p. 62.
50. See, for example, Ministry of Public Security, 'Study: Terrorists Post Info on Social Media Before Attacking', 12 June 2018, <https://www.gov.il/en/Departments/news/study_on_lone_wolf_terror_phenomena_120618>, accessed 9 July 2019; *Times of Israel*, 'Police Minister: Social Media Monitoring has Foiled 200 Terror Attacks', 12 June 2018, <https://www.timesofisrael.com/police-minister-social-media-monitoring-has-foiled-200-terror-attacks/>, accessed 9 July 2019.
51. MONEYVAL is the FATF-style regional body responsible for Council of Europe countries that are not members of the main FATF body.

laundering funds from illicit activities or financing terrorism.[52] The report also notes that payments made with modern technology leave an electronic trace – in contrast to cash – including an IP address or other leads that investigators can follow. While social media does not feature prominently, the report does offer examples of modern technologies that provide alternative payment channels, such as Apple Pay, Samsung Pay, Google's electronic wallet, the PayPal and Alipay e-commerce services and payment services using social media, such as through Facebook.[53]

## A Need to Recognise International Standards

Since 2001, terrorist financing has been universally criminalised, led by UN Security Council resolutions[54] and the implementation of domestic legislation.[55] The FATF has issued specific CTF recommendations and guidance since 2001. The regulated sector, including banks and money-service businesses, are under strict obligations to report suspicious activity that relates to terrorist financing to domestic financial intelligence units, and to comply with international and domestic sanctions obligations, including the UN, the US and the EU – or risk significant fines.

Organisations such as charities previously identified as vulnerable to abuse for terrorist financing[56] are likewise subject to scrutiny and oversight[57] to minimise this risk. In contrast to a general awareness of terrorist financing in these industry sectors, the potential role of social media in terrorist financing is less well understood or acknowledged than in other sectors, despite the evidence that social media is vulnerable to terrorist-financing activity, as described earlier. A heightened awareness in other sectors is due in large part to the coercive effect of the legal obligations placed on financial

52. Bank of Israel, 'Final Report: The Committee for Promoting the Use of Advanced Means of Payment in Israel', June 2017, p. 29, <https://www.boi.org.il/en/NewsAndPublications/PressReleases/Documents/Finalreport.pdf>, accessed 18 July 2019.
53. *Ibid.*, p. 9.
54. See, for example, the most recent counterterror financing UN Security Council Resolution 2462 (2019), passed in March 2019, <http://unscr.com/en/resolutions/doc/2462>, accessed 11 May 2019.
55. See, for example, 'Israel: Law No. 5765-2004, Prohibition on Terrorist Financing Law', 2004; 'Indonesia – Prevention and the Suppression of Terrorist Financing, Law No. 9, 2013'.
56. FATF, 'Combating the Abuse of Non-Profit Organisations (Recommendation 8)', June 2015.
57. See Charity Commission for England and Wales, 'Protecting Charities from Harm: Compliance Toolkit', Chapter 1, Module 7, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/568815/Chapter1_Module7.pdf>, accessed 12 May 2019.

services – failing to meet these obligations can result in major fines and reputational damage.[58]

This is not to say that there is no focus on terrorist financing by social media companies. For example, Facebook's Community Standards do not allow 'coordination of support for any of the [proscribed] organisations or individuals or any acts committed by them',[59] although there is no explicit reference to the requirement to combat terrorist financing as internationally mandated by the UN. Neither is any specific reference made to restrictions related to UN Security Council resolutions and sanctions.[60] In contrast, Facebook's Community Standards explicitly outlaw statements connected with money laundering.[61]

Similarly, although Twitter's terrorism and violent extremism policy outlaws affiliating with and promoting the illicit activities of a terrorist organisation or violent extremist group, including 'providing or distributing services (e.g., financial, media/propaganda) to further a terrorist organization's or violent extremist group's stated goals',[62] no explicit mention is made of terrorist financing or the various UN-mandated restrictions. YouTube restricts

