RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

Transnational Lessons from Terrorist Use of Social Media in South Asia

Aaditya Dave

Key Findings

- There are currently gaps in identifying terrorist content on various social media platforms. There may be a need for greater in-house expertise in technology companies, with the requisite language and cultural knowledge, to know where to look for content that might be missed by algorithms.
- There is a link between hate speech and terrorist activity in South Asia. Given the extent of inter-communal violence in the region, it is critical to carry out further research on this link.
- Terrorists' use of end-to-end encrypted communications is a common feature of all three case studies in this paper: Pakistan; Bangladesh; and Sri Lanka. However, government responses to this in South Asia have so far been unhelpful, as their suggestions have been unimplementable and social media blocks have had limited effectiveness.

Summary of Recommendations

- There is a need for greater public–private dialogue on how the internet and social media are used by terrorists and for counterterrorism. A multi-stakeholder approach would not only help technology companies develop better approaches to managing the issues but also build links between communities and authorities to develop more cooperative approaches.
- Governments should consult technology companies and civil society while designing regulations aimed at countering terrorist use of the internet to enhance the effectiveness and feasibility of regulations.
- Government officials in South Asia need to be trained on effective identification of terrorist content, reporting mechanisms and the use of metadata on encrypted communication platforms for investigative purposes.
- Technology companies should recruit more content moderators speaking Baloch, Sinhala, Tamil and Bangla, and support qualitative research into the dissemination of terrorist propaganda in regional languages.
- Social media platforms should consider developing easier ways for users to report terrorist content.
- Governments in South Asia need to clarify the scope of counter-extremism legislation and its applicability online, and clearly define hate speech and terrorist content.

Introduction

While terrorist use of social media is a focus of counterterrorism research, most work has been restricted to Western contexts. However, in South Asia,

use of the internet and cheap access to mobile data are growing rapidly.[1] For instance, Pakistan has an average cost of $1.85 per GB of data. While this is the 33rd cheapest rate for mobile data in the world, it is the second most expensive in South Asia. Sri Lanka and Bangladesh offer 1 GB of data at an average of $0.78 and $0.99, respectively.[2]

This has led to growing levels of internet penetration in the region. As of May 2019, the Pakistan Telecommunications Authority reported that out of a total 70 million broadband users (33.36% penetration), 68 million were mobile 3G/4G subscribers.[3] In Bangladesh in 2018, there were 92 million internet users (55% penetration), with 86 million of them using mobile internet.[4] In Sri Lanka, of 7 million internet users (34% penetration), 6.5 million used their mobile phones to get online.[5]

Cheap data and a proliferation of applications that provide end-to-end encryption means that communication in the region is easier than ever – including for those who seek to incite and organise violence.[6] Additionally, the widespread use of social media platforms, particularly Facebook, which offers free data or internet access through its Free Basics platform in Bangladesh and Pakistan, among others countries, gives these platforms a particularly significant role in the media and information space.[7]

---

1. As an example, the total number of internet subscribers in India has gone from fewer than one million in 2000 to 637 million in March 2019, see the annual Indian Telecom Services Performance Indicator Reports, available at Telecom Regulatory Authority of India, <https://www.trai.gov.in/release-publication/reports/performance-indicators-reports>, accessed 1 August 2019. In Myanmar, SIM cards went from costing over $1,000 under the military junta to as cheap as $1.60 in 2014, see Sebastian Strangio, 'Talk is Suddenly Cheap in Myanmar – And That Could be Costly', *Christian Science Monitor*, 15 August 2014.
2. Cable.co.uk, 'Worldwide Mobile Data Pricing: The Cost of 1GB of Mobile Data in 230 Countries', February 2019, <https://www.cable.co.uk/mobiles/worldwide-data-pricing/>, accessed 11 April 2019.
3. Pakistan Telecommunications Authority, 'Telecom Indicators', 2019, <https://www.pta.gov.pk//en/telecom-indicators>, accessed 10 July 2019.
4. DataReportal, 'Digital 2019: Bangladesh', 31 January 2019, <https://datareportal.com/reports/digital-2019-bangladesh>, accessed 11 April 2019.
5. DataReportal, 'Digital 2019: Sri Lanka', 31 January 2019, <https://datareportal.com/reports/digital-2019-sri-lanka>, accessed 11 April 2019.
6. For reporting related to Myanmar, see, for example, *BBC*, 'The Country Where Facebook Posts Whipped Up Hate', 12 September 2018. Also see Bharatha Mallawarachi, 'Sri Lanka Blocks Social Media as Anti-Muslim Rioting Flares', *Associated Press*, 7 March 2018.
7. Internet.org by Facebook, 'Where We've Launched', <https://info.internet.org/en/story/where-weve-launched/>, accessed 17 July 2019.

