Digitised Hate

Online Radicalisation in Pakistan & Afghanistan: Implications for India*

Peter Chalk**

Online radicalisation has emerged as an issue of increased concern to many governments around the world. A variety of violent religious, ethno-nationalist, xenophobic and single-issue movements have leveraged cyber platforms to recruit, indoctrinate and inspire, which has served to greatly expand their logistical and operational reach while simultaneously provided greater latitude for the execution of semi-autonomous attacks conducted by so-called "lone-wolf" terrorist actors. These dynamics have been on stark display across Western Europe, North America, the Middle East and Australasia for several

---

* This paper is based on the 2nd KPS Gill Memorial Lecture Series organized by the Punjab Police at Chandigarh on December 11, 2019.

** Peter Chalk is an adjunct senior political scientist at the RAND Corporation in Santa Monica, a subject matter expert with the Institute for Security Governance in Monterey and Associate Editor for *Studies in Conflict and Terrorism.* Dr. Chalk has regularly testified before the U.S. Senate on issues pertaining to national and international terrorism and is author of numerous publications on various aspects of low-intensity conflict in the contemporary world. Before coming to the United States, Dr. Chalk was a professor of politics at the University of Queensland, Brisbane, and a postdoctoral fellow in the Strategic and Defense Studies Centre of the Australian National University, Canberra.

years. However, they are now also being increasingly felt in theatres outside these core "digital" areas, including South Asia. This paper focuses on the manner by which the "virtual world" is impacting on militant extremism in two states that have long been held hostage to rampant terror in this part of the world – Pakistan and Afghanistan. It first discusses the nature of international security in the contemporary era before going on to look at how the Internet causally affects processes of radicalisation, the manner by which this is occurring within the specific Pak-Afghan context and the implications these influences have for India's national security interests. The essay concludes with some thoughts on remedial measures and best practices that can be instituted to effectively counter this growing threat.

The Nature of International Security in the Contemporary Era

In stark contrast to the Cold War, few of today's dangers take the form of overt military aggression stemming from a clearly defined sovereign source. By contrast, conflict and general threat definition have become far more diffuse and opaquer, lacking the simple dichotomies of the linear superpower division between the United States and the Soviet Union. The challenges currently confronting the global community more often stem from non-state actors and non-governmental processes, invariably transcend international boundaries, blur the distinction between civil and military security, frequently interact with one another to exacerbate their individual threat quotient and, for the most part, are not readily deterred by the physical defenses/borders that governments have traditionally relied on to protect their populations and territories.[1] In the

1 Peter Chalk, *Non-Military Security and Global Order: The Impact of Extremism, Violence and Chaos on National and International Security,* Macmillan, London 2000, pp.1-2.

words of James Woolsey, the former Director of the Central Intelligence Agency, "we have slain a large dragon, but now we find ourselves living in a jungle with a bewildering number of poisonous snakes. And in many ways the dragon was easier to keep track of."[2]

There are several fundamental features of the present international environment that are contributing to the spread of this global disorder:

- The emphasis on economic prosperity and power conceived in terms of wealth – itself amplified by the severe wealth disparities that exist in many parts of the world – which has led to the emergence of "black dollar" organisations seeking to satisfy their material aspirations on the back of sustained criminal enterprises.
- The resurgence of atavistic forms of ethno-national and religious identity, which has given rise to a dizzying array of highly fanatical movements that are quite prepared to shed blood in pursuit of their self-defined primordial interests.
- The rapid expansion of international transportation links, communication networks and financial flows, which has facilitated the transnational diffusion of security threats in such a way that novel and unanticipated hazards can quickly arise.
- The growth of unsustainable megacities, which has contributed to environmental degradation, over-population and pollution as well as helped spawn

2 Cited in John Ciccarelli, "Preface: Instruments of Darkness: Crime and Australian National Security," in John Ciccarelli ed., *Transnational Crime: A New Security Threat?,* Australian Defence Studies Centre, Canberra, 1996, p. xi.

squalid shanty towns that have acted as incubators for disease, crime and violence.[3]

One of the more notable threat contingencies that has arisen at the top of this new security agenda is terrorism, which as a phenomenon has, itself, become a far more complex and multifaceted problem for a number of reasons:

- Numerous conflict zones around the world have provided extremist militants with multiple fronts to not only operate simultaneously but also gain extensive first-hand combat experience.
- Globalisation, modern means of communication, increasingly efficient transportation networks and porous borders have all allowed terrorists to operate on a truly international basis, contributed to the growing spectre of volunteer foreign terrorist fighters (FTFs) and facilitated the emergence of a new 'breed' of violent extremist – the *ad-hoc*, amateur lone wolf.
- The proliferation of small arms and light weapons, which has provided terrorists and violent extremist (VE) groups with a range of tactical options that were formerly the reserve of governments and their armed forces. Somalia, Afghanistan, Nigeria, Yemen, Libya and Mali are just a few examples where non-state actors have been able to elevate their attack tempos to the extent that they now match or even supersede those of their sovereign adversaries.
- In many cases militant extremists are increasingly looking to inflict death not so much as a means of expressing identity but as a way of creating it. More specifically, terror is now being used as an all-

3 Peter Chalk, op. cit., p. 3-7.

encompassing end in itself with self-engorging and indiscriminate killing more the rule than the exception.

