Royal United Services Institute
for Defence and Security Studies

Global Research Network on Terrorism and Technology: Paper No. 1

# Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes

## What Can be Learnt from Efforts on Terrorist Financing?

Florence Keen

## Policy Recommendations

- Lawmakers developing a regulatory regime for communication service providers (CSPs) should engage with their counterparts involved in the response to terrorist financing to understand potential unintended consequences of this regime, including counterproductive incentives, risk displacement and other factors identified in this paper.
- Regulations should be developed with input from the CSP sector, to avoid counterproductive measures such as over-reporting, a tick-box approach to compliance, and discrimination against smaller entities that may have fewer resources to commit to regulatory compliance.
- As a complement to regulations, policymakers and CSPs should identify all areas in which public–private collaboration could strengthen the response to the terrorist use of online communication services (including but not limited to the removal of terrorist content).
- The various areas for collaboration should be articulated in a comprehensive strategy clarifying their role relative to overarching counterterrorism objectives and distinguishing between different threat actors.
- When developing and implementing collaborative models (including existing partnerships), public and private partners should consider the following factors: (1) legal and practical gateways for sharing information; (2) flexible membership; (3) transparency and accountability; (4) voluntary nature; (5) clear relationship with regulatory framework.
- Information sharing should initially focus on the sharing of common and emerging trends, best practices and redacted case studies, as opposed to sharing operational information. This will allow members from multiple jurisdictions to participate while ensuring that legal barriers to information sharing are not breached.

## Context and Rationale for the Project

- In response to the **use of social media and other online communication services for terrorist purposes**, such as recruitment, communication service providers (CSPs) face growing expectations to proactively detect, remove and/or report terrorist content. We have used the Gartner definition of CSPs,[1] and for the purposes of this paper have focused

[1] The Gartner definition of CSPs includes all service providers offering telecommunication services or some combination of information and media services, content, entertainment and applications services over networks, leveraging the network infrastructure as a rich, functional platform. CSPs include the following categories: telecommunications carrier, content and applications service provider, cable service provider, satellite broadcasting operator, and cloud communications service provider. See Garter IT Glossary,

on providers of internet-based services such as social media platforms, search platforms and media content platforms.

- The **new regulations** announced by the European Commission in September 2018 are illustrative of a global trend,[2] which includes the introduction of a legally binding one-hour content removal deadline following an order from competent authorities, and financial failure-to-comply penalties.
- The emerging regulatory regime governing CSPs features significant **parallels with global efforts to protect the financial system from terrorist financing** (TF). Under counterterrorist financing (CTF) rules, financial institutions must take measures to prevent the use of their services for terrorist purposes and to report suspicious activities to financial intelligence units.
- There is a growing body of academic and policy literature that focuses on the **effectiveness of the CTF regime** and the ways in which TF has evolved in recent years.[3] Additionally, the emerging trend towards public–private collaboration is increasingly recognised as an important tool in detecting and disrupting a broad range of financial crimes, including TF. Initiatives such as the UK's Joint Money Laundering Intelligence Task Force (JMLIT)[4] and the Netherlands' Task Force on Terrorism Financing[5] are illustrative of this form of partnership, and therefore provide a useful evidence base when considering the development of public–private collaboration within the CSP space.

'CSP (Communications Service Provider)', <https://www.gartner.com/it-glossary/csp-communications-service-provider>, accessed 15 January 2019.

[2] European Commission, 'State of the Union 2018: Commission Proposes New Rules to Get Terrorist Content Off the Web', IP/18/5561, press release, 12 September 2018, <http://europa.eu/rapid/press-release_IP-18-5561_en.htm>, accessed 20 November 2018.

[3] See, for example, Nicholas Ryder et al., 'The Financial War on Terrorism: A Critical Review of the United Kingdom's Counter-Terrorist Financing Strategies' in Colin King, Clive Walker and Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2008), pp. 781–806; Tom Keatinge, Florence Keen and Anton Moiseienko, 'From Lone Actors to Daesh: Rethinking the Response to the Diverse Threats of Terrorist Financing', *RUSI Newsbrief* (Vol. 38, No. 1, 23 January 2018).