This paper looks at how social media platforms have been instrumentalised for a variety of purposes by terrorist organisations in Pakistan, Bangladesh and Sri Lanka, and how the governments of those countries have tackled the issue. It aims to draw lessons from past cases and presents recommendations that might help mitigate the harm caused by such use. The paper focuses on these countries as, in addition to the increasing proliferation of the internet, they have experienced significant terrorist activity, either over a protracted period, as in the case of Pakistan and Bangladesh, or more recently, as in the case of Sri Lanka. India, another South Asian country which shares these characteristics, is the subject of another paper in this series and was thus not taken up here.[8]

The paper is based on a study of academic and grey literature, official documents and journalistic coverage. Owing to the fact that there is limited academic literature on this topic in South Asia, the latter three categories of literature provided more relevant information. Further, the research for this paper examined only English-language sources, so material in other languages, particularly, Urdu, Sindhi, Baloch, Tamil, Sinhala and Bangla, was not examined. This paper is therefore intended to provide a basis for future research using fieldwork and primary and secondary sources in local languages.

Pakistan

Of the three countries examined in this paper, terrorist networks in Pakistan have been the most well studied.[9] However, even in Pakistan, data on terrorist use of social media has been limited. A 2017 survey found that several groups proscribed in Pakistan – sectarian groups, global terrorist groups, and Baloch and Sindhi nationalists – maintained a considerable presence on Facebook in an official or unofficial capacity.[10] At the time, Facebook was used primarily to post pictures and videos with the aim of propagating ideology (through religious or political speeches), glorifying fighters, and providing updates on the groups' activities and events, and to direct users to private or offline

---

8.   Kabir Taneja and Kriti M Shah, 'The Conflict in Jammu and Kashmir and the Convergence of Technology and Terrorism', Global Research Network on Terrorism and Technology, No. 11, RUSI, August 2019.

9.   Bruce Riedel, 'Pakistan and Terror: The Eye of the Storm', *The ANNALS of the American Academy of Political and Social Science* (Vol. 618, No. 1, 2008), pp. 31–45; Madiha Afzal, *Pakistan Under Siege: Extremism, Society, and the State* (Washington, DC: The Brookings Institution, 2018)

10. Jahanzaib Haque and Omer Bashir, 'Banned Outfits in Pakistan Operate Openly on Facebook', *Dawn*, 14 September 2017. Ahle Sunnat Wal Jamaat (ASWJ), Jeay Sindh Muttahida Mahaz (JSMM) and Sipah-i-Sahaba (SSP) had the largest number of pages, while Lashkar-e-Jhangvi (LeJ), Tehreek-e-Taliban Pakistan (TTP), Tehrik-e-Nifaz-e-Shariat-e-Mohammadi (TNSM) and Jamaat-ul-Ahrar (JuA) had a smaller presence.

modes of communication and to other websites. Some Facebook pages were organised by district or electoral constituency and many used languages other than English, such as Urdu (or Romanised Urdu), Baloch or Sindhi. This allowed these groups to both highlight local grievances and remain under the radar for longer. While these pages are now offline, it is unclear whether this resulted from government requests or proactive measures taken by Facebook.

Apparently responding to the removal of terrorist content and accounts from mainstream social media platforms such as Facebook, Twitter and YouTube, terrorist groups in the region have largely migrated to other platforms and encrypted messaging apps. Telegram, which allows secret chats as well as open channels for broadcasting, became particularly favoured.[11]

Daesh (also known as the Islamic State of Iraq and Syria, ISIS), which announced the creation of its Khorasan province in January 2015,[12] initially claimed attacks in the country, such as an attack on a bus carrying members of the Ismaili community in Karachi (in conjunction with the Pakistani Jundallah), via jihadist Twitter accounts.[13] However, when Daesh claimed another major attack on a hospital in Quetta in August 2016 (in conjunction with the hard line Tehreek-e-Taliban Pakistan (TTP) splinter Jamaat ul-Ahrar [JuA]),[14] the announcement was put forward primarily on Telegram through its Amaq News Agency. In September 2018, when Daesh shared information about its links with Lashkar-e-Jhangvi (LeJ), claiming that LeJ had pledged allegiance to Daesh in 2015, this too was done on Telegram via its Al-Naba newsletter.[15] Finally, the announcement of a '*Wilayah* Pakistan' – or a Pakistan province – in May 2019, referenced while claiming an attack in Balochistan, was also made on Telegram.[16]