58. For example, in 2012, HSBC admitted to anti-money-laundering and sanctions violations and was fined $1.2 billion in a deferred prosecution agreement, see US Department of Justice, Office of Public Affairs, 'HSBC Holdings Plc. And HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement', 11 December 2012, <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations>, accessed 31 May 2019; and in 2014, BNP Paribas agreed to plead guilty and pay $8.9 billion for illegally processing financial transactions for countries subject to US economic sanctions, see US Department of Justice, Office of Public Affairs, 'BNP Paribas Agrees to Plead Guilty and to Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to U.S. Economic Sanctions', <https://www.justice.gov/opa/pr/bnp-paribas-agrees-plead-guilty-and-pay-89-billion-illegally-processing-financial>, accessed 31 May 2019.
59. Facebook Community Standards, '2. Dangerous Individuals and Organizations, Policy Rationale', <https://www.facebook.com/communitystandards/dangerous_individuals_organizations>, accessed 12 May 2019.
60. For the implementation of sanctions by technology companies, see Chris Meserole and Daniel Byman, 'Terrorist Definitions and Designations Lists: What Technology Companies Need to Know', Global Research Network on Terrorism and Technology, No. 7, RUSI, July 2019.
61. Facebook Community Standards, '4. Coordinating Harm, Policy Rationale', <https://www.facebook.com/communitystandards/coordinating_harm>, accessed 5 July 2019.
62. Twitter Rules, 'Terrorism and Violent Extremism Policy', March 2019, <https://help.twitter.com/en/rules-and-policies/violent-groups>, accessed 5 July 2019.

terrorism-related references to excluding the posting of footage depicting the aftermath of attacks.[63] And Telegram only restricts the promotion of violence on 'publically [sic] viewable Telegram channels'.[64] Although Telegram states in its Privacy Policy that if it receives a court order confirming that an accountholder is a 'terror suspect' it may disclose the accountholder's IP address and phone number to the relevant authorities, it notes that 'so far, this has never happened'.[65]

The terms and conditions of the crowdfunding site GoFundMe places responsibility on its users for content they upload, noting prohibition of the use of its services to raise funds for a number of crimes including terrorism, entities subject to US and other economic sanctions, and the funding of ransom, human-trafficking or exploitation.[66] This overt recognition of international obligations is in contrast to a sample of other crowdfunding sites researched, including JustGiving, Kickstarter, Fundly and Crowdrise,[67] who, while having rules relating to user conduct around the prohibition of obscene, defamatory or libellous content, do not mention the final destination of funds, nor the responsibility to ensure that funds do not circumvent sanctions or end up in the hands of bad actors. However, it is unclear how GoFundMe reports prohibited activity to law enforcement, given the explicit statement on its website that it is an administrative platform, 'not a broker, agent, financial institution, creditor, or … nonprofit corporation'.[68]

Social media companies thus vary significantly in their acknowledgement of terrorist-financing risks and demonstrate a varied understanding of international and domestic obligations to combat them. This would in part be addressed if social media companies screened for international and domestic designated entities (where appropriate[69]) and prevented them from abusing

63. YouTube, 'Violent or Graphic Content Policies', updated 2 July 2019, <https://support.google.com/youtube/answer/2802008?hl=en>, accessed 12 May 2019.
64. Telegram, 'Terms of Service', <https://telegram.org/tos>, accessed 12 May 2019.
65. Telegram, 'Privacy Policy: 8. Who Your Personal Data May Be Shared With', <https://telegram.org/privacy#8-3-law-enforcement-authorities>, accessed 12 May 2019.
66. GoFundMe, 'GoFundMe Terms & Conditions', last updated 20 May 2019, <https://www.gofundme.com/terms>, accessed 20 July 2019.
67. Just Giving, 'Just Giving's Terms of Service', <https://www.justgiving.com/info/terms-of-service-versions/terms-of-service-march-2019>, accessed 22 July 2019; Kickstarter, 'Terms of Use', <https://www.kickstarter.com/terms-of-use accessed>, 22 July 2019; Fundly, 'Fundly Terms of Use', <https://fundly.com/terms-of-use>, accessed 22 July 2019; Crowdrise, 'Terms and Conditions', <https://www.crowdrise.com/about/terms>, accessed 22 July 2019.
68. GoFundMe, 'GoFundMe Terms & Conditions', <https://uk.gofundme.com/terms>, accessed 22 July 2019.
69. Given the global footprint of larger social-media companies, there are geographies in which a sanctions designation is not recognised by the

