Research report for external body :
Macdonald, S., Grinnell, D., Kinzel, A. & Lorenzo-Dus, N. (2019). *A Study of Outlinks Contained in Tweets Mentioning Rumiyah.*

Royal United Services Institute
for Defence and Security Studies

Crime and Security Research Institute
Sefydliad Ymchwil Trosedd a Diogelwch

Digital Economy Research Centre

Global Research Network on Terrorism and Technology: Paper No. 2

A Study of Outlinks Contained in Tweets Mentioning *Rumiyah*

Stuart Macdonald, Daniel Grinnell, Anina Kinzel and Nuria Lorenzo-Dus

This paper focuses on the attempts by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) to use Twitter to disseminate its online magazine, *Rumiyah*. It examines a dataset of 11,520 tweets mentioning *Rumiyah* that contained an outlink, to evaluate the success of Daesh's attempts to use Twitter as a gateway to issues of its magazine.

Key Findings

- The primary tactic that Daesh employed was to post outlinks to a large number of different file-sharing sites. Most of these sites were smaller platforms, such as justpaste.it. There was no evidence of Daesh seeking to signpost Twitter users to copies of *Rumiyah* available from repositories maintained by researchers or NGOs.
- Twitter was effective in its response to Daesh's attempts to use its platform as a gateway to *Rumiyah*. The majority of outlinks to a PDF of the magazine either no longer work or meet with a requirement for a subscription and/or password. Moreover, a high proportion of the user accounts that posted outlinks to PDFs of *Rumiyah* were suspended and the tweets that these accounts posted received relatively few retweets.
- Botnets were responsible for a significant number of the tweets. Almost one-third of the tweets were the product of the 'Reffy Botnet' (ref.gl). This is a URL shortener that is commonly used in networks of ill-intent. Accounts that use it are now suspended by Twitter.
- Roughly one-third of the tweets outlinked to news reports and coverage of *Rumiyah*. Some of this news coverage had the effect of amplifying the message contained in the magazine. This raises questions about the role of traditional news media in the dissemination of terrorist propaganda.

Summary of Recommendations

- Where possible, Global Internet Forum to Counter Terrorism (GIFCT) members should develop shared automated systems that use behavioural cues to block terrorist content.
- There is a pressing need to expand membership of the GIFCT.
- Dialogue is needed between the GIFCT and the news media regarding the use of social media to share news coverage that has the effect of amplifying the terrorist message.

Overview

In response to Daesh's 'Golden Age' on Twitter,[1] in late 2014 the platform began an aggressive campaign of suspensions. Since then, Daesh's presence on Twitter has diminished significantly, with much of its community-building activities moving to other platforms, particularly Telegram.[2] As Maura Conway and colleagues concluded in their 2017 report *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts*, today Daesh's Twitter activity 'has largely been reduced to tactical use of throwaway accounts for distributing links to pro-IS content on other platforms, rather than as a space for public IS support and influencing activity'.[3]

This paper builds on the findings of *Disrupting Daesh*, as well as two other publications to which some of the present authors contributed.[4] The latter work focused on the profiles of Daesh throwaway disseminator accounts. It found that these accounts were mostly recently established (often less than one day old at the time of suspension). They had very few followers (sometimes none) and received few retweets. Some sought to compensate for this lack of visibility by repeat posting. Here, the focus of this paper shifts to a different aspect of Daesh's strategy with analysis of the outlinks contained in tweets mentioning *Rumiyah* – to learn more about the types of content these throwaway accounts outlink to, and the platforms on which this content is stored. The paper evaluates Twitter's response to Daesh's attempts to use the platform as a gateway to *Rumiyah* magazine and concludes by offering practical recommendations.

[1] Maura Conway et al., *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts* (VOX-Pol Network of Excellence, 2017), p. 28.

[2] Nico Prucha, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram', *Perspectives on Terrorism* (Vol. 10, No. 6, 2016), pp. 48–58; Stuart Macdonald, Sara Giro Correia and Amy-Louise Watkin, 'Regulating Terrorist Content on Social Media: Automation and the Rule of Law', *International Journal of Law in Context* (Vol. 15, forthcoming).