---

11. For a general explainer on why terrorist groups prefer Telegram, see Ahmet S Yayla and Anne Speckhard, 'Telegram: The Mighty Application That ISIS Loves – Part I', *VOX-Pol,* 7 June 2017, <https://www.voxpol.eu/telegram-mighty-application-isis-loves/>, accessed 22 July 2019. Note that while Telegram has taken action against jihadist accounts (see, for example, its ISIS Watch channel, <https://t.me/ISISwatch>), the platform continues to be used by terrorists, as outlined in the cases below.
12. Rezaul H Laskar, 'IS Announces Expansion into AfPak, Parts of India', *Hindustan Times*, 29 January 2015.
13. *BBC*, 'Pakistan Gunmen Kill 45 on Karachi Ismaili Shia Bus', 13 May 2015.
14. Bill Roggio, 'Jamaat-ul-Ahrar, Islamic State Claim Suicide Attack at Pakistani Hospital', *FDD's Long War Journal*, 8 August 2016.
15. *BBC Monitoring*, 'IS Reveals Rare Details of Ties with Pakistani Militant Group Lashkar-e-Jhangvi', 6 September 2018.
16. Robert Postings, 'ISIS Announces New India and Pakistan Provinces, Casually Breaking Up Khorasan', *The Defense Post*, 15 May 2019, <https://thedefensepost.com/2019/05/15/islamic-state-pakistan-province-al-hind/>, accessed 29 May 2019.

However, while Daesh and groups that have aligned with it in Pakistan have used online platforms to announce pledges or collaboration, there is limited open-source evidence to suggest that such engagement was facilitated online.[17]

The TTP has also used Telegram, primarily via its Umar Media wing, to claim attacks, make announcements and share material, including a magazine for women which called on women to 'join the ranks of mujahideen' and learn 'how to use a grenade' as well as 'simple weapons'.[18] Further, the Balochistan Liberation Army has used Telegram to promote their attacks and activities, most recently the attack in May 2019 on the Pearl Continental Hotel in Gwadar, using its Hakkal media wing.[19]

A 2017 investigation carried out by the Counter Terrorism Department of the Khyber Pakhtunkhwa Police following the arrest of a Daesh operative shed further light on how the group used social media. While almost all communication appeared to have been through Telegram, using frequently changing aliases, Twitter and Facebook were used to select targets on sectarian grounds. From a previous operation, the Counter Terrorism Department had tracked data usage to learn how the group communicated, and once they had discovered they were being tracked on Telegram, they tried to shift to another encrypted application, Signal.[20]

At around the same time, in November 2017, Pakistan blocked access to Telegram on government-owned service providers.[21] However, as will be noted in other cases as well, not only do such bans not prevent terrorists from using Telegram if they use virtual private networks (VPNs), they also do not stop them from using other apps which provide similar encrypted communication services.

Pakistan's National Action Plan for countering terrorism and extremism includes on its agenda a ban on the glorification of terrorists in print and electronic media, dismantling of terrorist communication networks, and

17. *Dawn*, 'IS Visits Militants in Balochistan: Jundullah Spokesman', 12 November 2014.
18. Memphis Barker, 'Pakistani Taliban Launches Women's Magazine Offering Advice on How to Use a Grenade', *The Telegraph*, 4 August 2017.
19. *The Defense Post*, 'Pakistan: 5 Killed in Gwadar Hotel Attack Claimed by Baloch Liberation Army', 12 May 2019.
20. Iftikhar Firdous, 'How a Selfie Cracked Da'ish in K-P', *Express Tribune*, 6 November 2017.
21. Pakistan Telecommunication Company Limited (PCTLOfficial), 'Dear Customer, As per PTA instructions Telegram Messaging Application on PTCL Network have been Blocked till further notice.' [Twitter post], 5:34am, 5 December 2018, <https://twitter.com/PTCLOfficial/status/928496107105251328?ref_src=twsr c%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E928496107105251328& ref_url=https%3A%2F%2Fpropakistani.pk%2F2017%2F11%2F17%2Ftelegram-blocked-pakistan%2F>, accessed 29 May 2019.

measures against the abuse of the internet and social media for terrorism.[22] To this end, the government has implemented measures for bottom-up social media monitoring and reporting. The Surfsafe portal and CHAUKAS app, for example, encourage users to anonymously report online extremist and hate content.[23] However, apart from uncertainty about the effectiveness of such a platform, it also has significant potential for misuse. Pakistan, where blasphemy can be punishable by death, has witnessed cases in which mobs have lynched individuals suspected of posting blasphemous content online.[24] Moreover, Pakistan's government has not defined hate content, which could be broadly interpreted, thus empowering radical and sectarian elements looking to exploit these tools.