their platforms to raise funds. In turn, governments should help the sector by providing them with context around why a group or individual has been designated, and with granular information such as email and IP addresses that would assist them in identifying bad actors using their platforms. As argued by Meserole and Byman, the technology sector, civil society and government could work together to develop a global, unbiased and real-time database of possible terrorist entities.[70]

## Public–Private Sector Collaboration on Terrorist Financing

Despite the role social media platforms may play in facilitating terrorist financing, the commitment to applying international sanctions and seeking to identify and disrupt financing activity is less explicit than in other sectors to which terrorists turn to facilitate fundraising, such as banks or charities. It is therefore unsurprising that interviews with social media companies and law enforcement agencies charged with identifying and disrupting terrorist financing suggest that CTF engagement is most often reactive on both sides, developing only when a terrorism investigation case is underway. One interviewee went as far as suggesting that social media companies 'refuse to cooperate' and only act when their rules – that they themselves define – are broken. This interviewee asserted further that anomalies in activity that are of use to security agencies are not tracked or reported by the social media companies, and that there is a need for regulations for the relationship to evolve.[71] Equally, there are indications that the private sector is often open to working with law enforcement counterparts, but does not receive adequate input in return. One representative of a social media platform based in Indonesia noted that their experience with law enforcement was 'mixed', with some agencies open to engaging with them and others unresponsive.[72] Ultimately, the relationship between the two sectors will inevitably vary between countries, and therefore it is hard to generalise.

Interviews in Israel and Indonesia with law enforcement and security professionals indicate that connections between government agencies and social media companies are most often maintained by cybersecurity units rather than counterterrorism units (and certainly not units responsible for identifying and investigating terrorist financing). However, clearly there is

government. The authors recognise that social-media companies must rightly remain sensitive to the political environments in which they operate, and acknowledge that it will not always be possible to comply with sanctions designations writ large.

70. Meserole and Byman, 'Terrorist Definitions and Designations Lists'.
71. Authors' interview with government security professional, Jerusalem, February 2019.
72. Authors' interview with policy head of a social media platform's Indonesian office, Jakarta, February 2019.

scope for greater inter-agency cooperation on this threat, and the need to incorporate SOCMINT into the traditional CTF response to ensure all relevant data is exploited.

Furthermore, security authorities appear to place their emphasis on terrorist propaganda, rather than the potential of social media to enable funding of groups subject to sanction, at times made by individuals who are also themselves identified and designated as terrorist actors by governments or the UN.[73]

The relationship between public and private sectors will inevitably vary by country, and it is important to recognise that often this form of interaction may not be viable in countries with fewer democratic processes. However, there appears to be a growing appetite for greater collaboration, with the Paris 'No Money for Terror' Conference in April 2018 calling for 'more active cooperation from the tech industry, including major Internet and social media platforms, with financial intelligence units, law enforcement, intelligence and investigation services, to counter terrorism financing' as well as the need for 'the tech industry, including major Internet and social media platforms, to adopt robust guidelines for the use of crowd-financing, payment services and community guidelines'.[74]

In addition, as social media facilitates cross-border communication, this provides another imperative for national law enforcement agencies to actively collaborate across borders and partner with counterterrorism agencies internationally to disrupt identified social media-enabled fundraising activity.