- Lastly, terrorists have become far savvier and more sophisticated in using information technology and online platforms to indoctrinate, recruit and plan.[4]

The analytical context for this paper is derived from this last aspect.

Online Platforms and their Impact Processes of Violent Extremism

Terrorists and VE groups use the Internet in much the same way as society as a whole does – to communicate, collaborate and convince. Organisations such as Islamic State (IS), al-Qaeda Central (AQC) and its various affiliates around the world, al-Shabaab, Boko Haram, the Taliban and Lashkar-e-Taiba (LeT) – to name but a few – have all exploited online forums and social media platforms to promote their ideologies, justify their actions, recruit foot soldiers, condemn 'infidels,' inspire attacks and encourage lone-wolf actions.

Messages and missives are directed at multiple audiences, although it is minors that are most commonly targeted. Two basic reasons account for this. First teenagers and adolescents have a very heavy online presence. Second, they are highly susceptible to simplistic, yet alluring extremist narratives that routinely emphasise parsimonious solutions to what are, in reality, highly complex problems. AQC and IS are exemplars of modern movements that have sought to leverage social media platforms as a means for simplifying the world and its complex human interactions to a single base denominator

4 For a seminal analysis of the manner by which terrorism has evolved in the modern era see Bruce Hoffman, *Inside Terrorism,* 3rd Edition, Columbia University Press, New York, 2006.

that is specifically tailored for youthful audiences. Although the two groups remain locked in a struggle for ideological supremacy, they have both put out a basic thematic message that routinely stresses highly linear black and white reasoning between right and wrong.

While currently much of the emphasis is on jihadist exploitation of the Internet and digital social media, it would be a mistake to suggest that it is only violent Islamists that have embraced online platforms to foster radicalisation. There are many other entities that have adroitly used these mediums for their own nefarious purposes, including pro-life militants, anarchists, Black Block anti-globalists, environmental and animal rights extremists, and white supremacists.

The far right has been especially active on-line and, indeed, many research groups in North America, Australia and Europe currently see the white supremacist and *jihadi* threats as two faces of the same coin. To give but two examples: In the US, where hate groups such as the Klu Klux Klan (KKK) historically grew primarily out of personal connections and word of mouth, today's xenophobic extremists have mastered how to exploit the Internet to reach, recruit and coordinate among a huge pool of potential racists.[5] And in the UK, the neo-Nazi group National Action (NA) was proscribed in 2016 precisely because of its digital glorification of violence, which has been leveraged to build up a 'fan' base through the use of explicit online material to reach new recruits and vulnerable audiences.[6]

---

5 Farhad Manjoo, "A Hunt for Ways to Combat Online Radicalization," *The New York Times,* August 23, 2017.

6 Sam Christie and Felix Allen, "Who are National Action? Neo-Nazi Terror Group Banned in the UK Who Praised Jo Cox's Killer Thomas Mair," *The Sun,* January 03, 2018.

How then do the Internet and associated social media platforms causally impact on processes of radicalisation?

First, information technology creates more opportunities for radicalisation by breaking down traditional barriers of geography and space, allowing extremists to interact with what would otherwise be unreachable target audiences in a real-time format.[7] In this manner the Internet serves as an accelerant for violent extremism in that it allows individuals to connect in an instantaneous and continuous way, effectively acting as a 'conveyor belt' for incubating would-be terrorists.

Second, social media networks algorithmically connect-like minded individuals and amplify their passions. This is the core of the business model upon which these platforms are based. However, these inter-personal ties and linkages can also channel people into 'echo chambers' where highly emotive content that would otherwise be deemed egregious or highly objectionable in the physical world gains a degree of – if not full – acceptability in cyber space. This self-bolstering dynamic plays an integral role in the reinforcement of extremist messaging, often at a rapid and extensive pace through the posting and reposting of individual tweets by hundreds of other users.[8]

Third, the Internet can give the illusion of strength in numbers where radicals brought together by online journals, blogs, services and chat rooms, more easily see themselves not as individuals but as an active part of a broader, networked

7 Ricard Apau, "Youth and Violent Extremism On Line: Countering Terror Exploitation and Use of the Internet," *African Journal for the Prevention and Countering of Terrorism*, Volume 7, Number 1, 2018, p. 26.