Similarly, the Prevention of Electronics Crimes Act (PECA), which was enacted in 2016 and attempts to plug a gap in the Anti-Terrorism Act of 1997 on terrorist use of the internet, has been criticised for containing poorly defined terminology and leaving room for the state to curtail free speech.[25] While PECA introduces a new offence of cyber terrorism, it fails to adequately differentiate between cybercrime, cyber warfare and online terror activities.[26]

Bangladesh

The first time Bangladesh received significant international attention with regard to Islamist militancy was when Fazlur Rahman, the 'amir of the Jihad Movement in Bangladesh', became one of the signatories to Al-Qa'ida's 1998 fatwa announcing its 'Jihad against Jews and Crusaders'.[27] Following this, in the late 1990s and early 2000s, Bangladesh witnessed attacks carried out by groups like the Harkat-ul-Jihad al-Islami Bangladesh (HuJI-B) and the Jamaat ul-Mujahideen Bangladesh (JMB), including an assassination attempt on a British High Commissioner in 2004 and a series of coordinated bombings across the country in 2005.[28]

---

22. National Action Plan, 2014, <https://nacta.gov.pk/nap-2014/>, accessed 12 April 2019.
23. Surfsafe, <https://surfsafe.pk>, accessed 12 April 2019; NACTA's Android-iOS App (CHAUKAS), <https://nacta.gov.pk/nacta-introduce-apps-citizens-2/>, accessed 12 April 2019.
24. Jibran Ahmed, 'Pakistani Student Accused of Blasphemy Beaten to Death on Campus', *Reuters*, 13 April 2017.
25. Raza Khan, 'Cyber Crime Bill Passed by NA: 13 Reasons Pakistanis Should be Worried', *Dawn*, 11 August 2016.
26. 'Prevention of Electronic Crimes Act 2016 (Pakistan)'.
27. World Islamic Front, 'Jihad Against Jews and Crusaders', 23 February 1998, <https://fas.org/irp/world/para/docs/980223-fatwa.htm>, accessed 2 July 2019.
28. *BBC*, 'Bangladesh Executes Islamist for 2004 British Envoy Attack', 12 April 2017; *The Daily Star*, '459 Blasts in 63 Districts in 30 Minutes', 18 August 2005.

Since 2013, however, Bangladesh has experienced a series of attacks against secular bloggers, gay rights activists, academics and non-Muslims who were perceived to be anti-Islamist.[29] The group blamed for many of these attacks is the Al-Qa'ida-affiliated Ansarullah Bangla Team (ABT, also known as Ansar Al-Islam), whose leader, Jasimuddin Rahmani, was active on platforms like YouTube and Facebook in soliciting recruits to engage in jihad and carry out targeted killings. The group has used online platforms, in particular Facebook, to select and monitor targets,[30] and has also used Telegram to both plan attacks and share content aimed at attracting recruits.[31] Additionally, before being removed from Twitter, ABT used the platform to publish propaganda and claim attacks,[32] and even though Rahmani has been in prison for five years, some of his videos are available on certain platforms even under channels that do not have a solely Islamist focus.

While Daesh had claimed a number of targeted killings and smaller attacks in Bangladesh in 2015 and early 2016,[33] the July 2016 massacre at the Holey Artisan Bakery in Dhaka brought to light the extent to which it had influenced local terrorist networks in Bangladesh.[34] Though the government had previously denied Daesh's presence in the country and blamed local groups, particularly the JMB, for terrorist activities, this attack showed that local groups were linked to Daesh. Coordinated and directed by Daesh members outside Bangladesh, the attackers reportedly used the encrypted

29. Emma Graham-Harrison and Saad Hammadi, 'Inside Bangladesh's Killing Fields: Bloggers and Outsiders Targeted by Fanatics', *The Guardian*, 12 June 2016.

30. Shahab Enam Khan, 'Bangladesh: The Changing Dynamics of Violent Extremism and the Response of the State', *Small Wars & Insurgencies* (Vol. 28, No. 1, 2017), pp. 191–217; Arifur Rahman Rabbi, 'Militants Stalked Xulhaz Through LGBTQ Platforms', *Dhaka Tribune*, 18 January 2019; *Al Jazeera*, 'Ansar Al-Islam Claims Bangladesh Student's Killing', 9 April 2016; *Prothom Alo*, 'Militants Planned to Attack Jail: RAB', 1 February 2019, <https://en.prothomalo.com/bangladesh/news/190528/Militants-planned-to-attack-jail-RAB>, accessed 17 April 2019.

31. International Crisis Group, 'Countering Jihadist Militancy in Bangladesh', Report No. 295, 28 February 2018; *Times of India*, 'Two Islamic Extremists Arrested for Plotting to Kill Bangladeshi Filmmaker', 11 December 2018.

32. CEP, '#AQIS Bangladeshi branch acct @AnsarAlIslam5 claims responsibility for assassination of #LGBT magazine editor' [Twitter post], 4:00pm, 26 April 2016, <https://twitter.com/FightExtremism/status/724976377448026112>, accessed 17 April 2019; *SITE Intelligence Group*, '"Ansar Al-Islam Bangladesh" Lists Categories of Potential Targets for Killing', 29 May 2015, <https://news.siteintelgroup.com/jihadist-news/ansar-al-islam-bangladesh-lists-categories-of-potential-targets-for-killing.html>, accessed 29 May 2019.