[3] Conway et al., *Disrupting Daesh*, p. 30.

[4] Daniel Grinnell et al., 'Who Disseminates *Rumiyah*? Examining the Relative Influence of Sympathiser and Non-Sympathiser Twitter Users', paper presented at the 2nd European Counter Terrorism Centre Advisory Group conference, Europol Headquarters, The Hague, 17–18 April 2018, <https://www.europol.europa.eu/publications-documents/who-disseminates-rumiyah-examining-relative-influence-of-sympathiser-and-non-sympathiser-twitter-users>, accessed 18 June 2019; Daniel Grinnell, Stuart Macdonald and David Mair, 'The Response of, and on, Twitter to the Release of Dabiq Issue 15', paper presented at the 1st European Counter Terrorism Centre conference on online terrorist propaganda, Europol Headquarters, The Hague, 10–11 April 2017, <https://www.europol.europa.eu/publications-documents/response-of-and-twitter-to-release-of-dabiq-issue-15>, accessed 18 June 2019.

Methodology

Data was collected between 1 November 2016 and 31 October 2017 with Cardiff University's Sentinel research tool.[5] For the purposes of the study, a tweet was included in the dataset if it satisfied the following five criteria: (1) mentioned the term 'Rumiyah'; (2) was posted within 21 days of the release of a new issue of *Rumiyah*; (3) was posted from an account that used the English-language interface (US or UK); (4) contained original content (in other words, was not a retweet); and (5) contained an outlink. In addition, the publicly available user data of these posts was collected, as were the details of each post (including when it was posted), the onward distribution counts of these posts, and the account status (at the end of the data-collection period).[6]

The research dataset encompassed nine issues of *Rumiyah*.[7] It contained a total of 11,520 posts. These posts contained a total of 892 distinct links and were posted by a total of 1,493 distinct user accounts.

Outlinking to Where?

The outlinks in the 11,520 posts in the dataset contained a total of 244 different hostnames. Table 1 shows the 10 most common hostnames, respectively ordered by the number of posts, the number of distinct links containing the hostname and the number of distinct users that posted the outlink.

[5] Alun Preece et al., 'Sentinel: A Codesigned Platform for Semantic Enrichment of Social Media Streams', *IEEE Transactions on Computational Social Systems* (Vol. 5, No. 1, March 2018), pp. 118–31.

[6] For the purposes of this study, Sentinel functioned only as a repository of structured data supplied by the Twitter streaming application programming interface.

[7] These were issues 3, 4, 5, 7, 9, 10, 11, 12 and 13. Issues 1 and 2 were published before the study began. Issues 6 and 8 were excluded from the study owing to the research data capture infrastructure not collecting all relevant tweets for the entirety of the data collection period following the release of these issues.

Table 1: The URLs to Which the Outlinks Led: Top 10 Hostnames

By number of posts		By number of distinct links		By number of distinct users posting the outlink			
Hostname	**Total**	**Hostname**	**Total**	**Hostname**	**Extant**	**Suspended**	**Total**
ref.gl	3,733	ref.gl	84	drive.google.com	3	561	564
drive.google.com	1,634	memri.org	69	cloud.mail.ru	1	351	352
cloud.mail.ru	878	archive.org	58	cldup.com	3	291	294
justpaste.it	535	drive.google.com	54	archive.org	6	215	221
cldup.com	475	justpaste.it	39	1drv.ms	0	180	180
archive.org	464	facebook.com	29	dropbox.com	0	133	133
yadi.sk	417	4shared.com	19	yadi.sk	1	124	125
1drv.ms	336	cldup.com	17	pc.cd	0	102	102
jpst.it	329	siteintelgroup.com	15	4shared.com	0	70	70
dropbox.com	188	cloud.mail.ru	14	cloudup.com	1	60	61

Source: Authors' research.