8 Daniel Byman, "An Intelligence Reserve Corps to Counter Terrorist Use of the Internet," The Hoover Institution, Aegis Series Paper No. 1018, 2018, p. 4.

extremist movement that operates nationally, regionally or even internationally.

Fourth, the Internet ensures a degree of anonymity – something that is particularly true for sites that enable encrypted communications such as WhatsApp, Telegram, Kik and Signal. This facet can encourage otherwise risk-averse individuals to engage in actions that they would not normally do in the physical world. More specifically, curious would-be militants may well feel more confident in approaching/contacting 'people of interest' in the cyber world, largely because the initial risk of detection by authorities is low.[9]

Fifth, the Internet offers a 'one-stop shop' for all the information an extremist may need to carry out a violent action – from how to manufacture and place Improvised Explosive Devices (IEDs) to suggestions for alternative, cheap methods of attack (such as the recent tactic of using cars, trucks and vans as ramming weapons) and ways of best publicizing a successful operation. In addition, it opens the way for 'cyber-coaching,' allowing militant leaders to keep in near-constant contact with attackers and prod, encourage, guide and facilitate their actions.[10]

Sixth, the Internet allows individuals to access radical content and entities from the comfort of their own personal space without having to physically attend secret gatherings at a pre-arranged meeting place.[11] In so doing it arguably enhances the potential for self-radicalisation where the entire process takes place online in the absence of any face-to-face contact.

9 See, for instance, Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges*, United States Institute for Peace, Washington D.C., 2006, p. 4.

10 Daniel Byman, op. cit., p. 5.

11 Charlie Winter, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," *Quilliam,* July 2015, p. 7.

This potential gives rise to the spectre of lone-wolf terrorism, a manifestation that is addressed below.

Seventh, the Internet and social media offer a cheap and effective propaganda capability, making it easy not only to disseminate information but also to create and tailor messages that are directly geared to buttress the militants' objectives. This facet reflects the basic fact that modern vectors of information technology allow violent extremists to bypass established media outlets, meaning they are no longer dependent on communication mediums that in the vast majority of cases are vehemently opposed to their ideology and cause.[12]

Eighth, the Internet provides an online platform for infusing terror. By loading videos of highly destructive attacks and posting images that graphically depict how 'traitors' will be dealt with, terrorists can leverage the virtual world to instil fear in enemy audiences and discourage moderates from speaking out against their actions. Multimedia content produced by IS is a classic example of this type of messaging at work. To reference just one example, before the group captured the Iraqi city of Mosul in June, 2014 it rolled out an extensive online campaign with text, images and video that threatened those living there with unparalleled death and destruction if they resisted.[13] Such intimidation was a deliberate tact designed to intimidate the urban population into submission and thereby minimise the likelihood of a local rejection of IS and its ideology.

One common theme running through many of these causal links is the notion of 'leaderless resistance,' which has, in varying degrees, come to characterise the organisational configuration

12 For a general discussion of this see Bruce Hoffman, *Inside Terrorism,* Chapter-5*,* Columbia University Press, New York, 2006.

13 Jared Cohen, "Digital Counterinsurgency: How to Marginalize the Islamic State Online," *Foreign Affairs,* Volume 94, Number 6, 2015, pp. 52-58.

of many terrorist movements in the contemporary era. First developed by Louis Beam, a Vietnam War veteran and former Grand Dragon of the Texas KKK, the main aim of the concept is to base a group on so-called phantom cells that operate independently of one another, but which are able through the combined force of their actions to precipitate a chain reaction that eventually leads to a national/global revolution.[14]

Information technology has been integral to the development of leaderless resistance by facilitating interactions between like-minded militants and providing a vector for circulating and distributing propaganda and information. Cyber-based mediums such as the Internet, chat rooms and online journals have all played a crucial role in ensuring that militant extremists are kept fully abreast of events, allowing for planned responses and attacks that are typically based on their individual initiative. Used in this way, digitised communications technology has both overcome the 'tyranny of distance' and obviated the requirement for orders and directives – thereby precluding the need for a physical group per se.[15]

The adoption of these amorphous and largely ephemeral linked structures marks a significant change in terrorist organisational dynamics, setting the US militia movement, European neo-Nazi organisations, anti-globalist radicals and the global jihadist nebula apart from the more established militant groups of the past. In particular, they have played a pivotal role in fostering what is rapidly emerging as a new norm in violent extremism – homegrown lone-actor terror. Although these individuals lack the training, resources and expertise to

14 Peter Chalk, et. al., *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act,* RAND, Santa Monica, 2005), 45, f/n 11.