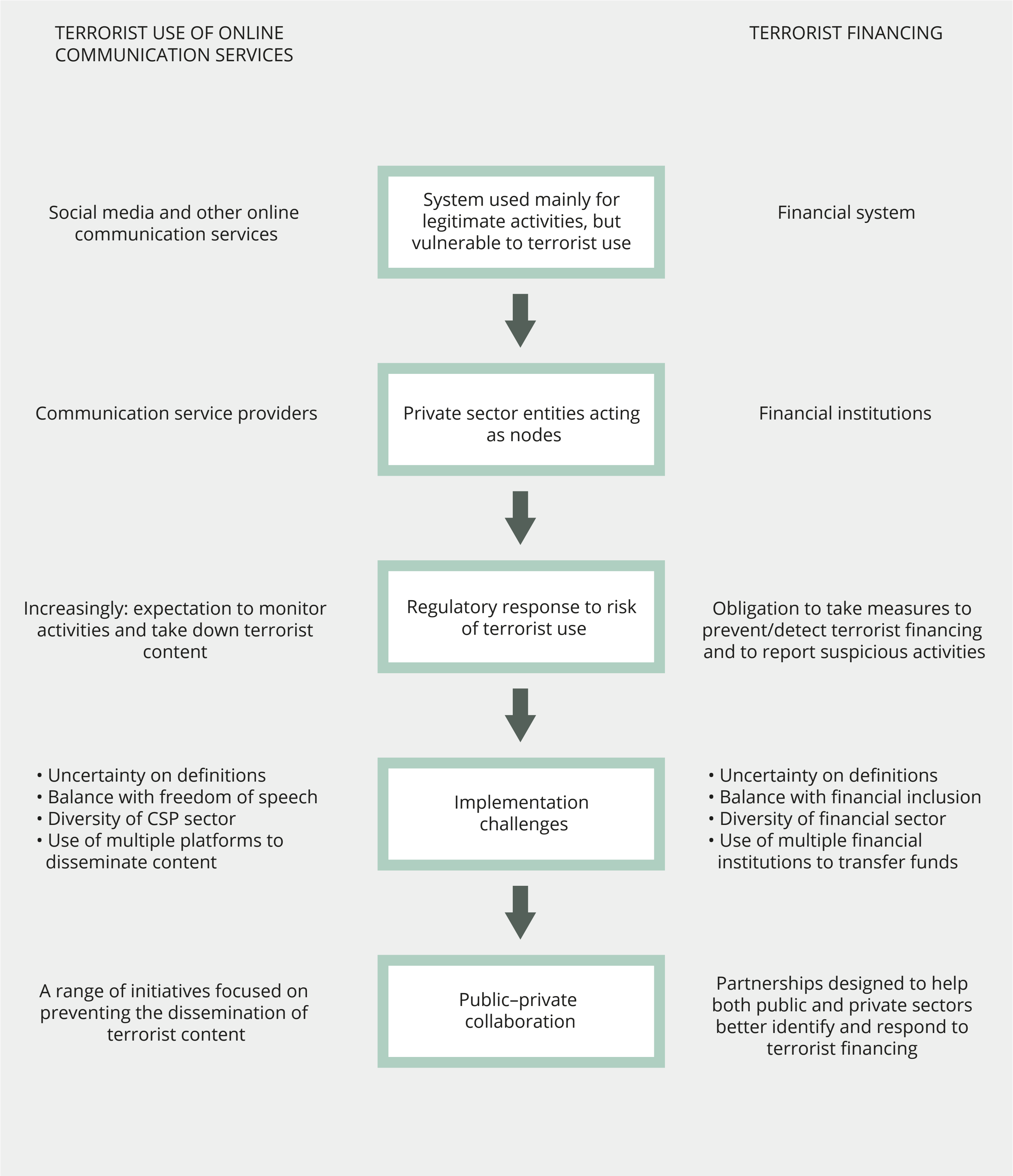
[4] National Crime Agency, 'Joint Money Laundering Intelligence Taskforce (JMLIT)', <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit>, accessed 24 November 2018.

[5] See Financial Intelligence Unit-  the Netherlands, 'FIU–the Netherlands Annual Report 2017', p. 31, <https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/7238-fiu_jaaroverzicht_2017_eng_web_1.pdf>, accessed 24 November 2018.

- Figure 1 summarises similarities and differences between the **role of private sector entities in responding to terrorist uses of online communication services, and to TF**. It is meant to give a high-level overview of the two models and does not reflect all nuances of national approaches.

Notwithstanding inherent differences between the two sectors, there are clear benefits in **taking lessons learnt from longstanding efforts on TF into account when developing a response to the online terrorist threat**. This coordination is becoming even more critical with the **integration of CSPs and the financial sector**, as in the case of peer-to-peer payments conducted over social media platforms.