## Conclusion

Global bodies such as the FATF continue to assess terrorist financing-related risks and the disruptive measures employed by countries, including the timely implementation of sanctions. Industry sectors that are vulnerable to abuse by terrorist financiers also attract close scrutiny, and while it is certainly not the central fundraising tool employed by terrorist groups, the ability of social media to amplify calls for funding is a clear threat that needs to be addressed. Whereas in the pre-internet era, terrorist and insurgent groups relied to a greater extent on state sponsorship or support solicited via word of mouth, the internet has facilitated calls for funding to reach individuals

73. See, for example, Keatinge and Keen, *Humanitarian Action and Non-State Armed Groups*; APG and MENAFATF, 'Social Media and Terrorism Financing'.
74. *France Diplomatie*, 'Final Statement - International Conference on Combating the Financing of Daesh and Al-Qaeda (Paris, 25-26.04.18)', <https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/events/article/final-statement-international-conference-on-combating-the-financing-of-daesh>, accessed 19 July 2019.

sympathetic to a cause who are far from a terrorist group's area of operation, supplementing or obviating their reliance on state sponsorship.

Although the current threat should not be exaggerated, it is important to monitor and track its development in light of terrorists' demonstrated ability to innovate and their interest in new technologies to further their aims. This can only be effective through the increased knowledge and understanding derived from public–private sector collaboration.

## Recommendations

The social media industry's engagement with CTF appears less vigorous than that of other sectors, such as charities, that have facilitated fundraising. This is a position that is attracting scrutiny from bodies charged with implementing and assessing the global CTF regime. Therefore eight recommendations are offered to assist policymakers and social media companies to engage more effectively with the global imperative of identifying and disrupting terrorist financing:

- Social media companies should recognise the political importance of CTF by explicitly reflecting the priorities of the UN Security Council and FATF in their policies, strategies and transparency reports.
- Furthermore, social media companies identified as being at high risk of exploitation should update their terms of service and community standards to explicitly reference and outlaw terrorist financing (consistent with universally applicable international law and standards such as those of FATF) and actions that contravene related UN Security Council resolutions and sanctions.
- Social media companies should clearly demonstrate that they understand and apply appropriate sanctions designations; at the same time, policymakers should ensure that sanctions designations include, where possible, information such as email addresses, IP addresses and social media handles that can support sanctions implementation by social media companies. The more granular the information provided by governments on designated entities, the more efficiently the private sector can comply with sanctions designations.
- Social media companies should more tightly control functionality to ensure that raising terrorist funding through social media videos, such as big-brand advertising and Super Chat payments, is disabled.
- Researchers and policymakers should avoid generalisations and make a clear distinction between forms of social media and the various terrorist-financing vulnerabilities that they pose, recognising the different types of platforms available, and the varied ways in which terrorist financiers could abuse them.
- Policymakers should encourage both inter-agency and cross-border collaboration on the threat of using social media for terrorist financing,

ensuring that agencies involved are equipped with necessary social media investigative capabilities.

- International law enforcement agencies such as Interpol and Europol should facilitate the development of new investigation and prosecution standard operating procedures for engaging with operators of servers and cloud services based in overseas jurisdictions to ensure that necessary evidence can be gathered in a timely fashion. This would also encourage an internationally harmonised approach to using social media as financial intelligence.
- Policymakers should encourage the building of new, and leveraging of existing, public–private partnerships to ensure social media company CTF efforts are informed and effective.

*Tom Keatinge is the Director of RUSI's Centre for Financial Crime and Security Studies.*

*Florence Keen is a Research Fellow in RUSI's Centre for Financial Crime and Security Studies.*

**About RUSI**

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

**About The Global Research Network on Terrorism and Technology**

The Global Research Network on Terrorism and Technology is a consortium of academic institutions and think tanks that conducts research and shares views on online terrorist content; recruiting tactics terrorists use online; the ethics and laws surrounding terrorist content moderation; public–private partnerships to address the issue; and the resources tech companies need to adequately and responsibly remove terrorist content from their platforms.

Each publication is part of a series of papers released by the network on terrorism and technology. The research conducted by this network will seek to better understand radicalisation, recruitment and the myriad of ways terrorist entities use the digital space.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel), and the Institute for Policy Analysis of Conflict (Indonesia).

The research network is supported by the Global Internet Forum to Counter Terrorism (GIFCT). For more information about GIFCT, please visit https://gifct.org/.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.




**Royal United Services Institute**
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)