15 See, for instance, Peter Chalk, "Grave New World," *Forum for Applied Research and Public Policy,* Volume 15, Number 1, 2000, pp.15-16.

execute large-scale strikes against well-protected facilities, they represent a unique and problematic policing challenge for at least six reasons:

- In many cases lone wolves have no prior attachment to militancy and, hence, may only be peripherally known to law enforcement and intelligence agencies, if at all. This makes them very difficult to track, predict and pre-empt.
- Lone wolves are potentially more prone to extreme acts of violence as their activities are neither defined nor bounded by the organisational constraints that have historically been imposed on members of more structured groups.
- The fluidity of lone wolves provides these individuals with the necessary latitude to initiate and develop independent operational strategies – an advantage that makes them more capable of coming up with new and unforeseen patterns of terrorist attacks
- While lacking the ability to decisively hit so-called 'hard' targets, lone wolves are perfectly able to attack the numerous civilian-centric 'soft' venues that abound in modern societies, such as shopping malls, cinemas, busses, metro/train stations, restaurants and pedestrian pathways. In so doing, they serve to greatly inflate the perceived threat of terrorism as their actions are specifically and necessarily directed against sites, locations and hubs that are integral to the day-to-day lives of ordinary citizens.
- Because they are not dependent on a large organisational structure, lone wolves can indefinitely sustain their activities on a minimum of resources that do not require financial outlays of the size that could attract

the attention of intelligence and law enforcement authorities.

The Pak/Afghan Context

What relevance does all this hold for the specific Pakistan/Afghanistan context? A plethora of terrorist and VE groups exist in the two neighbouring states, operating across a highly fungible border area that the US State Department has repeatedly described as a crucible for global terror. Among the more prolific organisations centred in the region are AQC, its affiliate al-Qaeda in South Asia (AQIS), the Taliban, the Haqqani Network, the Tehreek-e-Taliban Pakistan (TTP), IS, LeT, Jaish-e-Muhammed (JeM), Lashkar-e-Jhangvi (LeJ) and the Islamic Movement of Uzbekistan (IMU). These movements are all a product of the hardening of the religious divide that has occurred in South Asia over the past 20-30 years, engaging in communal violence, vehicle-improvised explosive bombings (VIEBs), drive-by shootings, kidnappings, assassinations and indiscriminate suicide attacks on an almost daily basis.

Although undeniably violent, terrorist exploitation of online platforms in the Pak/Afghan region has historically not been extensive due to the low penetration of social media in this part of South Asia. Indeed, when the Taliban governed Afghanistan, the Internet (along with movies and photography) was totally banned on the grounds that it promoted obscene, immoral and anti-Islamic material.[16]

However, in both states exposure to the Internet has risen with the passage of time. In Pakistan, the rate of penetration has increased from 15.5 per cent of the population in 2017, to 22.2 per cent in 2018 to 33.6 per cent in 2019 and there are

16 "Taliban Blackbans the Internet," *CNN.com*, July 13, 2001.

now over 70 million broad band users in the country.[17] While the vast bulk of these people go online for purely innocuous reasons there are growing indications that violent extremists are exploiting these mediums to further their own logistical and operational designs.

In 2017, a survey by the national *Dawn* newspaper found that 41 of 64 proscribed groups in Pakistan, including sectarian, Islamist and nationalist extremists, maintained an extensive presence on *Facebook* in an official or unofficial capacity. The site was variously being used to propagate militant ideology, glorify fighters, provide updates on a particular movement's activities and post pictures and videos. Some of the site's pages were organised by district or electoral constituency and many were published in languages other than English such as Urdu, Baloch and Sindhi.[18]

That same year, the banned Jamaat-ud-Dawa (JuD) – which acts as the charity arm of LeT – organised a series of social media workshops at Multan, Rawalpindi and Lahore to invite volunteers to join efforts in creating unrest in Jammu and Kashmir. Anti-Indian jihadist groups based in the region currently have around 17,000 fake *Twitter* accounts and are actively working through encrypted sites such as *WhatsApp* to instigate protests and riots in the valley.[19] Significantly, these same platforms have been used to establish operational and logistical links with AQIS, a Karachi based affiliate of AQC that was set up in 2014 to battle governments in Pakistan,

17 "Internet World Stats Usage and Populations Statistics: Pakistan," online at https://www.internetworldstats.com/asia/pk.htm; "Total Broadband Users in Pakistan Hit 70 Million," *The Express Tribune,* June 2, 2019.

18 Jahanzaib Haque and Omer Bashir, "Banned Outfits in Pakistan Operate Openly On Facebook," *Dawn,* September 14, 2014.

19 "JuD to Conduct Social Media Workshops to Create Unrest in Kashmir," *Asian News International,* April 4, 2017.

Afghanistan, Myanmar and Bangladesh in order to establish an Islamic State in South Asia.