Three important points emerged from Table 1. The first is the prevalence of file-sharing sites and smaller platforms. Sixteen different hostnames appear in Table 1, and of these, 11 are file-sharing sites. For both the first count (by number of posts) and the third count (by number of distinct users), nine of the top 10 hostnames are file-sharing sites. The exceptions are ref.gl and pc.cd. Second, a total of 2,102 distinct users posted the outlinks to the hostnames listed in the third count. Of these, 2,087 (99.3%) had been suspended by the end of the data-collection period. This high suspension rate strongly suggests that it was Daesh sympathisers who were posting outlinks to these file-sharing sites. Third, there is clear evidence of botnet activity. It is striking that ref.gl – which was top of each of the first two counts – does not feature in the third count at all. Known as the 'Reffy Botnet', ref.gl is a URL shortener that is commonly used in networks of ill-intent. In April 2018, all accounts using the ref.gl shortener were suspended by Twitter.[8] In the dataset, ref.gl was used in a total of 84 distinct links. These links appeared in a total of 3,733 posts (32.4% of the posts in the dataset). Just nine user accounts were responsible for these posts (and one of these accounts only posted a single tweet).[9] The tweets containing the Reffy Botnet were posted following the release of issues 10, 11, 12 and 13 of *Rumiyah* at an average rate of more than 50 tweets per day.

The hostname pc.cd also appeared to be connected to botnet activity. This hostname appeared in a total of 160 posts. These were all posted in the space of just over 25 hours,[10] by a total of 102 distinct user accounts (whose user names were randomised collections of letters). All of these user accounts were subsequently suspended.

Outlinking to What?

Table 2 breaks down the 892 distinct outlinks by the type of content each link led to. For those outlinks that no longer worked (for example, because the destination page had been removed or the hostname suspended), the type of content was determined by examining the text of both the URL and the post. Given the inherent limitations of relying on the wording of the URL and post, a distinction was drawn between categorisations in which there was a high degree of confidence and those in which there was only a moderate degree of confidence. As Table 2 shows, even after completing this process there remained a total of 29 outlinks that were so unclear that it was not possible to categorise them.

[8] Mike Farb, 'The Reffy Botnet', Medium, 29 April 2018, <https://medium.com/@unhackthevote/the-reffy-botnet-f8a7dc817e9a>, accessed 18 June 2019.

[9] The nine accounts were @MiddleBeast, @ExtremePropa, @ExtremistWatch_, @islamoinform, @JihadiInfo, @TabsTerror, @terror_history1, @terrorwatch1, and @VicPower87. The last of these was responsible for just one of the 3,733 tweets. All nine accounts have since been suspended.

[10] From 20:06 on 9 September 2017 to 21:26 on 10 September 2017.

Table 2: Types of Content Behind the Outlinks

Type of content	Number of distinct links (high confidence)	Number of distinct links (moderate confidence)	Total
Report/summary/information about *Rumiyah*	232	90	322 (36.1%)
PDF of *Rumiyah* (but no longer available)	79	228	307 (34.4%)
PDF of *Rumiyah* behind subscription or password protection	56	3	59 (6.6%)
Other content (not terrorism-related)	39	11	50 (5.6%)
Other content (terrorism-related)	27	4	31 (3.5%)
Academic analysis/writing	14	16	30 (3.3%)
Not possible to tell	-	-	29 (3.3%)
Picture of real *Rumiyah* issue	16	5	21 (2.4%)
Picture of fake *Rumiyah* issue	13	5	18 (2.0%)
PDF of *Rumiyah* (currently available)	15	0	15 (1.7%)
Suspicious ‘download’ button	5	0	5 (0.6%)
Fake issue of *Rumiyah*	5	0	5 (0.6%)
Total	501	362	892

Source: Authors’ research.

