Royal United Services Institute
for Defence and Security Studies

Global Research Network on Terrorism and Technology: Paper No. 11

The Conflict in Jammu and Kashmir and the Convergence of Technology and Terrorism

Kabir Taneja and Kriti M Shah

Key Findings

- Blanket policies to counter terrorist and related content are problematic. Social media companies must approach places such as Jammu and Kashmir with a more nuanced perspective, and build bridges between state and central governments along with civil society.
- Objectionable, propaganda content removal must take place faster. In Jammu and Kashmir, violent mobilisation based on online content (both fake and real) is seen as a major issue for law enforcement.
- WhatsApp is the most problematic platform in India. More attention is required to addresses the issues of fake content and propaganda tailored to this platform.
- Internet shutdowns by the state as a counterterrorist policy are largely ineffective. Platforms must factor in mobilisation as a metric when formulating policies to tackle content in a conflict zone.
- Content sharing requires more checks and balances, and the ease of sharing needs to be revisited in light of the kind of content shared and created by terror groups or individuals.
- Government and social media platforms currently suffer from a lack of trust between them; this needs to be bridged.

Summary of Recommendations

- The government should work with social media platforms, technology companies and civil society organisations to create a framework that clearly defines what constitutes extremist or terrorist content, without infringing on constitutional standards of freedom of speech.
- Counter-narratives should be developed with the help of civil society groups including teachers, religious leaders and social workers, which discredit and undermine messages of terrorism on the internet.
- The long-term impact of internet shutdowns should be carefully considered and technology companies should work with the government to find solutions for conflict-prone regions that avoid shutdowns, particularly in times of crisis.
- Social media companies should work towards reducing the time between when violent, militant content is reported, analysed and removed.
- The government should encourage social media platforms to set up local research units in conflict-prone regions, to gain a first-hand understanding of the conflict on the ground and how different narratives may aggravate or improve the problem.

Background

The rising use of smartphones, consumption of internet-based content and connectivity with people around the world through social media has turned out to be a double-edged sword. The same social media

platforms that are used to communicate with the world are now also used, effectively, by terrorist organisations for the same purposes. While the use of online communications to dispense propaganda is not new for Islamist terror groups, how these new tools are being used by groups such as Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) still remains under-researched in terms of data availability and studies conducted.

Jammu and Kashmir has flown under the radar of technology companies, possibly because of the precarious political and security situation in the region. However, within the last two decades the telecommunications industry in India has taken off, with the advent of cheap data, practically free phone calls and cost-effective Chinese smartphone manufacturers entering the market and overtaking traditional industry leaders such as Samsung. This has had a major impact on the situation in Jammu and Kashmir, with more people being connected online, but also having easier access to terrorist and militant propaganda.

Internet shutdowns have become commonplace in Jammu and Kashmir as a means of clamping down on propaganda, but also on the ability of people to mobilise in large numbers. While this is a method employed by the state as part of its counterterrorist strategy, glaring gaps exist between the state, social media platforms and citizens on how to deal with violent, extremist content online, in addition to the security situation on the ground.

This paper attempts to highlight the problems faced by social media companies with regard to dangerous content online, and to provide recommendations for what they can do in the context of Jammu and Kashmir's developing online theatre of both potential radicalisation and recruitment. It also provides the Indian government with recommendations for working with technology companies, law enforcement and security officials on the ground, highlighting the new challenges posed by the use of the internet by terrorists in Jammu and Kashmir.

Methodology

This paper is based on field research conducted in Jammu and Kashmir and New Delhi, including interviews with government officials, police, intelligence officers, journalists and citizens in Jammu and Kashmir. Given the non-existence of reports and research papers on the use of social media in Jammu and Kashmir in this context, this paper primarily relies on interview data, private sector data regarding smartphone use, and published information on militancy in Jammu and Kashmir from the Indian government.

Research Findings

Militant groups in Jammu and Kashmir use social media to glamorise jihad and entice potential young recruits to join their ranks.