Telegram is a further (encrypted) site that is increasingly being accessed in Pakistan. IS first used the platform to officially confirm the establishment of its Afghan-Pak Khorasan (ISK) province under the command of Hafiz Saeed Khan Orakzai on January 11, 2015, releasing a series of videos through its media office with the following pronouncement:

> There is no doubt that Allah the Almighty blessed us with *jihad* in the land of Khorasan. All of this is for the sake of establishing Shariah. Know that the Islamic Caliphate is not limited to a particular country. These young men will fight against every disbeliever, whether in the west, east, south or north.[20]

Since then, IS has adopted *Telegram* to target and recruit university students, doctors, engineers, lawyers, journalists, businessmen and other professionals who are increasingly being groomed as a mainstream membership element; announce responsibility for major attacks inside the country such as the suicide bombing of the Government Hospital in Quetta on August 8, 2016, that left more than 70 dead and another 130 injured; and verify tactical and transactional partnerships that have been forged with LeJ and other local groups such as Lashkar-e-Islam (LeI) and Jamaat-ul-Ahrar (JuA).[21]

The TTP is another group that has leveraged *Telegram*, in this case to claim responsibility for bombings, share tactical

20 Center for Strategic and International Studies Backgrounder, "Islamic State Khorasan (IS-K)", 2018, https://www.csis.org/programs/transnational-threats-project/terrorism-backgrounders/islamic-state-khorasan-k.

21 Kunwar Khuldune Shahid, "Islamic State Comes for South Asia," *The Diplomat,* June, 2019.

information and facilitate the dissemination of electronic publications. In this latter respect the group has increasingly focused its attention on exploiting he platform to radicalise young women, using the site to launch an online magazine in 2017 (named Sunnat-e-Khaula) that calls on females to join the ranks of the *mujahideen* and learn how to use combat weapons such as grenades and assault rifles.[22]

In a more general sense, the Internet has helped to fundamentally transform the perceived nature and character of the typical militant in Pakistan. As Bruce Hoffman, a Senior Fellow for Counter-Terrorism and Homeland Security at the Council on Foreign Relations has observed:

> The past stereotype of a jihadist from the mountains in traditional garb with bandoliers of ammunition slung over his shoulder has been replaced. The new generation consist of well-educated, cosmopolitan, university-educated Pakistanis drawn from middle-class backgrounds who can navigate our globalized society, whether virtually or physically, with ease and confidence.[23]

Although not as extensive as Pakistan, Internet access in Afghanistan has also shown a demonstrable increase in recent times, rising from just 6 per cent of the population in 2013

22 Madeeha Anwar and Pir Zubair Shah, "Pakistani Taliban Try to Broaden Reach with Women's Magazine," *Voice of America,* August 5, 2017. The TTP's emphasis on women reflects a growing appreciation of the operational, logistical and psychological benefits this particular demographic has to offer: females can penetrate targets more easily than men largely because modesty in the Muslim religion precludes more concerted body checks on them; they provide a critical support base as financiers and propagandists; and their attacks generally generate a higher shock value (as females are typically viewed as preservers, rather than takers of life).

23 Cited in "ISIS Courts White-Collar Recruits in Pakistan," *CBS News,* March 2, 2016.

to 17.6 per cent in 2019.[24] Currently about 40 per cent of households in the country have access to the Internet.[25] Again at least some of this online presence has been tied to terrorist and VE groups, including the Taliban, IS and AQC.

After being forcibly removed from power in 2001 the Taliban systematically moved to expand its leverage of information technology, increasingly viewing virtual platforms as a highly conducive forum from which to launch electronic propaganda warfare. The movement currently possesses several Internet domains, although the main one is *Alemarah*. The site is not interactive, mainly acting as a one-way dissemination tool. It is published in Pashto, Dari, Urdu, Arabic and English languages, which allows the group to target a variety of audiences, locally, regionally and internationally.[26]

The Taliban also makes extensive use of social media to distribute videos, films and electronic propaganda to countless Afghan cell phones at a time, as well as maintain contact with journalists, much of which is orchestrated through outlets such as *Facebook*, *Twitter* and *YouTube*. The movement has established an official media committee to oversee this effort and has reportedly set up a professional production studio, *Al-Shahamat*, to generate digital content. These same sites are used to reach foreign financiers/sympathisers and communicate with sister groups in other parts of the world.[27]

---

24 "Internet World Stats: Usage and Population Statistics: Afghanistan," online at https://www.internetworldstats.com/asia/af.htm.

25 Ezzatullah Mehrdad, "Inside Afghanistan's Online Battlefield: Social Media Provides Another Front for Battle between the Afghan Government and the Taliban," *The Diplomat,* October 2019.

26 Thomas Johnson, et. al., "The Taliban's Use of the Internet, Social Media Video, Radio Stations and Graffiti," in Thomas Johnson ed., *Taliban Narratives: The Use and Power of Stories in the Afghanistan Conflict,* Oxford Scholarship Online, Oxford, 2018.