For a total of 322 outlinks, the type of content was report/summary/information about *Rumiyah*. This category consisted largely of news items either specifically about a new issue of the magazine or in which *Rumiyah* featured prominently. In the entire dataset, there were just three posts that were retweeted more than 50 times during the data-collection period.[11] All three outlinked to the same news item in the UK's *Daily Mail* newspaper, titled 'ISIS Calls on Islamists to Carry out Knife Attacks in Areas Such as Alleys, Forests and Quiet Neighbourhoods and Told to Aim for "a Reasonable Kill Count" in Latest Magazine'.[12] The *Daily Mail* was one of two UK newspapers that, in the aftermath of the recent Christchurch, New Zealand attack, posted the video of the attack on its website. This has raised concerns about the traditional news media, especially as it has been reported that the attack video only went viral after this happened.[13] The dataset for this report raises similar questions. For example, one outlink led to an item published by the UK's *Metro* newspaper in September 2016. It describes how Issue 1 of *Rumiyah* states that killing disbelievers is a form of worship to Allah, 'even the blood of the kafir street vendor selling flowers to those passing by'.[14] Below this is a photo of a market trader at a flower stall, which *Rumiyah*'s producers had apparently taken from the trader's website. *Rumiyah* offers no indication of the trader's name or the location of his flower stall. By contrast, the item in *Metro* names the trader and states the area in which his stall is located. A simple Google search reveals that several other UK newspapers ran a similar story, including a local newspaper that named the street in which the flower stall can be found. The effect of this news coverage was thus to amplify – and, importantly, to sharpen – the message contained in *Rumiyah*.

Table 2 also shows that a total of 381 of the outlinks led to a PDF of *Rumiyah*. Of these, 307 (80.6%) were no longer available, 59 (15.5%) were behind a subscription requirement or password protection, and just 15 (3.9%) led directly to the PDF. The 381 outlinks contained a total of 48 different hostnames, which are listed in Table 3. Table 3 also shows the number of

[11] There were only 22 posts that were retweeted 10 times or more. Four of these outlinked to password-protected copies of *Rumiyah*, one outlinked to a PDF of *Rumiyah* that is no longer available. The others outlinked to news items (eight posts), academic analyses (six posts) and other terrorism-related content (three posts).

[12] Hannah Al-Othman, 'ISIS Calls on Islamists to Carry Out Knife Attacks in Areas Such as Alleys, Forests and Quiet Neighbourhoods and Told to Aim for "a Reasonable Kill Count" in Latest Magazine', *Daily Mail*, 5 October 2016. The three tweets received 220, 54 and 52 retweets respectively.

[13] Tech Against Terrorism, 'Analysis: New Zealand Attack and the Terrorist Use of the Internet', undated, <https://www.techagainstterrorism.org/2019/03/26/analysis-new-zealand-attack-and-the-terrorist-use-of-the-internet/>, accessed 18 June 2019.

[14] Ashitha Nagesh, 'Isis Magazine Urges Followers to Kill a Random Florist in Cheshire', *Metro*, 7 September 2016.

distinct outlinks containing each hostname, as well as the total number of posts containing these outlinks and the number of reposts these posts received. Hostnames for which there were just one or two distinct links appear in a single category, ‘Other hostnames’.

Two points in particular emerge from Table 3. The first is that 5,714 (83.9%) of the posts outlinked to just seven of the hostnames: drive.google.com; archive.org; ref.gl; cldup.com; cloud.mail.ru; 1drv.ms; and yadi.sk. Excluding ref.gl – discussed previously – Table 1 showed that a total of 1,736 distinct users posted links to these six hostnames. Of these, 1,722 (99.2%) had been suspended by the end of the data-collection period for this report. The second point is the ratio of posts to reposts. Between them, the 6,808 posts containing an outlink to *Rumiyah* received a total of just 800 reposts during the data-collection period (8.51 tweets per retweet). Together, the high suspension rate and low number of reposts indicate that Twitter was successful in frustrating efforts to use its platform to disseminate new issues of *Rumiyah*.