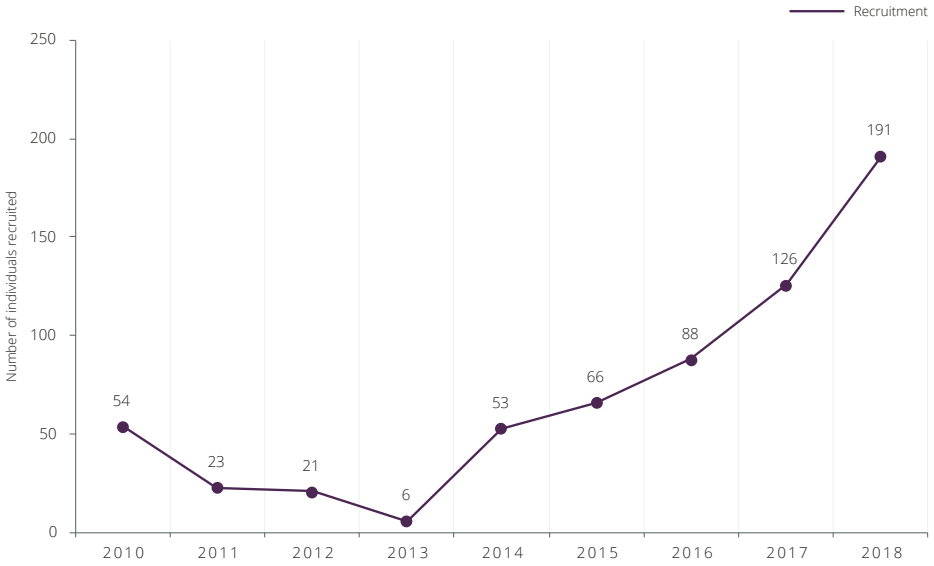
Until 2015, the use of social media platforms to propagate militancy in Jammu and Kashmir was limited. Burhan Wani, a 22-year-old militant commander of Hizbul Mujahedeen, changed this by posting photographs of himself and fellow militants on Facebook, which were then distributed further on other social media platforms.[1] The images of young men, part of the pro-Pakistan militant group, armed with guns and camouflaged outfits in the forests of Jammu and Kashmir, evoked a sense of fearlessness and defiance against the Indian state. It was unprecedented that militants would reveal their faces and names, much less post them online.

Data shows that over the years there has been a steady rise in people joining militant groups. The killing of Wani in 2016 by Indian security forces in a small village in the Anantnag district of Jammu and Kashmir, and an increasing number of anti-militancy operations, have failed to deter new militant recruits. Figure 1 demonstrates the number of militants recruited by Kashmiri and Pakistani groups since 2010. However, journalists on the ground in Jammu and Kashmir believed that since Wani's death, groups such as Hizbul Mujahedeen no longer require a social media 'poster boy' to spur recruitment. Instead, their social media outreach in Jammu and Kashmir focuses on distributing and sharing anti-India and anti-Indian security forces material and spreading a misinformation campaign against the state[2]. This includes more targeted productions, such as rap music videos promoting Kashmiri *azaadi* ('freedom') on YouTube, to garner support from Kashmiri youth.[3]

---

1. Mufti Islah, 'Burhan Wani's Viral Group Photo had 11 Militants. The Last of Them Was Killed Today', *News18,* 3 May 2019, <https://www.news18.com/news/india/burhan-wanis-viral-group-photo-had-11-militants-the-last-of-them-was-killed-today-2126901.html>, accessed 10 May 2019.
2. Outdated videos from Syria and Iraq are often passed off as videos of Indian military brutality in Kashmir. While many videos are taken down by platforms, some manage to remain. See, for example, Asian Live Updates, 'Viral video #kashmir Ya Allah Save us from Kuffars. This is what Indian army forces do to Kashmiri women's in front of her father. #Kashmiratrocities #IndianBrutality' [Twitter Post], 10:42pm, 24 January 2019, <https://twitter.com/asianliveupdate/status/1088688588139581441?s=19>, accessed 5 August 2019.
3. For example, see Najeeb Network, 'Kashmir Ki Azadi Tak | Raja Rapstar | Official Video | 2016 Latest', 3 September 2016, <https://www.youtube.com/watch?v=M9eJ8oozFfo>, accessed 3 May 2019.