33. Tim Lister et al., 'ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043', *CNN*, 12 February 2018.

34. Andrew Marszal and Chris Graham, '20 Hostages Killed in "Isil" Attack on Dhaka Restaurant Popular with Foreigners', *The Telegraph*, 2 July 2016.

communications service Threema to send pictures and videos of the attack and to communicate with Daesh leadership.[35] Daesh then released videos in English and Bangla which praised the fighters, and published articles including new information about the attack in its *Rumiyah* magazine.[36] Daesh also released a Bangla-language video in September 2016, which glorified the Dhaka attackers and justified the targeting of foreigners.[37]

Investigations also revealed the role of social media prior to the attack. Two of the attackers followed the pro-Daesh Twitter handle ShamiWitness as well as radical Islamist preachers Zakir Naik and Anjem Choudary.[38] Moreover, Saifullah Ozaki, the amir of Daesh in Bangladesh, played a key role in facilitating the merger of local groups to create a Daesh affiliate using Facebook,[39] and his communication and fundraising efforts were focused on encrypted communications services such as Wickr, WhatsApp, Telegram, Threema, Surespot, Chat Secure, Skype, Facebook, ProtectedText, Pidgin and Viber.[40]

Daesh has consistently used its Telegram channels to release Bangla material. For example, concurrently with the release of Abu Bakr Al-Baghdadi's most recent video message in April 2019,[41] an image with threatening messages in Bangla set against images of the Holley Artisan Bakery attackers appeared on the pro-Daesh Telegram channel Al-Mursalat, along with a threat in Bangla, Hindi and English warning of further attacks.[42] Moreover, in March 2019, via the Bangla-language At-Tamkin Telegram channel, Daesh encouraged

35.   Indrani Bagchi, 'Terrorists Used App to Hide Digital Footprint', *Times of India*, 5 July 2016.

36.   Ellen Barry and Maher Sattar, 'Bangladesh Siege Recalled in Militant's Words, and From Beyond the Grave', *New York Times*, 5 October 2016.

37.   *Dhaka Tribune*, 'Tamim Chowdhury Featured in New IS Publication', 5 October 2016.

38.   *Hindustan Times*, 'Dhaka Cafe Gunmen Followed "IS Recruiters", Controversial Preachers', 5 July 2016. The ShamiWitness Twitter account was shut down after the user's identity was revealed. See Chris Johnston, 'India-based Twitter Account Hailing Islamic State Jihadists Shut Down', *The Guardian*, 11 December 2014.

39.   Tasneem Khalil, 'Meet the Mastermind of the Holey Attack', *Dhaka Tribune*, 31 July 2017.

40.   Asia/Pacific Group on Money Laundering and Middle East and North Africa FATF, 'Social Media and Terrorism Financing', 23 January 2019.

41.   This was the first time Al-Baghdadi was seen on video since 2014, and was seemingly intended to indicate the continuing presence of Daesh and its leader following the group's loss of territory in Syria. See Ben Wedeman and Lauren Said-Moorhouse, 'ISIS Has Lost its Final Stronghold in Syria, the Syrian Democratic Forces Says', *CNN*, 23 March 2019.

42.   Middle East Media Research Institute, 'Jihad and Terrorism Threat Monitor (JTTM) Weekend Summary', 4 May 2019, <https://www.memri.org/reports/jihad-and-terrorism-threat-monitor-jttm-weekend-summary-352>, accessed 29 May 2019.

its followers to 'regroup and communicate with their representative in Bangladesh' and carry out attacks using cars or knives.[43]

Following the Dhaka attack, the counter terrorism and transnational crimes unit of Dhaka's police launched an app, Hello CT, which allows citizens to report information on terrorism as well as other crimes. However, while it is being used and updated frequently, its misuse, for example the submission of false information, has been acknowledged by law enforcement officials.[44]

Sri Lanka

Sri Lanka was rocked by coordinated bombings across the country on Easter Sunday 2019.[45] Although this attack appeared to be unexpected, it is now clear that the authorities were aware of jihadist intent and capability.[46] Moreover, the attacks followed an increase in hate speech and inter-communal tensions that were facilitated by social media. In particular, Facebook was used to spread disinformation and hate speech, while Facebook Messenger and WhatsApp were used to plan and coordinate violence.[47]

The Easter Sunday attacks were carried out by National Thowheed Jamath (NTJ), which had splintered from another Islamist extremist group – the Sri Lanka Thowheed Jamath – and been flagged to the authorities by the Muslim community in eastern Sri Lanka for three years.[48] However, prior to the attack, NTJ was known largely for desecrating Buddhist statues in Kandy in December 2018.[49] The group and the attacks were led by Zahran Hashim, a radical preacher from Kattankudy in the Eastern Province.

Organisationally, NTJ's social media presence was not, however, significant. The group had a Tamil-language Facebook page that was updated sporadically

43. Quote taken from Muktadir Rashid, 'Police Examine IS Threat on Social Media', *New Age Bangladesh*, 16 March 2019.

44. *Dhaka Tribune*, 'Hello CT: Almost 3k Info in a Month, in Arabic Too', 5 September 2016.