**Figure 1:** Similarities and Differences Between the Role of Private Sector Entities in Responding to Terrorist Uses of Online Communication Services, and to TF



TERRORIST USE OF ONLINE COMMUNICATION SERVICES

TERRORIST FINANCING

Social media and other online communication services

System used mainly for legitimate activities, but vulnerable to terrorist use

Financial system

Communication service providers

Private sector entities acting as nodes

Financial institutions

Increasingly: expectation to monitor activities and take down terrorist content

Regulatory response to risk of terrorist use

Obligation to take measures to prevent/detect terrorist financing and to report suspicious activities

- Uncertainty on definitions
- Balance with freedom of speech
- Diversity of CSP sector
- Use of multiple platforms to disseminate content

Implementation challenges

- Uncertainty on definitions
- Balance with financial inclusion
- Diversity of financial sector
- Use of multiple financial institutions to transfer funds

A range of initiatives focused on preventing the dissemination of terrorist content

Public–private collaboration

Partnerships designed to help both public and private sectors better identify and respond to terrorist financing

*Source: The author's research.*

# Method

This paper summarises the outcomes of a three-month research project conducted by RUSI's Centre for Financial Crime and Security Studies, under the umbrella of the Global Research Network on Technology and Terrorism. The research builds on the Centre's past work on the role of public–private partnerships in the disruption of crime and on CTF.[6] It also draws on:

- a comparative review of regulations applicable to CSPs;
- 12 semi-structured interviews conducted in July and August 2018 with CSPs, government, law enforcement and international agencies involved in the response to the online terrorist threat);
- a cross-sectoral workshop held at RUSI on 6 September 2018 with 25 representatives from government, law enforcement and the private sector involved in the response to either TF or the terrorist use of online communications services. It was organised in cooperation with Tech Against Terrorism.[7]

# Findings

The research team identified three areas where lessons learnt from the CTF context could benefit ongoing policy discussions on the response to the online terrorist threat:

- Potential unintended consequences of regulations
- Objectives for public–private collaboration
- Elements for collaborative models

### Potential Unintended Consequences of Regulations

**Recommendation 1:** The design of the response to the online terrorist threat should mitigate the risk of unintended consequences similar to those observed as a result of CTF regulations.

Based on RUSI's past work on CTF, potential unintended consequences of regulations may include:

- Regulatory pressure can create **counter-productive incentives**. In the financial sector, institutions concerned with failing to meet their CTF obligations have an incentive to file suspicious transaction reports to

[6] Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017); Keatinge, Keen and Moiseienko, 'From Lone Actors to Daesh'.

[7] See Tech Against Terrorism, 'About Tech Against Terrorism', <https://www.techagainstterrorism.org/>, accessed 25 August 2018.

be 'on the safe side' even when those reports are unlikely to have any real value for law enforcement. Such defensive reporting leads to an overwhelming number of reports that diverts resources from priority cases. These issues could be mitigated if regulations are designed with the input of CSPs from the outset, ensuring that regulators have a full understanding of the various CSP business models. In turn, CSPs should be **educated on the lessons learned from the CTF regime** about what constitutes useful information for law enforcement.

- An exclusive **focus on process-based compliance can distract from outcomes**. Supervision of financial institutions tends to focus on whether financial institutions follow processes that comply with regulations. This often leads to a tick-box approach, does not encourage financial institutions to take ownership of outcomes and favours the procedures that are focused solely on the avoidance of fines.
- Fines should only be levied if there is **clear evidence to support their use as a means of achieving desired outcomes**. As witnessed in the CTF context, fines are easily absorbed by larger financial institutions, and thus have little impact on the overall flow of terrorist funds across the formal financial sector.
- **High compliance costs and the fear of fines can deter smaller companies from operating within the regulated sector** and disclosing their activities. This must include an assessment of the resource and capability of individual CSPs to ensure that fines are commensurate to their business operations.
- Regulations can lead to **risk displacement** towards the most vulnerable parts of a sector, namely institutions with less developed controls. In some cases, consumers seeking to circumvent regulations deliberately turn to the weakest link. In other cases, institutions with strict controls deny services to entire groups of consumers that are considered high-risk, because the due diligence required would make the business relationship unprofitable for the institution. To mitigate for risk displacement, regulations should be harmonised across large and small entities, while ensuring that this does not price the latter out of business or prevent them from operating in certain jurisdictions.
- Regardless of compliance within the regulated sector, risk can also move to **new channels** outside the scope of regulations. For example, the regulations applied to financial institutions have led to the emergence of other forms of money laundering that do not involve financial transactions, but primarily involve trade. Like the appearance of virtual currencies in the financial sector, the blockchain technology could introduce new opportunities to disseminate terrorist content without the involvement of traditional CSPs.
- **Defining objectives too narrowly can skew the perception of effectiveness**. Similar to the focus on content takedown in the CSP context, CTF-related discussions and policies often focus exclusively on cutting off financial flows to terrorist groups and can therefore overlook other key parts of a comprehensive CTF strategy. For example, in the