Figure 1: Trends in Militant Recruitment, 2010–2018



Source: ORF Kashmir Tracker, Observer Research Foundation, October 2018, <https://www.orfonline.org/kashmir-conflict-tracker-45120/>, accessed 20 May 2019.

Organisations such as LeT and JeM also spread much of their anti-India images, videos, memes and misinformation through WhatsApp groups. This was visible on the mobile phones of five journalists and security analysts interviewed by the authors, who are or previously have been members of such WhatsApp groups. These groups, at times consisting of up to 100 people, are a tried and tested tool for militant groups to spread their message fast and wide. While security officials may be aware of such WhatsApp groups, their response capabilities are limited because of WhatApp's encryption policy and the fact that a majority of the phone numbers in each group are often not India-based. This means that security or government officials are unable to trace the numbers, even when receiving the metadata, without violating privacy regulations. This poses a serious problem for national security given that WhatsApp currently has over 200 million users in India and has been misused by some for terrorism purposes and to spark rumours that have led to a series of killings.[4]

The Indian government is currently working towards data protection legislation that will ensure that global technology companies maintain servers within the country, while ensuring higher standards for the protection of data, so as to not impede citizens' freedom of speech, if government agencies were to gain access to Indian citizens' data stored on platforms

4. U N Sushma, 'India Wants WhatsApp to Get a Grip on Fake News', *Quartz India*, 4 July 2018, <https://qz.com/india/1320859/after-a-spate-of-lynchings-india-blames-whatsapp-for-the-spread-of-fake-news/>, accessed 20 March 2019.

outside the country's judicial jurisdiction. To date, international social media companies have pushed back against this move.[5]

Some of the video content propagated by militant groups shows security forces seemingly interrogating or mistreating suspected militants.[6] Information about the event(s) in question is limited or misleading, and in some cases the security forces depicted are not even Indian. Such videos appear to be used by militant groups to undermine the authority of security forces, intentionally omitting any context or accompanying information about the video. These videos are circulated and shared, quickly going 'viral', and are shared in other cities across the country.

By the end of 2018, it was estimated that smartphones were used by 530 million people in India, and data has become cheaper as service providers compete to lower costs.[7] More people are now online for longer. There must be institutional urgency to better understand the serious, fast evolving threat to national security in the use of social media by militant groups.

The availability of low-cost smartphones and cheap mobile data has brought more Indians online than ever before, posing challenges for social media companies in monitoring and taking action against problematic content.

India has the cheapest rates for mobile data in the world. According to a recent study comparing mobile data pricing in 230 countries, India has the world's cheapest data, with the average cost of 1 GB being $0.26 (compared to $12.37 in the US and $6.66 in the UK, with a global average of $8.53).[8] Data prices in India have been further lowered by the entry of Reliance Communication's Jio into the market.[9] Service providers were forced to drop prices and offer cheaper data to compete with Jio's introductory offer of free 4G data for the first three months. Jio began test trials for its 4G service in May 2016 and within three months it had between 2.5–3 million users

5. *Times of India,* 'Facebook Takes a Tough Stand on Data Storage Amidst India's Localisation Push', 8 March 2019.
6. Hakeem Irfan, 'Video Showing Youth Tied to Army Vehicle Paraded as Warning for Stone Pelters in Kashmir Goes Viral', *Economic Times*, 13 July 2018.
7. *The Indian Express*, 'India Set to Have 530 Million Smartphone Users in 2018: Study', 16 October 2019, <https://indianexpress.com/article/technology/india-set-to-have-530-million-smartphone-users-in-2018-study-4893159/> accessed 2 April 2019.
8. Cable, 'Worldwide Mobile Data Pricing: The Cost of 1GB of Mobile Data in 230 Countries', <https://www.cable.co.uk/mobiles/worldwide-data-pricing/>, accessed 15 April 2019.
9. Ravi Agrawal, 'India's Digital Dreamer', *Foreign Policy*, <https://foreignpolicy.com/gt-essay/indias-digital-dreamer-technology-mukesh-ambani/>, accessed 14 April 2019.