45. Sugam Pokharel et al., 'Bombs Tear Through Sri Lankan Churches and Hotels, Killing 250 People', *CNN*, updated 25 April 2019.

46. *Dhaka Tribune*, 'Sri Lanka Seize Explosives from Local Islamist Radicals', 19 January 2019; *New York Times*, '"These Attacks Could Target Catholic Churches": The Warning That Sri Lankan Officials Failed to Heed', 22 April 2019.

47. Amanda Taub and Max Fisher, 'Where Countries are Tinderboxes and Facebook is a Match', *New York Times*, 21 April 2018; Rosie Perper, 'After Declaring a State of Emergency, Sri Lanka has Banned Facebook, Instagram, and WhatsApp', *Business Insider*, 7 March 2018.

48. Iain Marlow, 'Sri Lanka Muslims had Warned Officials About Group Behind Attack', *Bloomberg*, 22 April 2019; Hannah Beech, 'Sri Lankan Accused of Leading Attacks Preached Slaughter. Many Dismissed Him', *New York Times*, 25 April 2019.

49. *BBC*, 'Sri Lanka Attacks: Who are National Thowheed Jamath?', 28 April 2019.

and is now inactive. Most of the content on this page was not extremist, but rather focused on social outreach.[50] The group's Twitter page (NTJ @ntjinfo) is still active, but this too was updated infrequently, and there have been no posts since March 2018.

However, Hashim himself had a large social media following on Facebook and YouTube. Following a clash with Sufi Muslims in 2017, after which he went into hiding, Hashim began releasing videos preaching extremist and hate content.[51] Investigators now believe that these videos drew followers who would later become involved in violence, including two brothers who were influenced by the social media videos and then engaged with Hashim using private chat rooms. They would later become funders of the Easter Sunday plot and were among the suicide bombers.[52]

Investigation by the Sri Lankan authorities revealed that while these contacts were established well in advance, the plan and specific roles for the attack were only determined in the weeks leading up to it, and the perpetrators used Threema, the encrypted messaging service also used during the 2016 Dhaka attack, to communicate.[53] Other encrypted communications platforms, including WhatsApp, were also highlighted as having been used for communication, with a Sri Lankan software engineer, who was previously monitored by Indian intelligence agencies for suspected links to Daesh, possibly serving as a coordinator for the group and facilitating contact between NTJ and a smaller group with which some of the bombers were associated, the Jammiyathul Millathu Ibrahim.[54]

However, it became apparent from the scale of the attack that external support was likely, especially given the limited track record of NTJ. Two days after the attack, Daesh claimed responsibility via its Amaq News Agency, doing so not only in Arabic and English but also in Tamil and other regional languages, indicating an awareness of the target audience. This was followed by a more detailed claim, which highlighted Christians as the target and provided aliases for the bombers. Finally, Daesh released a photograph and

50. *BBC Monitoring*, 'Name in the News: Sri Lanka Radical Group National Thowheed Jamath', 22 April 2019.

51. *The Hindu*, 'Radical Cleric Hashim Linked to Blasts', 24 April 2019; Anbarasan Ethirajan, 'Sri Lanka Attacks: The Family Networks Behind the Bombings', *BBC*, 11 May 2019; Amarnath Amarasingham, 'Terrorism on the Teardrop Island: Understanding the Easter 2019 Attacks in Sri Lanka', *CTC Sentinel* (Vol. 12, No. 5, May/June 2019).

52. Meera Srinivasan, 'The Inside Story of the 9 Suicide Bombers Behind Sri Lanka's Savage Easter Attacks', *The Hindu*, 25 May 2019; *CBS News*, 'Rich Brothers Recruited via Facebook to Fund Sri Lanka Attacks, Cops Say', 3 May 2019.

53. Asiri Fernando, 'Easter Sunday Bombers Used High-Tech Communication: Army Chief', *Sunday Times*, 12 May 2019.

54. Simon Scarr et al., 'A Network of Extremism Expands', *Reuters*, 14 May 2019.

videos of the attackers, cementing its claim.[55] Moreover, Daesh's Al-Naba newsletter, distributed via Telegram, published an infographic, translated into several languages, promoting the Easter Sunday bombings.[56] Daesh Telegram channels also shared videos of fighters killed during a raid conducted by Sri Lankan police after the bombings at a hideout in eastern Sri Lanka.[57] These releases contained exaggerated claims, for example, portraying the raid as an ambush, or stating that the bombings claimed a thousand lives.

