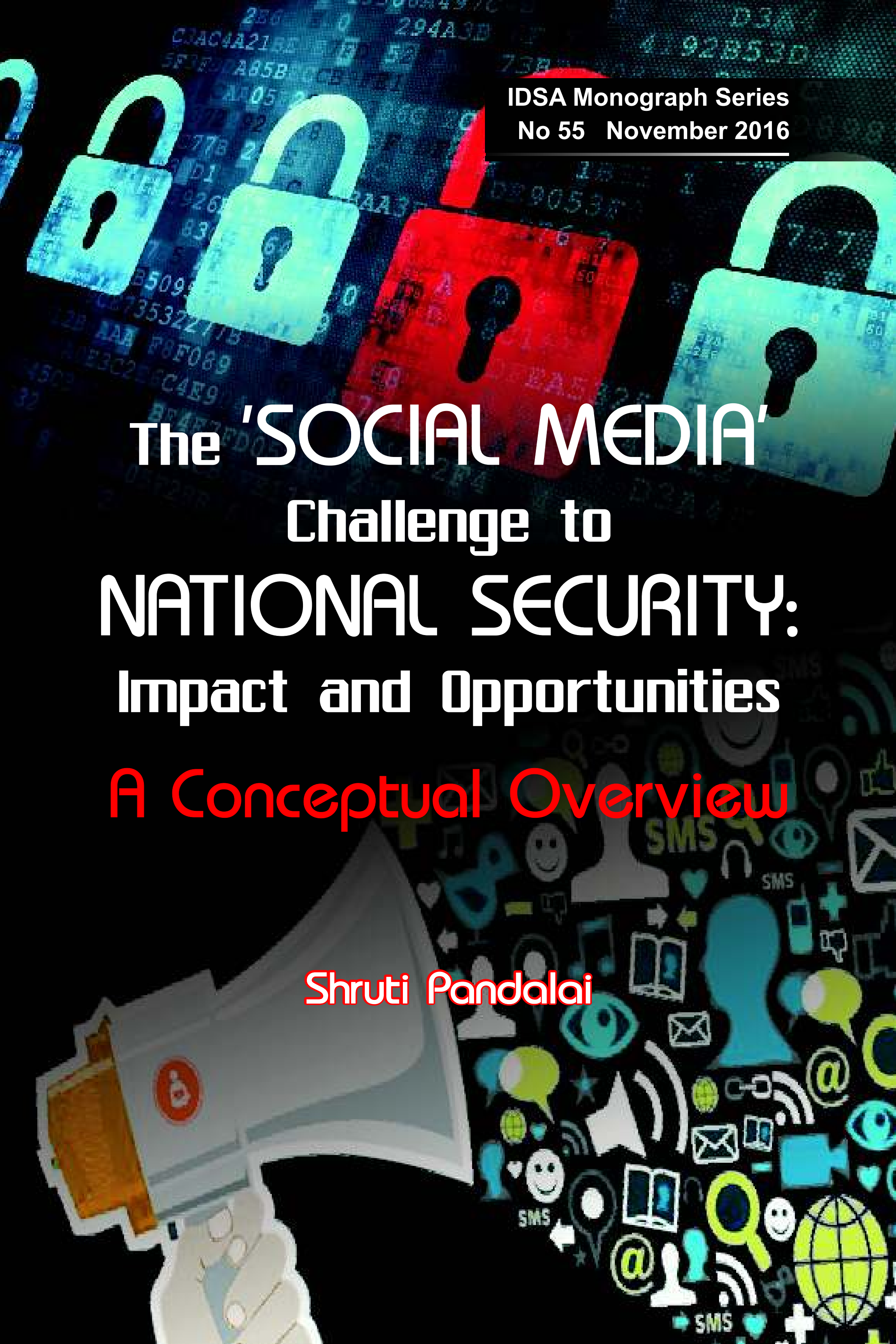
IDSA Monograph Series
No 55 November 2016

The 'SOCIAL MEDIA' Challenge to NATIONAL SECURITY: Impact and Opportunities

A Conceptual Overview

Shruti Pandalai



IDSA Monograph Series
No. 55 November 2016

The 'Social Media' Challenge to National Security: Impact and Opportunities

A conceptual overview

Shruti Pandalai

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-93-82169-68-0

Disclaimer: The views expressed in this Monograph are those of the author and do not necessarily reflect those of the Institute or the Government of India.

First Published: November 2016

Price: Rs. 150/-

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram
Marg, Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
E-mail: contactus@idsa.in
Website: http://www.idsa.in

Layout &
Cover by: Vaijayanti Patankar

Printed at: M/S Manipal Technologies Ltd.

Contents

Acknowledgements

Never before have our traditional understandings of concepts of security been challenged, as much as they have been, in the ever evolving landscape of technology. Social Media represents one such facet of this untamed universe, which is constantly testing our conventional understanding of the nature of risks to national security. While superficially the risks seem to outweigh the opportunities, a more nuanced understanding of the potential benefits of technology as a force multiplier, has been my key take away from this project.

This publication has been the result of a series of projects undertaken for various arms of the government of India in conjunction with the Institute of Defence Studies and Analyses. It was 2013 when I first started working on the project and since then many of the recommendations made by the author have been considered for implementation.

I am grateful to Dr Arvind Gupta, Deputy, National Security Advisor and former Director General IDSA and Brig (Retd.) Rumel Dahiya, former Deputy Director General, IDSA , both of whom pushed me to take up this fascinating field of study, which had been worked upon by very few scholars in India thus far. Their constant encouragement, support, and guidance helped me take my first tentative steps to working towards a conceptual framework of understanding the issue.

This author has benefited greatly from the insights provided by Shri Gulshan Rai, Special Secretary for Cyber Security at the Prime Minister's Office and former head of CERT-IN (Indian Computer Emergency Response Team) who patiently answered all my queries and guided my efforts. I am also grateful to Senior officials of the Maharashtra Police’s “Social Media Labs Project” and their partners from the Bombay Technology Centre , especially Mr Vijay Mukhi for their time and interest in my project. My interactions with Mr Nandkumar Saravade, former CEO of Data Security Council of India and current

CEO of the Reserve Bank of India's new IT subsidiary, helped shape my recommendations greatly.