without officially launching commercial operations.[10] Within six months, it had 100 million subscribers and launched its own range of mobile handsets to huge success.[11]

Between December 2016 to December 2017, Jammu and Kashmir recorded 1.85 million new wireless telephone subscribers. This 16.4% increase was the highest recorded by any state in the same period, with an increase from 11.27 million subscribers in December 2016 to 13.12 million a year later.[12]

Law enforcement officials have voiced their surprise and concern at the growth and rapid expansion of mobile phones.[13] New players entering the market have made the telecommunications industry hypercompetitive, leading to more people not only having access to a mobile phone, but higher quality 4G data. Given the rapid increase in smartphone usage, institutional responses to monitor potentially harmful content have been slow, and law enforcement officials have struggled to keep track of militant communications.

With cheap data costs come an increase in the number of the people and duration for which people remain online. The use of virtual SIM cards in this regard has been significant, especially in the case of Jammu and Kashmir.[14] The terrorist involved in the February 2019 attack in Pulwama used a virtual SIM card to keep in touch with his Pakistan- and Kashmir-based handlers.[15]

Members and, crucially, the administrators of WhatsApp groups linked to militant outfits have phone numbers with area codes from countries including the US, the UAE, Saudi Arabia and the UK. Many of these phone numbers are acquired using online services and products, such as VirtualPhone or Sonetel, which do not require in-person registration. This helps the militant outfits evade monitoring and interception by Indian security agencies.

10. Anuj Srivas, 'How Reliance Jio's Entry Tied Regulatory Knots Around India's Telecom Ecosystem', *The Wire*, 13 January 2018, <https://thewire.in/tech/reliance-jio-telecom-regulation-trai-anil-ambani>, accessed 13 March 2019.
11. Prasanto K Roy, 'Mobile Data: Why India Has the World's Cheapest', *BBC News*, 18 March 2019.
12. Telecom Regulatory Authority of India, 'Yearly Performance Indicators of Indian Telecom Sector (Second Edition) 2017', 4 May 2018, <https://main.trai.gov.in/sites/default/files/YPIRReport04052018.pdf>, accessed 15 May 2019.
13. Authors' interview with senior Jammu and Kashmir police officer, Srinagar, 5 February 2019.
14. Virtual SIM cards, unlike regular mobile SIM cards, are associated with a cloud-based mobile number. They can be purchased online and used to make and receive phone calls, videos and images through an application.
15. *The Hindu*, 'Virtual SIMs Used in Pulwama Terror Attack; India to Approach U.S. for Help', 24 March 2019, <https://www.thehindu.com/news/national/virtual-sims-used-in-pulwama-terror-attack-india-to-approach-us-for-help/article26625294.ece>, accessed 1 May 2019.

There is a perception among government and security officials in Jammu and Kashmir that internet shutdowns have been a successful tool in controlling of the formation of potentially violent gatherings. This paper finds evidence to the contrary.

Security officials state that the main purpose of an internet shutdown in Kashmir is to prevent the mobilisation of people during a sensitive time. This is why during times of shutdowns, public transportation comes to a standstill.[16] The death of a militant or arrest of a separatist leader can spark protests or demonstrations that bring hundreds into the streets. The shutdown of internet services allegedly helps to control the spread of information, whether it be via text message or social media posts, so that groups of people do not congregate, potentially posing a security threat.

There is a dearth of publicly available data on the number of and rationale behind internet shutdowns in Jammu and Kashmir. Data from the Software Freedom Law Center (SFLC), which maps internet shutdowns across the country, shows that between January 2012 and May 2018, the Indian government ordered 174 internet shutdowns of various durations and for various reasons across 19 states. Of the 174 reported incidents, 124 targeted only mobile internet services. This is significant given that over 95% of internet users in India access the internet through their mobile phone.[17]

While government officials state that internet shutdowns are a pre-emptive measure to maintain security and stability, the data on internet shutdowns in Jammu and Kashmir shows otherwise.[18] The SFLC shows that in 2017, the internet was shut down 32 times in Jammu and Kashmir, of which 28 were a pre-emptive measure (before an incident had taken place). In 2018, while the internet was shut down only 17 times, it was done as a reactive measure 11 times.[19] No studies have been done to empirically justify the