27 Bashir Ahmad Gwakh, "The Taliban's Internet Strategy," *Radio Free Europe,* September 9, 2011.

Since commencing operations in Afghanistan in 2015 – formalised by the announcement of its ISK province that same year – IS has used hundreds of fake accounts on *Facebook*, *Twitter*, *Instagram* and *Telegram* to find recruits and promote the group's ideology and propaganda. These efforts have borne dividends and are generally thought to have played a significant contributory role in helping to build an active multi-national membership that is now conservatively estimated to number between 3,500 and 4,000 fighters.[28]

IS has also leveraged the Internet and social media platforms to export its violent ideology to the West. The group released congratulatory videos following the 2016 attacks in Orlando, Florida and Magnaville, France and has subsequently used cyber-space to inspire, direct and authorise additional autonomous-cell and lone wolf attacks in both the United States and Europe.[29]

For its part, AQC has used the Internet and social media platforms to tap into the plethora of local grievances that abound in Afghanistan – ranging from physical insecurity to government corruption, poverty and growing social inequality – and incorporate these into a wider, all-encompassing Islamist narrative aimed at furthering popular legitimacy and justice. Mimicking similar efforts in countries such as Yemen, Syria, Libya, Turkey and Pakistan, the ostensible aim has been to generate and solidify a unique 'glocal' self-identity that is now emerging as the foundation for an all-encompassing grand

28 Claire Parker, "The Islamic State is Far from Defeated. Here's What you Need to Know About Its Affiliate in Afghanistan," *The Washington Post,* August 19, 2019; Abdul Basit, "IS Penetration in Afghanistan-Pakistan: Assessment, Impact and Implications," *Perspectives on Terrorism,* Volume 11, Number 3, 2017, p. 23.

29 Center for Strategic and International Studies, op. cit., 2018.

strategy to guide AQC's evolving operational trajectory – both in Afghanistan as well as other key theatres around the world.[30]

Implications For India

Terrorist and violent extremist use of the Internet and online platforms in Pakistan and Afghanistan has direct relevance for the national security of India. As noted, *Twitter* is already being used to promote riots and protests in Kashmir and now that the province has been stripped of its special autonomous status[31] groups such as LeT (acting through JuD) will doubtless seek to escalate the tempo of this unrest through other online mediums.

In addition, Islamabad's Inter-Services Intelligence (ISI) Directorate, which has a long history of backing anti-Indian outfits operating in the disputed territory, may well leverage encrypted social media sites, secure telecommunication platforms and online mapping technology to covertly facilitate jihadist recruitment drives or directly support terrorist strikes in the region. The 2008 Mumbai massacre, which resulted in 164 fatalities and over 300 injured, is germane in this regard. The perpetrating group is widely regarded to have been the Kashmir-oriented outfit, LeT, and the ISI is generally considered the key supporting agency that bankrolled and guided the attack. Notably, the 10 terrorists who conducted the operation received orders from their handlers in Pakistan via Voice over the Internet Provider (VoIP) phone services and

30 Bruce Hoffman, "Al-Qaeda's Resurrection", *Council on Foreign Relations*, March 6, 2018.

31 In October 2019, the Modi government formally revoked Jammu and Kashmir's constitutional autonomy and split the disputed state into two federal territories that would be ruled directly from Delhi. The move was aimed at integrating what many viewed as an outlying province back into the mainstream Indian polity.

were able to quickly navigate their way to targets across the city with the assistance of digitiSed Google Earth images that were transmitted from Islamabad.[32]

Ominously a high-level meeting between the ISI and various terror groups took place in Islamabad in 2019, during which a plan was reportedly fleshed out to conduct fresh attacks in Kashmir and other parts of the country. Among those in attendance were representatives from JeM and LeT.[33] The former was behind the 2019 Pulwama attack that left 44 police reservists[34] dead, while as noted, the latter is widely believed to have been responsible for the 2008 Mumbai atrocity. Should another incident on the scale of either of these two events occur, it could trigger a severe Indo-Pak stand-off that, if not carefully managed, could quickly escalate to the level of a major military confrontation between the two nuclear-armed states.

Because information technology has been so integral to the genesis of leaderless resistance - which as an organisational construct has as much relevance for extreme Islamist movements as the far right – it could also be effectively used to inspire and endorse militant strikes by lone or semi-independent actors in India. Working from its enclaves in Afghanistan, IS has been doing this for some time with regards to attacking the West and there is no reason why similar action could not be undertaken that targets prominent cities such as Delhi, Mumbai, Bangalore, Chennai or Ludhiana.

---

32 Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks," *The New York Times,* December 8, 2008.

33 Jitendra Bahadur Singh, "Desperate for International Attention, Pakistan's ISI Meets Terror Groups to Plan Attacks Across India," *India Today,* September 10, 2019.