The round table discussions on my initial paper presentations, which drew the expertise of : Shri Hormis Tharakan, Former Chief of The Research and Analysis Wing (R&AW), Shri Alok Vijayant, Director, National Technical Research Organisation (NTRO), Shri Pawan Duggal, Cyber Security Expert and Advocate, Supreme Court, Shri Nawal Bajaj, Director Maharashtra Police Academy and Founder Social Media Labs, Mumbai Police, Shri Sanjay Bahl, Director General, CERT-IN, Mr Ponnurangam K, Founding Head, Cyber Security Education and Research Centre (CERC) IIT-Delhi, Mr Saikat Dutta, Former Editor National Security, Hindustan Times and Mr Raheel Khursheed, Head, News, Politics and Government at Twitter-India , were immensely helpful in building an accurate and comprehensive assessment of the issue and I am indebted to them for sharing their valuable insights.

As a young scholar, one is always grateful when senior scholars at IDSA guide your efforts. The final draft of this publication benefited from the constructive criticism of Ms Prabha Rao , Senior Fellow, IDSA. I would also like to thank Shri Jayant Prasad, DG, IDSA for giving us young scholars opportunities to pursue multi-disciplinary research and encouraging and supporting us to produce publications which place a premium on quality.

Finally, my eternal thanks to my family : my parents - Ravi and Shyamla, my husband - Mohit, my sister- Smriti and my little star Tara , who are my support system. Their faith in my abilities makes me want to better myself and constantly push the envelope.

Shruti Pandalai
Associate Fellow
New Delhi

Chapter 1

Understanding Social Media and its Impact

"The internet is the largest experiment involving anarchy in history. (…) It is a source for tremendous good and potentially dreadful evil, and we are only just beginning to witness its impact on the world stage."[1]

- Eric Schmidt, Executive Chairman, Google and Jared Cohen, Director, Google Ideas

1.1 Introduction

In the internet of things, ideas take a gigantic leap every day and disruption (both good and bad) is the norm. One such disruption which has revolutionised the way information is exchanged in real time has been the advent of Social media. It has triggered an information revolution the world over that has forced people, governments and organisations, both public and private, to rethink strategies on how they manage their information and engage in an increasingly interconnected world. It has challenged information hierarchies, opened up access and produced an entirely new ecosystem of information exchange. Technological innovations are rapid and constantly evolving, making barriers, borders and control irrelevant.

Such unprecedented developments in Information Communication Technologies (ICTs) provide immense potential for successful participative governance initiatives in India. The Prime Minister's Office is leading by example to harness the opportunities provided by the medium to empower the Indian economy. But technology is a double edged sword. It also throws up new challenges in the realm of law and order. and security for governments that need to be dealt with innovatively.

[1] Eric Schmidt and Jared Cohen, *The New Digital Age - Reshaping The Future of People, Nations and Business*, John Murray, London, 2013.

Social Media and *Social Networks* in actual terms *differ* as social media is a communication channel that transmits information to a wide audience and is usually a one-way street, while social networks facilitate the act of engagement between likeminded people, groups or communities.

However, as pointed out in the Department of Electronics and Information Technology (DeitY) draft of the *"Framework and Guidelines for Use of Social Media for Government Organisations"*[2]– more often than not social media in recent times has become synonymous with social networking sites like *Facebook*, *YouTube*, and micro-blogging sites like *Twitter*. It can hence be broadly defined as any "web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user content."

1.2 Growth of Social Media in India

The latest figures peg social media users in India at 143 million and a 100 percent jump in the number of users in rural India from 2014 to 2015.[3] The report by the Internet and Mobile Association of India says, "The fact that almost two thirds of the users are already accessing social media through their mobiles is a promising sign. With the expected increase in mobile traffic the number of users accessing social media on the mobile is only bound to increase,"[4] Despite internet penetration not crossing 16% of the population, the availability of low cost mobile devices has become a game changer.[5]

[2] For more see: "Department of Electronics and Information Technology Framework & Guidelines for Use of Social Media for Government Organisations", p. 6, accessed on URL: https://negp.gov.in/pdfs/Approved_Social_Media_Framework_and_Guidelines%20_2_.pdf, on 1 September 2013.

[3] "Use of social media doubles in rural India", *The Hindu*, 20 June 2015, accessed on URL: http://www.thehindu.com/sci-tech/technology/internet/social-media-use-doubles-in-rural-india/article7334735.ece on 15 May 2016.

[4] Ibid.

[5] "Mobile Internet users in India to reach 371 mn by June 2016", *The Indian Express*, 4 February 2016, accessed on URL: http://indianexpress.com/article/technology/tech-news-technology/mobile-internet-users-in-india-to-reach-371-mn-by-june-2016/, on 15 May 2016.

India ,with an estimated 371 million Mobile internet users, is the largest market for social networking site *Facebook* after the US.[6] Of its 142 million strong user base in India, 133 million access the social media platform through their mobile phones.[7] *YouTube*, Google's video sharing website, gets 60 million hits a month in India.[8] Micro-blogging site *Twitter* has 22.2 million users in India, making it its third largest user base in the world.[9] These numbers are mind boggling and have far reaching implications in terms of security, law and order.

Government agencies may not be able to match pace with the radical innovations in technology, but they will have to be proactive in their engagement and outreach efforts in e-governance, ensure collaboration of citizens and building of secure communities, and have standard operating procedures in place which could be operationalised in times of emergency.

1.3 Impact of social media and new challenges.

For the Indian government, the internet remains the chosen platform for socio-economic empowerment schemes, which also makes India uniquely dependent on internet platforms for its development while, at the same time, it heightens the risks of India's vulnerabilities.[10]

[6] Ibid.

[7] "Facebook user base crosses 142 million in India", *The Livemint*, 9 March 2016, accessed on URL: http://www.livemint.com/Consumer/tv2ZJPoaI6jldOZhZKkw4J/Facebook-userbase-crosses-142-million-in-India.html on 15 May 2016.

[8] Yuthika Bhargava, "YouTube sets eyes on Indian mobile Internet users", Hindu Business Line, 16 June 2014, accessed on URL: http://www.thehindu.com/business/Industry/youtube-sets-eyes-on-indian-mobile-internet-users/article6120220.ece on 16 June 2014.

[9] "India Has 22.2 Million Twitter Users: Report", *The Huffington Post*, 28 January 2015, accessed on URL: http://www.huffingtonpost.in/2015/01/28/twitter-india-userbase-report_n_6562950.html on 15 May 2016.

[10] Report on CYFY 2013: India Conference on Cyber Security and Cyber Governance, 14-15 October, New Delhi, organised by ORF-FICCI, accessed on URL: http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf on May 1, 2014.