16. Authors' interview with a senior Jammu and Kashmir police officer, Srinagar, 5 February 2019. See *The Kashmir Walla,* 'Shutdown in South Kashmir's Kulgam, Train and Mobile Internet Service Suspended', 29 April 2019, <https://thekashmirwalla.com/2019/04/shutdown-in-south-kashmirs-kulgam-train-and-mobile-internet-service-suspended/>, accessed 1 May 2019; *New Indian Express,* 'Restrictions, Shutdown Continue in Jammu and Kashmir', 8 May 2018, <http://www.newindianexpress.com/nation/2018/may/08/restrictions-shutdown-continue-in-jammu-and-kashmir-1811774.html>, accessed 8 May 2019.
17. Software Freedom Law Center, 'Living in Digital Darkness: A Handbook on Internet Shutdowns in India', May 2018, pp. 1, 63, <https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2C%20May%202018%20-%20by%20SFLCin.pdf>, accessed 3 May 2019.
18. Authors' interview with a Jammu and Kashmir police officer, Srinagar, 6 February 2019.
19. Software Freedom Law Center, 'Living in Digital Darkness'.

claimed effectiveness of internet shutdowns on people's mobility, which is a significant challenge.

While the state's logic suggests that shutdowns prevent mass mobilisation in precarious times and have been a successful short-term solution, they are not a foolproof method of preventing mobilisation or violence. People have found alternative ways to communicate during times of shutdowns, through landlines or word of mouth, according to security officials on the ground. Interviews with citizens in Srinagar indicate that when the internet is down in a particular district, many travel to adjoining districts to upload or send videos.[20]

In 2016, after security forces killed militant leader Burhan Wani, large-scale violent protests broke out in the Kashmir Valley. Dozens of people were killed and over 100 were injured in clashes with security forces across the region.[21] Internet services and mobile services on prepaid numbers were suspended in the state. While internet services were restored in Jammu and Kashmir after 17 days, it took nearly five months for the internet to return for post-paid numbers, and six months for prepaid numbers. Despite the internet being shut down, thousands gathered for Wani's funeral.[22] The shutdown of social media did not deter large crowds from gathering and pelting stones at security forces.

Security officials also pointed out some unintended side effects of a shutdown that work against the state. Before conducting an arrest or capture of a militant leader, the government might shut down the internet as a preventive measure, to ensure there are no information leaks that may tip off the target. As one police officer highlighted, the loss of internet service is in itself a possible warning sign for militants, who then become more cautious and suspicious of an impending attack against them.[23]

Internet shutdowns also affect local news media organisations. Every year, irrespective of the security situation, the internet is shut down in Jammu and Kashmir on India's Republic Day and Independence Day. A visit of the prime minister to Srinagar is preceded by a blanket mobile internet ban in the city as a security precaution. While this upsets the local population, it

20. Authors' interview with a journalist, Srinagar, 4 February 2019.
21. R Meenakshi, 'Kashmir on the Boil: A Timeline', *The Hindu*, 21 July 2016; *Al Jazeera,* 'Protests in Kashmir Despite Curfew', 11 July 2016. The number of people killed vary in different news reports.
22. Business Standard, 'Thousands Gather for Funeral of Burhan Wani', 9 July 2019, <https://www.business-standard.com/multimedia/video-gallery/general/thousands-gather-for-funeral-of-burhan-wani-37352.htm>, accessed 30 July 2019.
23. Authors' interview with a Jammu and Kashmir police officer, Srinagar, 6 February 2019.

also ensures that Kashmiri online news websites cannot effectively report on the visit. Minimal media coverage of the prime minister's visit does a disservice to the objective of demonstrating state reach from the capital into Jammu and Kashmir, missing an opportunity to reduce the appeal of the militant–separatist narrative espoused by violent extremists.

There is a significant policy gap when it comes to the state creating an alternative narrative to counter messaging online.