34 Personnel of the Central Reserve Police Force, CRPF.

The virtual links that AQIS has established with Kashmiri militants could also serve as a medium through which to encourage and instigate attacks in northern India. Undertaken as part of the overall objective to establish a Muslim State in South Asia, this would conceivably be of considerable interest to AQC as it would signify the effective Islamisation of a conflict that has long acted as a major thorn in Delhi's side. When taken in the broader context of AQIS' growing ties to the Taliban and the group's increasingly explicit moves to hijack the rapidly expanding Rohingya crisis in Bangladesh and Myanmar, this would represent a major surge in AQC's regional operational capabilities, directly threatening the stability of India's wider geo-strategic neighbourhood. Such a scenario could become a real possibility should a US troop drawdown occur in Afghanistan – something that Donald Trump, the former US President has repeatedly called for – as it would create a void that terrorists and VE groups would no doubt quickly seek to fill by leveraging instruments of both physical and cyber power.[35]

Lastly, an intensive social media effort aimed at radicalising young Sikhs is currently being waged by pro-Khalistani militants based in Pakistan and Diaspora groups operating out of the US, UK and Canada. There are growing indications that the ISI is orchestrating much of this activity as part of a wider campaign to co-join instability in Punjab with unrest in Kashmir. Indeed, the aforementioned 'terror conference' that the Directorate organised in 2019 also included leading members of the Khalistani Zindabad Force (KZF), which according to intelligence sources in Delhi were strongly urged

35 The Soufan Center, *Al-Qaeda in the Indian Subcontinent: The Nucleus of Jihad in South Asia,* New York, January 2019, p. 10.

to make their operational channels available for facilitating attacks across India as a whole.[36]

Conclusion: Responding to Online Radicalisation

All of this begs the question of exactly how should South Asian governments respond to and counter online radicalisation? Action in this area will require governments, civil society groups and the private sector to join and collaborate in fine-tuning best practice solutions.

Thus far, most of the focus has been on introducing legislation and initiatives that allow governing authorities to identify, block and expeditiously delete any malignant electronic information or communication that is deemed to pose a national security risk. In Pakistan, for instance, a series of laws are in place to prevent the misuse of the Internet and social media platforms, including the Prevention of Electronic Crimes Act (PECA) , the Anti-Terrorism Act (ATA), the Investigation for Fair Trial Act (FTA), the National Counter-Terrorism Authority Act (NACTA) and the National Plan for Countering Terrorism and Extremism (NPCTE).[37] Islamabad has also implemented measures for bottom-up social media and monitoring, introducing a digital portal and mobile app called *Surfsafe* to encourage Internet users to anonymously report any extremist or online hate content they come across.[38]

While such measures may work to temporarily disrupt the propaganda, recruitment and operational activities of terrorist

36 Jitender Bahadur Singh, "Desperate for International Attention, Pakistan's ISI Meets Terror Groups to Plan Attacks Across India, op. cit., 2019.

37 "Legal Provisions on Fighting Extremism: Pakistan," The Law Library of Congress, https://www.loc.gov/law/help/fighting-extremism/pakistan.php; "Pakistan Passes Controversial Cyber-Crime Law," *Reuters,* August 12, 2016.

38 Madeeha Anwar, "Pakistan Launches Application to Combat Cyberextremism," VOA, January 30, 2018.

and violent extremist groups, they are essentially stop-gap remedies that militants can quickly overcome by switching to other platforms, communicating through VoIP services, accessing Virtual Private Networks (VPNs), opening new accounts or simply operating through proxies. These initiatives may also serve to merely drive militants further underground by seeking refuge in the 'dark web' where they are effectively beyond the reach of any formal monitoring mechanisms.

Just as importantly, approaches along these lines have very real implications for three intrinsic values that most democratic nations hold as sacrosanct: freedom of speech, the right to privacy and net neutrality. Pakistan's PECA, which was introduced in 2016, is a case in point. The legislation has been widely criticised for containing poorly defined terminology as to what constitutes cyber terrorism, how this differentiates from cybercrime and what mechanisms are in place to ensure any censoring activities are necessary and enacted for the greater public good.[39]

A more holistic and effective response would involve directly intervening in the process of radicalisation. Bringing communication experts and civil society groups together to develop and execute alternative messaging campaigns that credibly challenge the foundations of terrorist propaganda are essential to this effort, as is promoting awareness and education among the youth so they can make critical and informed choices about what they see and read online. To the extent possible, these should be run as government-independent programs as lessons (good and bad) from the UK, France, Saudi Arabia, Singapore and Indonesia, among others, have all shown this is

39 Matthew Marcus, "Pakistan's Assault on Digital Rights," *The Diplomat,* February 27, 2017; Farieha Aziz, "Pakistan's Cybercrime Law: Boon or Bane?"*, Heinrich Boll Stiftung,* February 14, 2018.

the best way of maximising the prospects they will be viewed as unbiased and neutral in terms of content and direction.