Table 3: Outlinks to a PDF of *Rumiyah*, by Hostname and Number of Posts

Hostname	Number of distinct links to a PDF	Number of posts containing a link to the PDF	Number of reposts containing a link to the PDF	Total number of posts and reposts
drive.google.com	53	1,631	85	1,716
archive.org	53	442	171	613
ref.gl	32	1,450	81	1,531
justpaste.it	29	82	138	220
cldup.com	26	562	70	632
4shared.com	18	103	15	118
cloud.mail.ru	13	877	37	914
siteintelgroup.com	13	27	70	97
mediafire.com	13	44	11	55
1drv.ms	12	335	10	345
dropbox.com	12	188	13	201
pietervanostaeyen.com	12	17	25	42
memri.org	12	15	2	17
yadi.sk	11	417	4	421
almlf.com	10	15	7	22
counterjihadreport.com	8	46	31	77
up.top4top.net	5	27	10	37
trackingterrorism.org	5	5	6	11
facebook.com	3	3	0	3
Other hostnames	41	522	14	536
Total	381	6,808	800	7,608

Source: Authors' research.

Outlinks to Openly Available PDFs of *Rumiyah*

Table 4 details the 15 outlinks to openly available PDFs of *Rumiyah*.[15]

Table 4: Outlinks to Currently Available PDFs of *Rumiyah*

Hostname	Number of posts containing the link	Number of times the posts have been reposted	Number of users that posted the links	Status of user accounts
cloud.mail.ru	154	0	154	All suspended
qb5cc3pam3y2ad0tm1zxuhho-wpengine.netdna-ssl.com	14	3	6	Five extant, one suspended
adobe.ly	4	0	2	Both extant
drive.google.com	2	1	2	One extent, one suspended
azelin.files.wordpress.com	2	1	1	Extant
azelin.files.wordpress.com	2	0	1	Extant
jihadology.net	1	0	1	Extant
cloud.mail.ru	1	0	1	Suspended
cloudup.com	1	0	1	Suspended
pietervanostaeyen.com	1	0	1	Extant
clarionproject.org	1	2	1	Extant
magentacloud.de	1	0	1	Suspended
magentacloud.de	1	0	1	Suspended
reddit.com	1	0	1	Suspended
reddit.com	1	0	1	Suspended
Total	187	7	175	

Source: Authors' research.

[15] The researchers shared the 15 URLs with the relevant authorities. Some have subsequently been removed.

Three points emerge from Table 4. First, there is again evidence of botnet activity. While the 15 outlinks appeared in a total of 187 posts, 154 of these posts contained the same URL. These 154 tweets were all posted by different users. The names of all these users were randomised collections of numbers and letters, and all accounts had been suspended by the end of the data-collection period – although curiously the outlink remained functional. The other 14 outlinks appeared in a combined total of 33 posts. These tweets were posted by a total of 19 distinct users.[16] They received just seven retweets.

Second, the fact that 12 of the user accounts remain extant is not necessarily indicative of a failure on Twitter's part to enforce its terms of service, which prohibit promoting and recruiting for a violent extremist group. In accordance with this, the accounts of non-Daesh sympathisers who posted outlinks to the group's magazine (for example, for research purposes or general interest) were not suspended.

Third, it is noteworthy that four of the URLs in Table 4 outlink to repositories maintained by researchers (and a fifth outlinked to a repository maintained by an NGO, the Clarion Project). Three of these URLs outlinked to the website jihadology.net.[17] This site has received much scrutiny in recent months, with reports that the UK government urged WordPress.com to place the site's contents behind password protection or close it altogether.[18] However, in terms of the specific study for this report, it seems clear that Daesh sympathisers did not seek to use Twitter to signpost users to copies of *Rumiyah* on jihadology.net. Not only were there only five posts containing outlinks to jihadology.net in the entire dataset of 11,520 tweets – with these five posts receiving a total of just one retweet during the data-collection period – but none of these five tweets was posted by a Daesh sympathiser.[19]

The fourth URL outlinked to the site pietervanostaeyen.com. This site is also hosted by WordPress.com, but is password protected. Users are required

[16] The figures in the relevant column in Table 4 add up to 21. The reason for this apparent disparity is that there were two users that shared more than one of the outlinks. The same user shared both of the outlinks to reddit.com, and another user shared two distinct links to jihadology.net.

[17] The two links using the hostname azelin.files.wordpress.com, plus the one using jihadology.net.