There is currently a major disconnect between security officials on the ground and the central government on the ways to deal with terrorist propaganda on the internet. Security officials on the ground pointed out that while several proposals on counter-narratives and draft frameworks from security forces have been submitted, they have apparently not been taken into consideration by the Home Ministry, having been, in these officials' opinion, lost in bureaucratic inefficiency or given inadequate attention.[24]

The state has no policy towards countering radical, extremist propaganda online, other than reporting content to social media platforms and waiting for them to take it down. However, the removal of a few websites or videos does not solve the larger problem, as videos are downloaded almost immediately, quickly going viral.[25]

Law enforcement and security officials who have worked on the ground for years have an understanding of the urgency and importance of creating counter-narratives online through a well-trained digital team that monitors, filters, engages with and creates content that provides alternative thinking and messaging to counter militant propaganda.

Recommendation for Government and Social Media Companies

Recommendations for Government

- While the Indian government has set up a number of cyber security agencies involved in media surveillance (such as the New Media Wing and Electronic Media Monitoring Centre under the Ministry of Information and Broadcasting), and monitoring and analysing content on the internet (such as the proposed National Media Analytics Centre under the Ministry of Communication and Information Technology),[26] it must also

24. Authors' interview with a senior Jammu and Kashmir police officer, Srinagar, 5 February 2019.
25. Authors' interview with a senior newspaper journalist, Srinagar, 7 February 2019.
26. For India's cyber security institutions, see Internet Democracy, 'Watchtower: Mapping the Indian Government's Cyber Security Institutions', <https://

develop legislation that strictly governs these initiatives. To ensure that the government has certain powers to monitor social media for the sake of national security while maintaining individuals' constitutional rights, such as the right to free speech, the government should ensure issues such as surveillance reforms which are currently not covered by the draft Comprehensive Data Protection Bill are addressed.[27] Such legislation should strike a balance between access to certain user information and privacy of citizens' data. This can be done by establishing an independent civil society organisation that is formed by a cross section of data protection analysts and experts, that ensures government requests to access information are legitimate and necessary.

- The Indian government should work with social media platforms and civil society organisations to create a framework that clearly defines extremist/terrorist content, without infringing on constitutional standards of freedom of speech.
- Such a framework should include policies that distinguish between radical propaganda (including material produced by separatist groups) and content that may threaten security and stability. This should be in line with social media platforms' 'statement of rights and responsibilities' or 'community guidelines'. It is important for the central government to work with state governments to help define 'dangerous content', to ensure that frameworks are universal in nature, without taking into account the nature of localised conflicts. By working together with a cross section of state government and civil society groups, the government can set the agenda on what constitutes safe versus dangerous content, with controlled risk of bias mitigated among a variety of stakeholders.
- Government, private sector companies (including technology and social media platforms) and civil society organisations (including teachers, religious leaders and social workers) should work together to develop a framework that discredits and undermines messages of terrorism on the internet. The government should create a programme for engagement with youth leaders, students and young political leaders that remains institutionalised, irrespective of change in administration, specifically educating users in how terrorists use the same platforms as they do.

---

internetdemocracy.in/watchtower/>, accessed 18 March 2019.

27. The Data Protection Bill 2018 provides overarching data protection legislation while introducing important concepts such as collection limitation, data storage limitation, transparency, security safeguards and centralised data protection. See Supratim Chakraborty and Aritri Roy Chowdhury, 'The Personal Data Protection Bill 2018: An Answer to India's Data Protection Issues?', *Business World*, 1 January 2019, <http://www.businessworld.in/article/The-Personal-Data-Protection-Bill-2018-An-Answer-To-India-s-Data-Protection-Issues-/01-01-2019-165633/>, accessed 28 March 2019.