The UK's PREVENT program is a case in point. Instituted as an integral component of the country's Counter-Terrorism strategy (CONTEST), it is essentially aimed at pre-empting vulnerable populations from being radicalised and drawn into violent extremism. Part of this endeavour involves the use of grassroot organisations, specialist public relations agencies and media companies to develop on-line and off-line alternative and counter-narratives that are then directed at those deemed to be most at risk to terrorist recruitment. However, overseeing this work is a secretive government department called the Research, Information and Communications Unit (RICU), the activities of which was for many years kept from public scrutiny. When investigative journalists revealed the extent of RICU's behind the scenes role in 2016, PREVENT's strategic communications effort suffered a serious setback simply because it could no longer be presented as an independent, community-based campaign.[40]

It is crucial that efforts to develop cogent and consistent alternative and counter narratives on the Internet are accompanied by corresponding measures taken in the physical world. There are numerous places of religious worship and instruction in Afghanistan and Pakistan that exist in the absence of official control and which have been tied to inflammatory preaching and teaching of the sort that fans the ardour of violent extremism. The hate-laden public sermons and lectures put out by these ostensibly legal organisations need to be checked – if not entirely eliminated – as in many cases they eventually find

40 Ben Hayes and Asim Qureshi, "Going Global: The UK Government's 'CVE' Agenda, Counter-Radicalization and Covert Propaganda," *tni,* May 10, 2016.

their way onto social media platforms in the form of brazen video messages and clips.[41] Again, it is vital that any action taken in this area emanates from accredited, locally respected and independent religious scholars and community elders. If there is even a slight suspicion that the moderate messaging campaign is being controlled or directed by the government, its overall credibility is likely to be seriously jeopardised.

In all cases timing is key. There is often a brief window of opportunity to positively influence an individual who has exhibited an initial interest in an extremist ideology. If the intervention comes after a decision has been made to join the cause or commit a violent act, it will almost certainly be too late.[42] For instance, research conducted in Europe and Asia has shown that when jihadists began planning their trips to join the Taliban and AQC in Afghanistan and IS in Syria and Iraq, they were too far down the extremist path to receive, much less accept, any new information that was presented to them as to why they should not go.[43]

Tech companies, big and small, must also move to proactively champion digital resilience by ensuring that condemnations, refutations and alternatives to terrorism are sufficiently present and accessible online. Ad targeting, one of Google's most effective marketing technologies, could be leveraged to ensure that these missives are consistently pushed to online users who exhibit traits that may abet radicalisation.[44]

41 Mina Sohail, "Fighting Terrorism on Social Media: Pakistan Is Trying to Combat Terrorist Organizations, with Mixed Results," *The Diplomat,* March 2015.

42 See for instance, Jytte Klausen, *A Behavioral Study of the Radicalization Trajectories of American 'Homegrown' Al-Qaeda-Inspired Terrorist Offenders,* US Department of Justice, National Criminal Justice Reference Service, Washington D.C., November 2016, p. ii.

43 Farhad Manjoo, op.cit., 2017.

44 Ibid.

Finally, there is room for developing responses that have a more tactical and strategic bent, especially in the short-term. Police forces, spy agencies and service providers could, for example, all usefully exploit the online interactions of terrorists and extremist sympathisers to gain intelligence on their activities and gather evidence that can then be used for prosecutorial purposes. The Afghan government is moving in this direction and now regularly (if not systematically) monitors social media pages to identify and arrest those who post messages in support of the Taliban.[45] If developed adroitly and with due consideration for oversight and accountability, such interventions could pay dividends in terms of blunting violent online logistical and operational designs.

Digitisation represents one of the modern world's most liberating innovations. It is essential that this communication tool is used for the purpose it was created – to promote knowledge, debate, discussion and inclusivity – rather than subverted to sow the seeds of intolerance, hatred and violence.

45 Ezzatullah Mehrdad, op. cit., 2019.

SOUTH ASIA TERRORISM PORTAL

SOUTH ASIA TERRORISM PORTAL (SATP) is a major platform for the projection of data, research, analysis and news on terrorism in South Asia, and provides critical new inputs for the counter-terrorism effort. SATP is the largest and most comprehensive Portal of its kind, and already contains over 85,000 pages of information.

Unique features include assessments and background reviews of all major internal conflicts in the South Asian region, an extensive coverage of major terrorist outfits through individual profile pages, and timelines for each conflict. TERRORISM UPDATE, a news briefs page, is updated on a daily basis. Researched articles published in FAULTLINES: THE K.P.S. GILL JOURNAL OF CONFLICT & RESOLUTION and the South Asia Intelligence Review are available for free download. The database, information, research material and various other features on SATP are continuously expanded.

SATP is a project executed under the aegis of the Institute for Conflict Management (ICM), a registered non-profit society which seeks to focus on various problems and issues related to terrorism, insurgency, low intensity warfare and other sources of internal strife in South Asia. FAULTLINES is a sister project that is also promoted by the ICM.

Visit us at: www.satp.org