In the last few years alone, India has witnessed the potential of the social media in co-ordinating large scale protests across the country with the 'India Against Corruption' movement led by Anna Hazare in 2011. While these protests were largely peaceful, they did test the local security infrastructure in terms of sheer numbers. We saw a repeat of events in the aftermath of the tragic Delhi gang rape incident in 2013 where a large number of protestors mobilised themselves with the help of social media.

In a more ugly turn of events, mobile and social network interface was used to send offensive clips and hate messages that triggered panic and mass exodus of north east Indians from large parts of India in the aftermath of the ethnic clashes in Assam in 2012. In September 2013, a morphed video on YouTube was used to fan communal riots in Muzaffarnagar in Uttar Pradesh and led to mass panic. These incidents snowballed into a cyber-security challenge and exposed a facet of the medium that could be exploited by anti-national elements and required immediate attention.

In 2014, the arrest of a Bangalore based executive, Mehdi Masoor Biswas, accused of being the man behind terror group Islamic State's (ISIS) most influential Twitter handle in India, *@ShamiWitness* brought to surface the extent of the threat posed by the misuse of social media at home.[11] Two years on, a propaganda video released by ISIS shows alleged Indian Jihadists fighting in Syria and calling for more Indian recruits to join the cause.[12] The threat has really come to bear upon India and has proved that social media has become a potent tool for radicalisation by terror groups.

This paper will discuss these cases more elaborately in sections ahead.

[11] "Police arrest Bengaluru exec behind ISIS Twitter handle @ShamiWitness", *firstpost.com,* 14 December 2014, accessed on URL: http://www.firstpost.com/india/police-arrest-bengaluru-exec-behind-isis-twitter-handle-shamiwitness-1848493.html on 15 January 2015.

[12] "Islamic State releases video allegedly showing Indian jihadists fighting in Syria", *The Indian Express*, 25 May 2016, accessed on URL : http://indianexpress.com/article/india/india-news-india/isis-releases-video-showing-indian-jihadists-fighting-in-syria-2810827/#sthash.kiSGYOOk.dpuf on 25 May 2016.

In addition to this, we are also witnessing the growth of the "new media phenomena" in India where traditional media (mainly television) is increasingly relying on social media to feed its 24-hour news cycles and picking content and coverage led by social media trends.[13] This symbiotic relationship has doubled the impact on consumers and has given social media platforms more visibility. The convergence of various forms of media—television, social, and online networks as instruments of information and generators of user content—have multi-dimensional implications for law and order as well as security.

Social media's capacity to spread information at extremely high volumes and velocities needs to be tapped into by security and law enforcement agencies to wrest control back from perpetrators of crimes. The answer lies not in blocking the medium, but within the medium itself which provides avenues for engagement, connectedness, and collaboration and can also double up as reservoir of *open source intelligence* if used to its optimal potential.

DeitY's *Framework of Guidelines* has correctly observed that "while at a personal level, the uptake and usage of such media is gaining rapid popularity, use and utility of such media for official purpose remain ambiguous. Many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement and worries of backlash, creating synergies between different channels of communication, compliance with existing legislations, etc."[14] This paper aims to tackle all these issues and investigate the acceptance, scope of engagement and institutionalisation of a social media policy in supplementing efforts of security and law enforcement agencies in India.

[13] For more, see: Shruti Pandalai, "Lessons from 2011: The New Media Revolution is a Strategic Asset", IDSA Policy Brief, 13 January 2012, accessed on URL : http://idsa.in/system/files/IB_Lessonsfrom2011TheNewMediaRevolutionisaStrategicAsset.pdf, on 1 September 2013.

[14] For more, see: "Department of Electronics and Information Technology Framework & Guidelines for Use of Social Media for Government Organisations", p. 6, accessed on URL: https://negp.gov.in/pdfs/Approved_Social_Media_Framework_and_Guidelines%20_2_.pdf, on 1 September 2013.

Chapter 2

Scope, Limitations, Research and Methodology

This paper draws on the author's work over the last three years on the subject for the Ministry of Home Affairs and The National Security Council, who had commissioned projects to study *'The Impact of the Rise of Social Media on National Security*." Many of the project's recommendations have, in the interim, found implementation. The author had set out to evaluate the perceptions, current capacities and challenges faced by security and law enforcement agencies in India while grappling with the phenomenon of social media. The aim was to identify future obstacles including legal challenges and recommend frameworks and best practices which would make social media a force multiplier for security and law enforcement agencies.

Understanding the phenomenon of social media and its implications for security is a vast subject. Hence, this paper limits its scope to focus on how security and law enforcement agencies can use social media platforms *internally*: 1) to inform and engage with citizens to build secure communities which share information; 2) to ensure presence to combat misuse of social platforms to spread malicious rumours which may trigger problems for internal security and law and order, and prepare standard operating procedures for times of emergency; 3) to use data available freely on social media platforms to gauge the mood of citizens on issues, predict patterns and possible flash points of disturbances, and prevent and react to cyber-crimes; 4) to build actionable intelligence which may support human intelligence efforts which could be shared across agencies, with built in safeguards to ensure that there is no encroaching upon the privacy of citizens.

The approach is two pronged: encouraging engagement by building capacity and mining the open source information provided by the platform for actionable intelligence. It is important to highlight that this paper *does not* get into the issue of "mass surveillance" of closed and encrypted messages on social media which has raised concerns of internet censorship, violation of privacy and freedom of speech and expression. The emphasis is on using the medium of social media to combat threats and develop robust counter narratives.

The research questions that seek to be addressed are in the realm of engagement, technology, capacity, process and legal challenges.

Engagement: Has the Indian government and its agencies done enough to use social media as a force multiplier for internal cohesion? How is social media being used by countries abroad to enhance security, law and order? What are the best practices?

Technology: What is social media analytics and how does it work? Does the Indian government have the capacity in terms human talent and Internet Infrastructure to undertake such an exercise?

Capacity and Process: Do we need to think about specialised cadres and agencies to deal with the medium to harness its potential? What have been the lessons learnt so far? Are there pilot projects which can be emulated nationally? What will be the scope of public-private partnerships for the same? What is the framework required for co-ordination between agencies that needs to be refined? How do we institutionalise a social media policy for government agencies going beyond a framework of guidelines?