case of self-funded cells and lone actors, using financial intelligence for counterterrorism purposes (for example, to understand how networks operate) is a more realistic and relevant response to TF than trying to prevent financial flows altogether. Yet, financial intelligence will only be fully leveraged if its use is recognised as a positive outcome of the CTF regime, alongside preventive measures. Similarly, while the takedown of terrorist content online is vital, it is also important to utilise the intelligence value of the content itself.

- **Internationally mandated regulations can be used by certain governments as a justification to crack down on civil society.** For example, the need to address TF risks in the charity sector has been invoked as a basis for disproportionate regulations that have hampered the ability of NGOs to operate effectively. Similarly, a disproportionate application of regulations against online terrorist propaganda can have a significant impact on free speech. This is particularly relevant for CSPs that operate globally and must remain sensitive to the political environments of multiple jurisdictions.

### Objectives for Public–Private Collaboration

**Recommendation 2:** As a complement to regulations, policymakers and CSPs should identify areas in which public–private collaboration could strengthen the response to the terrorist use of online communication services.

Based on past experience in the area of CTF, public–private collaboration will be crucial in developing and implementing a comprehensive response to the use of the internet by terrorist groups. The objectives for such cooperation should be designed with input from all relevant sectors from the outset but remain adaptable to the moving TF landscape. These objectives will vary among countries and over time, depending on the terrorist threat and the level of trust between authorities and relevant CSPs. Priority objectives identified during this research, and through RUSI’s past work on CTF, could include the following:

A. Agree a comprehensive strategy of public–private collaboration to respond to the terrorist use of online communication services.
   - This strategy should outline the precise form of public–private collaboration that is entailed, such as physical, periodic meetings to discuss common and emerging trends, and the sharing of best practices and redacted case studies as relates to the terrorist threat online. Reference to the UK’s JMLIT TF working group and the Netherlands’s TF Taskforce may provide useful examples of the various approaches that could be taken.
   - The response to the terrorist use of online communication services should not be reduced to one type of intervention, such as taking down terrorist content.

- To use available resources effectively, a comprehensive strategy should clarify the expected role of each measure relative to overarching counterterrorism objectives, bearing in mind that this role may vary depending on the threat actor.
- A strategy assigning clear responsibilities for each objective would also reduce the risk of duplication and help streamline communications.

B. Prevent terrorist propaganda.

- This is the area where public–private and industry collaboration has been most active to date, for example through Internet Referral Units that help social media companies identify content promoting terrorist activities, or through industry-led databases of hashes preventing the same terrorist content from being repeatedly uploaded (for example, the GIFCT database).
- Subject to appropriate vetting, sharing and consolidating contextual information would help CSPs monitor content in an effective and proportionate manner. Building on initiatives such as the Knowledge Sharing Platform developed by Tech Against Terrorism, this could include information on: the factors of radicalisation; reasons why a certain group is proscribed; which groups are active; whether any days of action are planned; which hashtags or slogans might be used; and symbolic content.

C. Address other ways in which terrorist groups can use online communication services.

- Propaganda is the primary, but not the sole, way in which terrorist groups use online communication services.
- Other risks include opportunities to raise and transfer funds, plan operations and collect intelligence. Assessing and addressing some of these risks may require collaboration with other actors, for example with the financial sector (including 'FinTechs') and law enforcement agencies focused on TF in the case of fundraising.
- The growing integration of financial technology into communication platforms, in particular via peer-to-peer (P2P) lending, may further exacerbate the TF vulnerabilities presented by the internet. By offering users the ability to transfer funds over their platform, companies are providing a financial service and should therefore be regulated and monitored accordingly to prevent terrorist abuse.