Days prior to the attack, Tamil-language Telegram channels named Islamic State – Tamil and The Strangers Channel were circulated among Tamil-speaking Daesh supporters and were used to disseminate jihadist propaganda. Al-Ghuraba (Stranger) Media was also the name under which Zahran Hashim shared videos on Facebook.[58] Even after the attack, content featuring Hashim, which has now been taken down, was available for a few days on YouTube and Facebook.[59] It is also notable that Hashim's videos resonated beyond Sri Lanka. In particular, they emerged in multiple investigations into Daesh cells in India.[60]

Following the attacks, the Sri Lankan government blocked Facebook, WhatsApp, Instagram, YouTube, Viber, Snapchat and Facebook Messenger.[61] The government claimed this was necessary to maintain social order, and this action was praised by some commentators and Sri Lankan citizens as necessary to stop the spread of misinformation and prevent further violence.[62] However, other observers have criticised the step as

55.   Thomas Joscelyn, 'Terrorists in Sri Lanka Swore Allegiance to Abu Bakr Al-Baghdadi', *FDD's Long War Journal*, 23 April 2019, <https://www.longwarjournal.org/archives/2019/04/terrorists-in-sri-lanka-swore-allegiance-to-baghdadi.php>, accessed 8 May 2019.

56.   Thomas Joscelyn, 'Sri Lankan Security Forces Clash with Islamic State Loyalists', *FDD's Long War Journal*, 27 April 2019, <https://www.longwarjournal.org/archives/2019/04/sri-lankan-security-forces-clash-with-islamic-state-loyalists.php>, accessed 8 May 2019.

57.   *Ibid.*

58.   *BBC Monitoring*, 'IS Supporters Celebrate Sri Lanka Attacks in Absence of IS Claim', 22 April 2019.

59.   Newley Purnell, 'Sri Lankan Islamist Called for Violence on Facebook Before Easter Attacks', *Wall Street Journal*, 30 April 2019.

60.   *The Hindu*, 'NIA Arrests Youth Planning Suicide Attack in Kerala', 30 April 2019; *Newshub.lk*, 'IS Cell in India had Facebook Chats in Tamil with Zahran Hashim', 13 June 2019.

61.   NetBlocks, 'Social Media Blocked in Sri Lanka Following Church and Hotel Bombings', 21 April 2019, <https://netblocks.org/reports/social-media-blocked-in-sri-lanka-following-church-and-hotel-bombings-XaAwlQBM>, accessed 8 May 2019.

62.   Kara Swisher, 'Sri Lanka Shut Down Social Media. My First Thought was "Good."', *New York Times*, 22 April 2019; Devana Senanayake and Emily

anti-democratic, as Sri Lanka's state agencies have a history of excesses, and rumours and disinformation circulated on state-controlled media have in the past led to violence against minorities, most notably the Black July pogroms that initiated the Sri Lankan Civil War in 1983.[63] Furthermore, an assessment of a social media block following the March 2018 violence indicated that users continued to access blocked platforms using VPNs, rendering the ban ineffectual while simultaneously making it more difficult to track extreme content and hate speech.[64]

Discussion

Three issues emerge from these country case studies.

There are currently **gaps in identifying terrorist content on various platforms**. Though most groups active in the region are no longer allowed on major platforms, and prominent channels and pages are shut down quite quickly, not all content is caught. One of the key issues that emerged in the aftermath of the violence in March 2018 was the lack of language expertise within Facebook, coupled with the issue of algorithms designed to detect hate speech in English being insufficient to work to similar effect for languages like Tamil or Sinhalese.[65]

To close this gap as far as possible, there may be a need for greater in-house expertise in technology companies, with the requisite language and cultural knowledge to know where to look for content that might be missed by algorithms.[66] For example, on larger platforms, content may be shared via outlinks to smaller platforms, rather than being presented directly. Technology companies have significantly increased their investment in developing manpower and technology to address these issues.[67] However, there is a risk that not pre-empting the impact of their platforms on existing tensions in the region may cause a repeat of events in Myanmar, where

Tamkin, 'Why Some Sri Lankans Welcomed the Social Media Ban After Bombings', *Washington Post*, 23 April 2019.

63. Graeme Wood, 'Why Sri Lanka Silenced Social Media', *The Atlantic*, 22 April 2019; Megha Rajagopalan, 'Banning Social Media in the Wake of the Sri Lanka Attacks Doesn't Make Much Sense', *Buzzfeed News*, 22 April 2019.

64. Yudhanjaya Wijeratne, 'Sri Lanka's March 2018 Social Media Block, Analyzed With Data', *Medium*, 5 April 2018, <https://medium.com/@yudhanjaya/sri-lankas-march-2018-social-media-block-analyzed-with-data-b1efd6189009>, accessed 18 June 2019.

65. Louise Matsakis and Issie Lapowsky, 'Don't Praise the Sri Lankan Government for Blocking Facebook', *Wired*, 23 April 2019.