Legal Tangles: Experts have said the IT Act, 2008, is ill-equipped to deal with the challenges presented by social media and hence there is a rise in breach of privacy cases. What are the prerequisite amendments/ checks and balances that need to be put in place to avoid misuse? What are the terms that need to be re-negotiated with the intermediaries who provide platforms for social media networks? Can there be a balance between security requirements and privacy concerns?

The challenges seem many, but addressing them will provide both clarity and a set of clear recommendations that can be adopted by the agencies concerned.

2.1 Methodology

This paper draws from the author's interviews carried out as part of her ongoing research on the subject. These include over forty primary interviews conducted through 2014 with high ranking officers from the police and security agencies, experts and senior officials from nodal agencies in-charge of cyber security in the country, scientists and academic experts in cyber security, practitioners of cyber law, representatives of social media platforms like Facebook, Twitter and Google, and journalists covering the beat. This author has benefited greatly from the insights provided by senior officials of the Maharashtra Police's "Social Media Labs Project" and their partners from the Bombay Technology Centre as also research in Online Social Media Analytics done by the Cyber Security Education and Research Centre (CERC) at IIIT-Delhi. The literature drawing upon best practices in intelligence and policing using social media is based primarily on experiences of the developed countries.

The paper also draws from a discussion on the author's work presented at a Round Table Discussion of Experts on July 2, 2014 moderated by former Director General of IDSA and the current Deputy National Security Advisor, Dr Arvind Gupta. The Experts included Shri Hormis Tharakan, Former Chief of The Research and Analysis Wing (R&AW), Shri Alok Vijayant, Director, National Technical Research Organisation (NTRO), Shri Pawan Duggal, Cyber Security Expert and Advocate, Supreme Court, Shri Nawal Bajaj, Director Maharashtra Police Academy and Founder Social Media Labs, Mumbai Police, Shri Sanjay Bahl, Senior Consultant, *CERT-IN*, Mr Ponnurangam K, Founding Head, Cyber Security Education and Research Centre (CERC) IIT-Delhi, Mr Saikat Dutta, Editor National Security, *Hindustan Times* and Mr Raheel Khursheed, Head, News, Politics and Government at *Twitter-India*. The discussion and recommendations made during the same have been incorporated in this paper.

Chapter 3

Adapting Social Media for Effective Engagement and Policing: West vs India

3.1 The Western Policing Experience

The leap in technology and advances in internet infrastructure in developed countries has meant that social media is used extensively by many countries to offer better services to citizens and collect and supplement intelligence efforts. Departments adopt different strategies—*Push* (disseminate information), *Pull* (silently observe/ obtain information) or *Engage* (interact and encourage two way communication on social media)—to interact with citizens.[1] They use social media: to establish a voice and presence on the platform and invite citizen engagement, embed information in new media channels that citizens frequent daily, leverage crowds to pull information on security/law and order issues, for co-ordinating community policing efforts and to put a human face on policing.[2]

For example, they use social media to provide beat meetings or neighbourhood police interaction sessions, updates on missing person cases, etc. In UK, the Greater Manchester Police started a program where citizens could join police on the *beat and blog/tweet* about their experiences.[3] Following them, the Vancouver police and the Zurich

[1] N. Sachdeva and P. Kumaraguru, "Online Social Media and Police in India: Behaviour, Perceptions, Challenges", Cybersecurity Education and Research Centre (CERC), IIIT-Delhi, May 2014, Report sent by authors to IDSA Scholar.

[2] "Best Practices in Social Media Adaptation", *The Composite Project : Comparing Police Studies in the EU*, Partly funded by the EU, 2012, accessed on URL: http://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf on 5 Feb 2014.

[3] Sachdeva and Kumaraguru, "Online Social Media and Police in India: Behavior, Perceptions, Challenges", n. 1.

city police, also initiated a programme called *'tweet-a-thons'* that lasted 24 hours. During that time, the forces published all activities on incoming alarm calls and police operations in Twitter messages in order to show the public the broadness of police operations and tasks and in order to build special attention from the media that further increased the number of their followers.[4] Similarly, the Seattle police launched *@GetYourBikeBack* program to help owners get their lost bikes.

Yet, the west also has experience of social media being used to recruit terrorists for the al Qaeda, co-ordinate looting and defy police during the 2011 London Riots and organising flash mobs.[5] Despite the debate on the misuse of Twitter during the Boston Terror Attacks in 2013, the *@bostonpolice* department received a lot of praise for using social media for battling rumours and ensuring citizen safety.[6] In the case of *London Riots* and *Boston Terror attacks*, social media was used effectively to deliver real time data, aid investigation and damage control – lessons from which could benefit the Indian experience and, hence, will be discussed briefly.

3.1.1 The 2011 London Riots

Triggered by protests over a custodial death of a coloured citizen, which snowballed into riots and was characterised by mass looting and violence lasting for several days. Rioters used location specific media technologies to communicate, posted pictures of themselves next to stolen goods, used a smartphone app called *Sukey* to identify physical location of police forces in real time and used Blackberry messenger to co-ordinate attacks.[7] Thus, the UK government found itself legally

[4] "Best Practices in Social Media Adaptation", n. 2.

[5] R. Gupta and H. Brooks, *Using Social Media for Global Security*, Wiley & Sons, Indianapolis, Indiana, 2013, p.14.

[6] Edward F. Davis III, Alejandro A. Alves and David Alan Sklansky, "Social Media and Police Leadership: Lessons From Boston", March 2014, Harvard's Executive Session on Policing and Public Safety, accessed on URL: http://news.harvard.edu/gazette/wp-content/uploads/2014/04/Social-Media-and-Police-Leadership.pdf on 1 June 2014.

[7] Gupta and Brooks, *Using Social Media for Global Security*, n. 5, pp.8-4.

and technologically challenged in the midst of an attack. However, the police and public hit back by using the very same social media technologies to capture rioters and secure their communities.