This will help tap into discontent among the youth, listening and offering alternative viewpoints.[28]

- Any counter-narrative propagation by the state should be devoid of political bias or affiliation. An excessively pro-government line can be counterproductive. Any counter-narrative must be to the benefit of Indian security and democracy, not a political party. This can be achieved by having a variety of civil society actors working with the government and technology companies to determine what may work as effective counter-narratives. In Jammu and Kashmir, little work has been done by the government to develop web-based counter-narratives. Such a method should be piloted on the ground and tested for its effectiveness.
- While social media platforms can limit channels of communication for terrorists, it is up to governments to create content that counters terrorist messaging. There should be greater collaboration with social media platforms and civil society organisations to effectively counter speech and ensure its supply to sensitive regions. The government should maintain a full-time digital team based in Jammu and Kashmir that takes into consideration the suggestions and experience of security officials on the ground who are tackling the threat, in a constitutional manner.
- The long-term social impact of internet shutdowns should be carefully considered. Internet shutdowns are resented by the people living in Jammu and Kashmir, causing not only a disruption to the day-to day lives of citizens, but a negative impact on businesses and commerce.[29] The government therefore should reconsider decision-making behind internet shutdowns.
- While the shutdown of internet services is often counterproductive, it appears that it will continue to be used as a tool by the state during times of crisis or perceived crisis in Kashmir. Technology companies should work with the government to find solutions in conflict-prone regions, and in times of crisis, that avoid shutdowns. Based on an interview with a senior member of the National Security Council Secretariat, the authors believe that currently, the state also employs this method due to lack of available technological alternatives.[30]

Recommendations for Social Media Companies

- Law enforcement officials in Jammu and Kashmir have had difficulty in tackling or removing separatist content from social media sites, including content that promotes violence against the Indian state. While

28. Maya Mirchandani, 'Countering Violent Extremism: Lessons from India', Observer Research Foundation, September 2017, <https://www.orfonline.org/research/countering-violent-extremism-lessons-india/>, accessed 24 April 2019.
29. Majid Maqbool, 'Frequent Internet Bans are Slowly Choking Kashmir's Online Businesses', *The Wire*, 18 July 2017, <https://thewire.in/business/internet-shutdowns-kashmir-business-start-up>, accessed 30 March 2019.
30. Authors' interview with a former intelligence officer and member of the National Security Council Secretariat, New Delhi, 30 January 2019.

such content is almost always reported immediately, this paper finds that violent content sometimes remains online long enough for it to be circulated and downloaded widely. Therefore, social media companies should work towards shortening the time between when violent content is reported and when it is removed.

- Technology companies have recently begun to demonstrate their ability to target fake accounts, using algorithms and artificial intelligence to identify patterns of activity that do not necessarily access the content of accounts.[31] While this leads to the weeding out of fake, automated accounts, commonly known as 'bots', automation itself may not be the answer to all such issues. Differentiating between separatist and militant content, for example, should also require human review.
- This paper has also identified a difference of perspective between social media platforms and Indian law enforcement. For example, in the case of Jammu and Kashmir, videos that call for self-determination, or *azaadi* (freedom), are often not removed as they are seen by platforms as 'dissenting videos' and therefore protected speech. However, in Jammu and Kashmir, such material is perceived by law enforcement as having the potential to encourage, support or legtimise violence. The lack of action or unrushed manner of responding to requests from Indian law enforcement by social media platforms in this regard have caused police structures to see these companies as problems in themselves. This should be addressed.
- Social media platforms should consider setting up local micro-research units in Srinagar in association with an Indian research or educational institution such as Tata Institute of Social Sciences or one of the Indian Institute of Technology branches. This would help social media platforms to better understand the type of content that typically circulates in the region and also give assurance to law enforcement of the seriousness of the platform's commitment.
- While platforms work on a community standards policy of reporting content, the process of removing material is regarded by security officials in Srinagar as slow and bureaucratic. Where content reported by law enforcement and government officials does breach policies, platforms should act faster. Improving functionality in conflict-prone regions could involve a suspension of the 'share' button or disabling comments for certain, controversial material, or a pop-up window asking users to confirm if they want to share potentially controversial information.

Kabir Taneja is an Associate Fellow at the Observer Research Foundation.

Kriti M Shah is a Junior Fellow at the Observer Research Foundation.

31. Tony Romm, 'Facebook Removed 3 Billion Fake Accounts over a Six-Month Period', *Washington Post,* 23 May 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 reflect the views of RUSI or any other institution.

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

Cover image courtesy of PPstock/stock.adobe.com.

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)