[18] David Bond, 'How Extremist Videos are Hitting UK Relations with US Tech Groups', *Financial Times*, 3 December 2018. It should be noted that the GIFCT has funded Tech Against Terrorism to develop a new interface for jihadology.net, to ensure that particularly sensitive content is only accessible to users with registered academic/research, governmental, journalistic or humanitarian email addresses.

[19] The three users that posted these five tweets were two academic researchers and an individual tweeting in a personal capacity.

to register for an account. In spite of this, the outlink collected led directly to a PDF of an issue of *Rumiyah* without requiring a password.[20] Moreover, the owner has in any event publicly stated that he approves every request he receives for access to the website, explaining that he lacks the capacity to vet those who request access.[21] This raises doubts about whether the introduction of password protection on jihadology.net would in fact limit the availability of the materials it contains, in the absence of sufficient resources to vet access requests properly.

Conclusion and Recommendations

The aim of this study was to examine in more detail Daesh's attempts to use throwaway accounts to signpost users to copies of its magazine, *Rumiyah*, on other platforms, to evaluate the extent to which Twitter operates as a gateway to the magazine. Ample evidence was found of Daesh employing this tactic. There were outlinks to a large number of different file-sharing sites, most of which were smaller platforms, although, interestingly, there was no evidence of Daesh seeking to signpost Twitter users to copies of *Rumiyah* that are freely available from repositories maintained by researchers or NGOs. Twitter's response to Daesh's attempts to use the platform as a gateway to *Rumiyah* appeared effective. The vast majority of outlinks to a PDF of the magazine either no longer work or are met with a requirement for a subscription and/or password. Moreover, a high proportion of the user accounts that posted outlinks to PDFs of *Rumiyah* were suspended and the tweets that these accounts posted received relatively few retweets.

In the light of these findings, the following recommendations are offered:

- Larger social media companies have automated means that employ behavioural cues to block content (for example, abnormal posting volume or using trending hashtags to gain attention). This is valuable in the present context, given the finding that botnet activity played a significant role in efforts to disseminate *Rumiyah*. By contrast, many smaller companies rely exclusively on humans to use content-based cues to identify and remove terrorist content. **Where possible, GIFCT members should develop shared automated systems that use behavioural cues to block terrorist content**.
- **There is a pressing need to expand membership of the GIFCT**. At present the GIFCT has 14 members, a small number in comparison to the 244 different hostnames contained in the research dataset. Many smaller technology companies lack the capacity needed to meet the standards

[20] This was tested for every other issue of *Rumiyah* stored on the website and this problem only existed for this one issue.

[21] Bob Garfield, 'Archiving Terrorist Propaganda', WNYC Studios, 22 March 2019, <https://www.wnycstudios.org/story/archiving-terrorist-propaganda-jihadology>, accessed 18 June 2019.

imposed by the GIFCT eligibility criteria. Some lack the willingness to abide by these criteria. Here policymakers have an important role to play, providing the support required by the former and offering appropriate incentives to the latter.

- The role of the traditional news media in the dissemination of terrorist propaganda must be addressed. At present the public debate in Western countries focuses on the responsibilities of large technology platforms. But **discussions about the responsibilities of platforms should be broadened to include traditional news media, to examine issues such as the sharing of news coverage that has the effect of amplifying the terrorist message**. As Assistant Commissioner Neil Basu, Head of Counter Terrorism Policing, stated in an open letter following the attacks in Christchurch, New Zealand, 'it's time to have a sensible conversation about how to report terrorism in a way that doesn't help terrorists'.[22]

Stuart Macdonald is Professor of Law in the School of Law at Swansea University

Daniel Grinnell is Research Associate in the School of Social Sciences at Cardiff University

Anina Kinzel is a Doctoral Candidate in Applied Linguistics at Swansea University

Nuria Lorenzo-Dus is Professor of Linguistics in the Department of Applied Linguistics at Swansea University

[22] National Police Chief's Council, 'Head of Counter Terrorism Policing Issues Open Letter About Reporting of Terrorism', 20 March 2019, <https://news.npcc.police.uk/releases/head-of-counter-terrorism-policing-issues-open-letter-about-reporting-of-terrorism>, accessed 13 June 2019.

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 necessarily 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)