The Metropolitan Police (MET) and the Greater Manchester Police (GMP) used Twitter extensively to support investigations and to seek information on offenders. Both forces also used the photo-sharing site *Flickr* to publish photos of perpetrators captured on CCTV. GMP further promoted their crowd sourcing efforts and launched a campaign entitled *'shop a looter.*[8] Large posters in the city showed the faces of suspects and asked people to help with their identification. *Twitter* was used to announce the campaign. Both forces provided phone numbers or links to their websites where the public could submit information.[9]

3.2.2 Boston Bombing, 2013

The Boston Police Department (BPD) used the potential of social media for information dissemination and community policing in April 2013 during the very dramatic and constantly developing investigation into the explosion of two bombs at the finish line of the Boston Marathon. BPD successfully leveraged *Twitter* to keep the public informed about the status of the probe, to calm nerves and request public assistance, to correct misreporting, and to ask for public restraint in the tweeting of information from police scanners.[10]

All of the BPD tweets were sent from one official Twitter account, which was directly overseen by BPD's public information bureau chief, lawyer and a former television journalist Cheryl Fiandaca.[11] Assisted by two officers and three civilians, she operated *@bostonpolice* as a 24-hour "digital hub" for information about the investigation. She and her staff were briefed by commanders three to five times per day

[8] "Best Practices in Social Media Adaptation", n. 2.

[9] Ibid.

[10] The information in this section is entirely based on the analysis available in Davis III, Alves and Sklansky, "Social Media and Police Leadership: Lessons From Boston", n. 6.

[11] Ibid.

during this period. BPD tweets rapidly became the most trusted source of information about the status of investigations.

The department also leveraged its popular Facebook page. Through the week, the official page published images of the suspects, license plate information to support a BOLO (Be on the Lookout), a map of the cordoned-off area in the immediate aftermath, maps directing the media to conferences and approved parking areas, and updates about public transit service interruptions related to the investigation.[12] In the days that followed, BPD also used its Facebook page to memorialise the deceased victims and to send messages of condolence and support to survivors. Except for the misidentification of a student named Sunil Tripathi, as a suspect by social media enthusiasts indulging in a public investigation, which led to momentary chaos, the *@bostonpolice* was able to project itself as the authority for information and co-ordination during the crisis and restrict damage.

3.2 The Indian Policing Experience

The acceptance and adaptation of social media into policing and citizen engagement in India has been relatively slower. This has been due to perception barriers stemming from organisational cultures developed over time. There is also apprehension related to lack of clarity on how to use the technology.[13] In addition, the absence of adequate internet infrastructure, lack of immediate availability of talent, shortage of personnel and soft skills required to deal with a medium like social media at local levels has been a challenge.[14] Multiplicity of languages in India require further customisation of technology which, in turn, requires investment, both human and capital as well as re-drawing of budget plans, neither of which have happened on the ground.[15]

[12] Ibid.

[13] Based on Author's interviews conducted with Senior IPS officers Mr Sivanandan, ex DGP, Maharashtra; Mr Nandakumar Sarvade, Former Maharashtra IPS and Cyber Security Expert; and Mr Vijay Mukhi, Cyber Security Expert and Member of Bombay Technology Centre, between 14 and 20 February 2014 in Mumbai.

[14] Ibid.

[15] Ibid.

Despite *DeitY's Framework of Guidelines* encouraging agencies to develop and customise social media policy frameworks for themselves, very few have actually put together frameworks and institutionalised them. Experts who have trained some personnel as a part of pilot projects say the road ahead is a tough since a majority of police personnel in India, who are expected to pick up and engage with this medium, don't even have the basic skills required to deal with computers.

Research conducted to gauge perceptions of police personnel in India on using social media for policing reveal some valuable insights.[16] The sample survey conducted with 445 policemen and 205 citizens exposed a perception gap between law enforcement agencies and people in terms of using social media for policing. Status updates of Delhi, Bangalore, Chennai and Uttar Pradesh police forces on social media were also studied to analyse police interaction.

It was found[17] that officers preferred using social media as a one-way-communication channel to either *push* information or *pull* information rather than as a medium for interaction. It was thought to be an effective tool to monitor and track problems, rumour detection, traffic management, issue advisories, and to understand public opinions on various issues. The utility of these pages for investigation and monitoring was not very clear. However, they recognised top three uses of social media to be crime investigation, intelligence, and public relation/ reputation management. In contrast, for citizens, social media engagement for policing meant notifying the public of crime problems, of emergency situation or disaster related issues, and crime prevention activities.

Police officers expressed concern over multiplicity of fake profiles, threats of sabotage of official pages or that citizens might ask controversial questions, which might create problems for police departments. Questions were also raised on the utility of social media

[16] Sachdeva and Kumaraguru, "Online Social Media and Police in India: Behavior, Perceptions, Challenges", n. 1.

[17] Ibid.

with the state of internet penetration in the country. This despite the evidence emerging from Muzzafarnagar riots where violence spread in rural areas using social media from mobile technologies. Many believed social media would be helpful only when it was available in local/regional languages. The survey responses also emphasised the need from within the police force for a clear policy on the use of social media, with the pre-requisite dos and don'ts, to be conceptualised and institutionalised for the personnel.[18]

It has been noticed that initiatives using social media for effective policing in India has seen efforts which are largely individual or particular state-police force driven. For example, the Maharashtra Police department has launched a SMS-based tracking system called *"Turant Chauvis"* which promises to redress citizen complaints within 24 hours in terms of a first response.[19]

The Delhi Traffic Police too has taken to Facebook and Twitter to ease handling of traffic related issues, while the Indore police use the medium to track criminal activity.[20] Karnataka police, apart from using the medium for traffic management and information dissemination, had also started leveraging social media in 2010 to solve criminal cases establishing a 'HelpKarnatakaCID' page.[21] The Kerala police recently established presence on Facebook and Twitter and are experimenting with more features to enhance service delivery to citizens apart from

[18] Ibid. Similar conclusions were arrived at during conversations conducted by author with senior IPS officers and cyber security experts.

[19] For more see: "Department of Electronics and Information Technology Framework & Guidelines for Use of Social Media for Government Organisations", p. 6, accessed on URL: https://negp.gov.in/pdfs/Approved_Social_Media_Framework_and_Guidelines%20_2_.pdf, on 1 September 2013.

[20] Ibid.

[21] "Karnataka police sleuths on Facebook and Twitter", *Daily News & Analysis (DNA)*, 7 May 2010, accessed on URL: http://www.dnaindia.com/bangalore/report-karnatakas-police-sleuths-now-on-facebook-and-twitter-1393091, on 5 February, 2014.

the online tracking of petitions, reporting of crimes, payment of traffic violation fines and filing of missing children reports that already exist.[22]

However, building an effective two-way engagement with citizens using social media and building communities which help in collaborative policing are goals which currently seem to be far away in the future. Naturally, a force used to strict hierarchy and bureaucracy cannot be expected to change overnight. It is imperative though that a top-down approach that encourages out of the box solutions and adoption of flexibility be initiated to take advantage of platforms like social media for effective governance.