D. Gain a better understanding of the terrorist threat.

- The terrorist use of online communication services (like the terrorist use of the financial system) creates opportunities for law enforcement to gather intelligence on terrorist networks, propaganda methods, the exposure of certain geographic areas to propaganda, and other factors informing the terrorist threat assessment.

- Public–private collaboration can help ensure that intelligence is retained and can be exploited. However, enhanced collaboration will require a robust legal and oversight regime to address concerns relating, for example, to data protection, proportionality, consent, foreseeability and accountability.

E. Develop a coordination network that can be leveraged in the aftermath of an attack.

- In the case of an attack, CSPs can provide critical assistance to law enforcement to rapidly understand the profile and relationships of involved individuals. Partnerships focusing on CTF show that such post-crisis coordination requires personal relationships that are built over time and can be leveraged when needed.
- In addition to efforts targeting the terrorist use of CSPs, the same network can be used to coordinate an emergency response, for example, by relaying state communications or by providing practical assistance to the population.

### Elements For Collaborative Models

**Recommendation 3:** When developing and implementing collaborative models, public and private partners should consider the following factors: (1) legal and practical gateways for sharing information; (2) flexible membership; (3) transparency and accountability; (4) voluntary nature; (5) clear relationship with regulatory framework.

Based both on past experience in the CTF area and on challenges that are specific to the online terrorist threat, these elements are likely to enhance the effectiveness and sustainability of collaborative models in this area:

A. Legal and practical gateways for information sharing

- In the CTF context, public–private sharing of operational information relies on clear legal provisions (for example, section 314(a) of the US Patriot Act, or section 7 of the UK Crime and Courts Act 2013). A robust framework is also necessary for private-to-private sharing of personal data (for example, among financial institutions with exposure to the same criminal network). At the international level, the Egmont Group of Financial Intelligence Units allows for a more rapid exchange of information than traditional mutual legal assistance.

- Considering the global remit of most CSPs, a collaborative group will probably include actors from multiple jurisdictions, thus increasing the legal barriers to information sharing. It is therefore advisable that information sharing be initially limited to the sharing of common and emerging trends, best practices and redacted case studies, as opposed to operational information. If the group's remit expands, this topic should be addressed again.
- The effectiveness of collaboration also depends on the resources available to co-design common/compatible systems that allow partners to share data securely and efficiently. Public–private collaboration is still often hindered by technological obstacles.

B. Flexible membership

- The membership for every stream of public–private collaboration needs to be determined in light of the specific objective. Lead agencies should determine on a case-by-case basis which stakeholders need to (and can) be involved, and, for each member organisation, which expertise is needed – for example, policy, content moderation, or investigation.
- For certain streams, representatives from other sectors should be involved (for example, financial institutions in the case of TF risks on social media; civil society organisations, users and data protection authorities in the case of strategic discussions).
- Two-tier membership should be considered in areas of collaboration involving sensitive information, with a small group of actors conducting a joint analysis, and a larger group being notified of key findings (including typologies and trends) through alerts.

C. Transparency and accountability

- Public–private collaboration should be publicly announced, with endorsement from leaders in both the public and private sectors, and an explanation of the respective roles of all parties involved.
- To maintain the public's confidence, the format and mandate of any collaborative effort should be subject to a regular debate between members, other sectors, civil society and policymakers regarding the proportionality balance between outcomes on the one hand, and resource and privacy implications on the other.
- Additional safeguards should apply whenever personal data is shared.

D. Voluntary nature

- Public–private collaboration on CTF suggests that voluntary collaboration is the most likely to lead to positive outcomes, as all parties should participate in good faith.
- A voluntary model is likely to be less formal, which is important to encourage participation from smaller platforms.
- Voluntary collaboration can also be promoted by ensuring buy-in from users.

E. Clear relationship with regulatory obligations

- Public–private collaboration is not a full substitute for regulations.
- At the same time, the link between regulatory requirements and collaborative initiatives must be clear. In other terms, supervisors in charge of enforcing regulations should have a process to recognise a company's contributions to a public–private initiative, in order to encourage such contributions (especially for small companies with limited capacity).

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

*The author would like to thank all participants who shared their invaluable insights into the topic both in interviews and during the cross-sectoral workshop. She would also like to thank her former RUSI colleague Olivier Kraft, who was instrumental in delivering this project.*

**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 author, 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. RUSI is a registered charity (No. 210639).

**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)