66. Yudhanjaya Wijeratne, 'Big Tech is as Monolingual as Americans', *Foreign Policy*, 7 May 2019.

67. Maggie Fick and Paresh Dave, 'INSIGHT – Facebook's Flood of Languages Leave it Struggling to Monitor Content', *Reuters,* 23 April 2019.

Facebook, which became nearly synonymous with the internet in the country, was instrumentalised by members of the Myanmar army to demonise and incite violence against the Rohingya community.[68]

There is a link between hate speech and terrorist activity in South Asia. For example, according to Sri Lankan security officials, the spate of anti-Muslim violence in Sri Lanka in recent years may have led to higher rates of radicalisation among youth.[69] This is not surprising, given that terrorist groups exploit local grievances to recruit and radicalise. Notwithstanding the fact that there were numerous intelligence failures and coordination issues within the Sri Lankan government in the lead-up to the Easter attack,[70] it is critical to carry out further research on the link between hate speech and terrorism, given the extent of inter-communal violence in the region.

Terrorists' use of **end-to-end encrypted communications** is a common feature of all three case studies, and is also an issue elsewhere in the region. India has been at the forefront of this debate regionally, with the government focusing on WhatsApp in particular. However, the Indian government's proposal to force service providers to hand over encrypted messages has been described by WhatsApp as 'over-broad' and would lead to a different product that would not be 'fundamentally private'. [71] While the conversation in India is largely in the context of misinformation and fake news leading to inter-communal violence or influencing elections, it highlights the potential trade-off between privacy and security. Government bans do not effectively tackle the issue either. For example, Pakistan's decision to ban Telegram after it was identified as a means for Daesh to launch attacks did not anticipate the migration to other platforms that followed.

---

68. Alex Warofka, 'An Independent Assessment of the Human Rights Impact of Facebook in Myanmar', *Facebook Newsroom*, 5 November 2018, <https://newsroom.fb.com/news/2018/11/myanmar-hria/>, accessed date 11 April 2019; Paul Mozur, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military', *New York Times*, 15 October 2018.

69. Meera Srinivasan, 'Sri Lanka Easter Blasts: "Anti-Muslim Riots a Possible Trigger"', *The Hindu*, 27 April 2019.

70. Harin Fernando, 'Some intelligence officers were aware of this incidence. Therefore there was a delay in action. What my father heard was also from an intelligence officer. Serious action need to be taken as to why this warning was ignored. I was in Badulla last night' [Twitter post], 9:20am, 21 April 2019, <https://twitter.com/fernandoharin/status/1119999431909228544>, accessed 24 April 2019; Jeffrey Gettleman et al., 'Sri Lanka was Warned of Possible Attacks. Why Didn't it Stop Them?', *New York Times*, 22 April 2019.

71. Stephanie Findlay, 'WhatsApp Says Indian Rules on Encryption "Not Possible" to Meet', *Financial Times*, 6 February 2019.

Recommendations

- **There is a need for greater public–private dialogue on how the internet and social media are used by terrorists and for counterterrorism.** The current approach of blanket bans, popular among governments in the region, does not deal with the issue and may in fact undermine positive online activity. At the same time, governments currently have little recourse apart from this, as they are reliant on platforms to take action. There is thus a need for a multi-stakeholder approach, which would not only help technology companies develop better approaches to managing the issues but also build links between communities and authorities to develop more cooperative approaches.

- **Governments should consult technology companies and civil society while designing regulations aimed at countering terrorist use of the internet**. Currently, government measures may be too broad or impractical, which may result in loopholes or unintended consequences.[72]

- **Government officials in the region need to be trained on effective identification of terrorist content, reporting mechanisms and the use of metadata on encrypted communication platforms for investigative purposes**. This would allow a middle ground between enabling law enforcement authorities to carry out investigations while maintaining the privacy and security afforded by end-to-end encryption. Training could be provided by Internet Referral Units (for example, in Europol), possibly with experts from the technology sector, and would need to be discretionary, considering the risks of empowering authoritarian governments.

- In addition to developing more effective algorithmic detection and removal for regional languages, **technology companies should recruit more content moderators speaking Baloch, Sinhala, Tamil and Bangla**, and support qualitative research into the dissemination of terrorist propaganda in those languages.

- Social media platforms, particularly ones which allow engagement or consumption of content without the need to create an account, **should consider developing easier ways for users to report terrorist content**, while ensuring protection against misuse of such functionality.

- **Governments in South Asia need to clarify the scope of counter-extremism legislation and its applicability online, as well as clearly define hate speech and terrorist content.**

Aaditya Dave is a Research Analyst focusing on South Asia in the International Security Studies department at the RUSI.

---

72. See, for example, Patrick Howell O'Neill, 'Australia's New Encryption Law Is Forcing Tech Companies To Help With Surveillance', *Gizmodo*, 28 May 2019, <https://gizmodo.com/australia-s-new-encryption-law-is-forcing-tech-companie-1835074557>, accessed 2 July 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 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.