[22] "Kerala Police logs onto social media bandwagon", *KeralaITNews*, 3 February 2014, accessed on URL: http://keralaitnews.com/1629/kerala-police-logs-on-to-social-media-bandwagon on 7 June 2014.

Chapter 4

Adapting Social Media for Developing "Actionable Intelligence"

4.1 Mining social media for intelligence

Law enforcement agencies across the globe are using a superior form of "Open source Intelligence" to engage, collate, analyse and predict, and share intelligence using data gleaned from social media networks, also known as Social media intelligence (SOCMINT).[1] This analysis uses *social media data*, that is, all the user generated data on social media platforms with their *metadata* (which includes information of the user, location, time and date details of post, number of people who viewed and shared the post, etc.) to identify people, networks, patterns and events that contribute to actionable intelligence.[2] This requires *Big Data analysis* skills which include computational techniques to deal with huge amounts of data and the means to sift through them, and collate the results for further analysis.[3] The box ahead displays the relevant problems for analysis and the techniques used for drawing patterns and predicting events from social media data.

[1] R. Gupta and H. Brooks, *Using Social Media for Global Security*, Wiley & Sons, Indianapolis, Indiana, 2013, pp. 45-70.

[2] Ibid., pp. 71-72.

[3] Ibid., p. 72.

Table 4.1 a: Techniques employed for mining open data

Techniques	Description
Social network Analysis	Analysis includes studying social networks, both online and offline, and understanding relationships and individuals that make up networks
Language and Sentiment Analysis	Used to identify patterns in linguistic content on social media platforms that reveal insights on events and behaviour
Volumetric Analysis	Focuses on discovering associative and predictive relationships between events or behaviour and changes in volume or traffic or activity in social media platform.
Co-relation and Regression Analysis	Used to establish association between direct and indirect causal relationships between various factors and things.

Source: Based on information taken from R. Gupta and H. Brooks, *Using Social Media for Global Security*, Wiley & Sons, Indianapolis, Indiana, 2013, pp.69-71.

Table 4.1 b: Relevant Problems for Analysis

Problem Set	Description	Examples
Understand the structure of social networks	Track developments of relationships between people online and offline and understand how they use social media	Identifying the extent and use of social media by criminals
Identify key people and relationships	Determine who in social networks wields influence over people in networks and has the ability to affect their behaviour and relationships	Finding out means and methods by which anti-national elements carry out recruitment and what is their target population?
Determine the proliferation of Ideas in networks	Understand in real time which topics and ideas individuals and groups are discussing and sharing	Identifying violent/ extremist literature rhetoric or offensive material which may spread panic among people if unchecked.
Understand and forecast behaviour	Co-relate behaviour, environmental constraints, and discussions on social media platforms in real time data to determine how individuals or groups might behave in the future	How are criminals using social media to inflame tensions and is their use of the medium changing to avoid policing?
Understand and forecast events	Using real time data on social media platforms and co-relating with events and environment constraints to predict likelihood of specific events occurring in the future.	Determine likelihood of flash mobs, protests and spread of violence in emergency situations.

Source: Based on information taken from R. Gupta and H. Brooks, *Using Social Media for Global Security*, Wiley & Sons, Indianapolis, Indiana, 2013, pp. 45-71.

The success in getting actionable intelligence from social media platforms depends on 1) determining collection needs 2) collection of data 3) filtering of data: noise vs. signal 4) storing and managing data and 5) analysing data using appropriate algorithms and tools.[4]

Notwithstanding the *Wikileaks* and Snowden revelations of mass surveillance and snooping under the NSA Prism programme, the US law enforcement agencies seem to have developed frameworks and security safeguards to institutionalise use of open source social media for actionable intelligence.[5] Whether Indian enforcement agencies should take a cue from their western counterparts in terms of using social media for undercover investigations can be debated as it opens up issues of privacy violation. However, other practices like requirements of strict compliance review, timely review and destruction of recorded data, case by case oversight by a chief information security officer, allowing of news media to report on the agency's social media policy for better compliance and transparency, are practices which can be incorporated depending on the needs and requirements of Indian agencies.[6]

A cautionary note is required here to reiterate that social media intelligence and techniques are not infallible, however refined and institutionalised they may be. For instance, the US Department of Homeland Security (DHS) once ruined an Irish tourist's vacation because of a tweet. In 2012, before leaving for a holiday to the US, Leigh V Bryan excitedly tweeted "he was going to destroy America," only to find himself detained 12 hours later in a cell with Mexican drug dealers, pending an investigation with DHS upon his arrival.[7] Hence, intelligence gathered from social media can only supplement and provide context to hard intelligence gathered by law enforcement agencies and it always needs verification.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] R. Gupta and H. Brooks, *Using Social Media for Global Security*, Wiley & Sons, Indianapolis, Indiana, 2013, p. xxv.

4.2 The Indian Experience: Social Media Labs: success and limitations

In contrast, the Indian experience in using content from open social media platforms for intelligence gathering has been limited to a few pilot projects. Indian police personnel interviewed do believe in the usefulness of social media in providing actionable intelligence in two prominent aspects – rumours that manifest in violent public upsurge and simmering public opinion about various issues.[8] Despite apprehensions remaining over constraints like volume of content generated and need for extensive cyber networks, there was an agreement on the usefulness of the medium's speed of delivering real time data for predicting protests and its reach in emergencies like riots, terror strikes or countering of hateful propaganda which is inciting violence.[9]

The *Social Media Labs* Project:[10] In May 2013,the Maharashtra Police took the first initiative in this direction by setting up a pilot project to track activity on social media to gauge public moods on issues and 'step-up its preparedness' in anticipating and handling sudden flare ups. The first of its kind in the country, the Lab was established with the Mumbai police roping in the industry body NASCOMM (The National Association of Software and Services Companies) for providing technical infrastructure, support and training, and used social media

[8] N. Sachdeva and P. Kumaraguru, "Online Social Media and Police in India: Behaviour, Perceptions, Challenges", Cybersecurity Education and Research Centre (CERC), IIIT-Delhi, May 2014, Report sent by authors to IDSA Scholar.

[9] Ibid. Also, extensive interviews conducted by scholar with senior IPS officials during research for the project.

[10] The information in this section is based on the scholar's interaction with all stakeholders responsible for putting together the Social Media Labs Project. This includes senior officers from the Maharashtra Police, Cyber experts involved in the project, officials from NASSCOMM and Social media monitoring tool provider *SocialappHQs.com*.

monitoring tools provided by Indian technology-development entrepreneurs *SocialAppsHQ*. Rajat Garg, CEO of *SocialAppsHQ.com* says, "The app tracks and provides sentiment analysis, identifies behavioural patterns, influencers and advocates, tracks increase in chatter and generates alerts in real-time on social media platforms."[11] He reiterated that the lab processes only the data that is available on public platforms using algorithms and brings out patterns, which are then further analysed to identify various activities. Thus, the idea is that through automated social media intelligence tools like *SocialAppsHQ.com*, police can now find out anti-social groups actively participating in creating disturbance and take timely and preventive measures, Garg elaborated.

But the software was just one part of the exercise. Senior IPS officers who conceptualised this project told me that 25 police personnel, five officer level and twenty constables, were specifically handpicked for running the 24x7 lab after a rigorous exercise of interviews which gave weight to aspirants with a technology background or interest. Training capsules were designed in collaboration with experts from IIIT-Delhi, cyber experts and technologists in Mumbai, who provided basic hands on training to personnel to engage with the medium. In keeping with the requirements of the Mumbai police force, a list of keywords was prepared which would help the personnel spot trends and identify issues that required immediate attention. The personnel were divided into three shifts and mandated to come up with two reports a day which were sent to all police heads.

Early success: One member of the special team said that despite basic levels of technology, training and relative inexperience of the squad, the pilot project had many deliverables in its short life span. Examples given included:1) gauging of mood in social media helped anticipate a law and order situation when the chief of a political outfit asked party

[11] Interview with Rajat Garg, CEO, *SocialAppsHQ.com*.

[12] "Raj Thackeray booked for violence", *The Hindu*, 14 February 2014, accessed on URL: http://www.thehindu.com/news/cities/mumbai/raj-thackeray-booked-for-violence/article5627711.ece on 1 June 2014.

workers to stop paying tolls and "smash those who ask for it."[12] Having anticipated the backlash, the Mumbai police was able to rein in the violence unleashed by party workers relatively quickly. 2) A cyber expert closely involved with the project also highlighted how the lab has been successful in keeping in check the spread of a lot of communal content available on such platforms. A particular incident involving an offensive picture morphed to show desecration of a religious text was spotted before it went viral and fermented trouble in Mumbai.

Scope and Challenges: Naval Bajaj, Senior IPS officer of the Maharashtra Police, said that there was recognition among the top brass of the state police force that they "could not afford to miss the bus,"[13]and that such initiatives must be replicated throughout the state in the immediate term and also develop the application at a national scale in the long term. It was also pointed out that "policemen cannot be turned into technologists"[14] and there was a need to think of bringing in professionals for such specialised teams. The cyber security experts agreed with the assessment saying that as the scale of projects grow to meet with the growing challenges in the cyber space, constabulary level of talent will not suffice.[15] Technologists pointed out that the operation is currently hamstrung by budgets and to keep pace with events in such active mediums, more sophisticated technology and application platforms would be required.[16] All stakeholders recommended conceptualising architecture for the use of the medium within the legal

[13] Interview with Naval Bajaj, Senior IPS officer of the Maharashtra Police conducted in Mumbai on 20 February 2014.

[14] Ibid.

[15] Interview with Vijay Mukhi, Cyber Security Expert and member Bombay Technology Centre, conducted on 19 February 2014 in Mumbai.

[16] Interview with Rajan Luthra, RIL Foundation, part of NASCOMM collaboration on Social Media Labs Project, interviewed on 18 February 2014 in Mumbai.

framework, allocation of budgets for Public-Private Partnership Models and streamlining standardisation for tools and platforms for the proposed exercises.[17]

In my interaction with experts, three cases were discussed where actionable intelligence generated by *Social Media Labs* could have helped situations:

4.2.1: Protests over Delhi gang rape case December 2012

Public anger over the brutal and horrific rape of a young medical student in a moving bus in the capital and outrage over rising incidents of violence against women in Delhi, found an outlet on social media platforms. People used social media to mobilise and co-ordinate collective action in the form of protests on the street.[18] The Delhi government and police were completely unprepared and had not anticipated the large numbers of protestors who took to the streets in the capital. The police clampdown that followed was criticised heavily as the protests turned violent. In such situations, *Social Media Labs* would be helpful in gauging public sentiment, identifying movement of protestors and key influencers, predicting the scale of protests, and help authorities plan contingencies.

[17] The information in this section is based on the scholar's interaction with all stakeholders responsible for putting together the Social Media Labs Project. This includes senior officers from the Maharashtra Police, Cyber experts involved in the project, officials from NASSCOMM and Social media monitoring tool provider *SocialappHQs.com*.

[18] Ruchira Singh, "Delhi gang rape: People unite through social media to bring the outrage on streets", *IBNLive.com*, 22 December 2012, accessed on URL :http://ibnlive.in.com/news/delhi-gangrape-people-unite-through-social-media-to-bring-the-outrage-on-streets/311769-3-244.html on 1 June 2014.

4.2.2: Assam Riot and mass exodus of North East Indians from urban centres: July-August 2012

It began with ethnic clashes in the North Eastern state of Assam in late July of 2012. Hindu members of the indigenous Bodo tribe clashed with Bengali-speaking Muslim settlers and migrants. More than 300,000 refugees were relocated to a heavily guarded camp; their houses were burned, and 78 people were reported dead.[19] In cities like Bangalore, Pune, Chennai, and Mysore, riots and smaller clashes broke after protests over attacks on Muslims in Assam turned violent.[20] Then, in a sudden development, texts and photographs warning of renewed attacks began circulating throughout urban cities threatening retaliation against non-Muslims from the north east to avenge the attacks in Assam.[21] Train stations were swamped, and refugee camps swelled.[22]

Urban residents received on their telephones texts and doctored photographs of an alleged riot in progress.[23] These morphed images of mutilated bodies were actually doctored from photographs of mass deaths in other contexts (e.g., an earthquake in Tibet in 2008, a 2008 cyclone in Myanmar).[24] The messages went viral on all social media

[19] J.F. Hill, "India's Internet Freedom Nightmare", *The Diplomat*, 25 August 2012, accessed on URL http://thediplomat.com/2012/08/indias-internet-freedom-nightmare/?allpages=yes on 1 June 2014.

[20] Ibid.

[21] Ibid.

[22] "Threats trigger NE Exodus (photo feature)", *Hindustan Times*, 17 August 2012, accessed on URL:http://www.hindustantimes.com/photos-news/photos-india/threatstriggerneeexodus/Article4.aspx on 1 June 2014.

[23] S. Mondal, "Mischief Potential of Social Media in Full Play", *The Hindu*, 17 August 2012, accessed on URL: http://www.thehindu.com/news/cities/bangalore/mischief-potential-of-social-media-in-full-play/article3781473.ece, on 1 June 2014.

[24] Ibid.

platforms triggering mass panic and exodus on North East Indian citizens from various cities.[25] One person was arrested in Bangalore for sending out 20,000 messages.[26]

The misinformation campaign fuelled by social media misuse went unchecked by both media and authorities in the initial phase of rumour mongering. By the time authorities discovered the cause of panic, damage had been done.[27] A diplomatic row proceeded with allegations levelled against Pakistan, which were denied by their government.[28] The Indian government was out of options and decided to ban bulk sms services and block over 300 websites.[29] This move was criticised and the government was accused of shooting the messenger and not dealing with the actual problem with proactive measures.[30] The legal challenges that the government faced in dealing with social media providers and fears regarding internet censorship were many. These will be dealt in greater detail later in the section dealing with the legal regime required dealing with cases for social media.

[25] Ibid.

[26] Johnson T.A., "Man held in Bangalore sent messages to 20,000: probe", *The Indian Express*, 22 August 2012, accessed on URL: http://archive.indianexpress.com/news/man-held-in-bangalore-sent-messages-to-20-000-probe/991361/ on 1 June 2014.

[27] Anil Kumar, "We had no idea this would happen Karnataka Minister Says", *The Times of India*, 18 August 2012, accessed on URL: http://timesofindia.indiatimes.com/city/bangalore/Exodus-of-northeast-people-We-had-no-idea-this-would-happen-Karnataka-minister-says/articleshow/15547895.cms on 1 June 2014.

[28] "India shares evidence on inflammatory content triggering NE exodus with Pak", *The Indian Express*, 29 August 2012, accessed on URL: http://indianexpress.com/article/india/latest-news/india-shares-evidence-on-inflammatory-content-triggering-ne-exodus-with-pak/ on 1 June 2014.

[29] "Centre bans bulk SMSes to end Northeast panic", *The Indian Express*, 18 August 2012, accessed on URL: http://indianexpress.com/article/cities/ahmedabad/centre-bans-bulk-smses-to-end-northeast-panic-3/ on 1 June 2014.

[30] Hill, "India's Internet Freedom Nightmare", n. 19.

Cyber experts point out that with *Social Media Labs*, law enforcement agencies could have understood what was agitating public sentiments and identify and target groups radicalising people. A counter offensive squelching the misinformation campaign could have been launched immediately. Having spotted the offensive images, techniques like "reverse image search" could be utilised to find the true origins of the photos and this information could have been shared through verified accounts of police forces. Intelligence garnered from social media platforms could have also helped first response teams like CERT-In to effectively ban websites spreading malicious content and reduce time lags, rather than imposing an en-mass blockade. In short, more preventive measures could have been employed to assist forces on the ground.

The Assam case has alerted authorities to the growing potential for cyber-attack using social media, where hoax messages are incorporated into a stream of otherwise legitimate messages. It also demonstrated how quickly mobile apps and text services could be misused to disseminate false information.[31] This technology has been identified as *Robot Twitter accounts*, that is, "Accounts that are created by computer code to send the same or highly similar messages onto the Twitter platform, polluting the information stream with messages that appear to come from many different people (rather than just one person)."[32] Keeping up with technological leaps will hence become more imperative.

[31] Rebecca Goolsby, Lea Shanley, and Aaron Lovell, "On Cybersecurity, Crowdsourcing, and Social Cyber-Attack ",*Commons Lab Policy Memo Series Vol. 1*, 26 February 2013, Wilson Centre, accessed on URL: http://www.wilsoncenter.org/publication/cybersecurity-crowdsourcing-and-social-cyber-attack, on 1 June 2014.

[32] Ibid.

4.2.3: Muzzafarnagar Riots in UP in September 2013

Exactly a year later, in September 2013, a fake video shot in Pakistan, showing two boys being killed in the Pakistani city of Sialkot, was reportedly circulated in Muzzafarnagar in Uttar Pradesh, triggering communal riots that killed 40 people.[33] The video was allegedly repackaged to represent a Muslim mob lynching of two boys in communal violence in UP.[34] The incident highlighted the use of social media platforms in rural India via mobile phone technology and the potential to misuse it for communal polarisation.

While the UP Chief Minister and his government blamed social media for fuelling riots,[35] media reports emerged blaming the government for not reacting to information it was sitting on from Meerut, where a right wing party worker has been arrested for posting the video online.[36] There was a clear absence of a sustained information campaign to defuse rumours and social media was not engaged even in the aftermath.

As in the case of the Assam riots, *Social Media labs* could have identified the offensive video and established its manipulation, thereby helping officials correct the spread of rumours and plant an effective counter offensive in terms of an information campaign. It could have also helped target individuals/groups/platforms being used to spread malicious content and provide actionable intelligence to prevent the situation from escalating.

[33] Zia Haq, "A dangerous trend: social media adds fire to Muzaffarnagar clashes", *Hindustan Times*, 9 September2013, accessed on URL: http://www.hindustantimes.com/india-news/a-dangerous-trend-social-media-adds-fire-to-muzaffarnagar-clashes/article1-1119655.aspx on 2 June 2014.

[34] Ibid.

[35] Omar Rashid, "Social media rife with inflammatory material in Muzaffarnagar", *The Hindu*, 9 September 2013, accessed on URL: http://www.thehindu.com/news/national/other-states/social-media-rife-with-inflammatory-material-in-muzaffarnagar/article5110034.ece, on June 2, 2014.

[36] Ibid.

In all of these cases above, it is clear that social media misuse can be stalled by the authorities by using the means provided by the medium itself. The *Social Media Labs* experiment, manned by specialists with clear SOPs (Standard Operating Procedures) on dealing with dissemination of information to counter the medium's manipulation can effectively nip all law and order challenges before they escalate. However, this is easier said than done. This requires an attitudinal change in organisational culture and investment in both capacity and infrastructure that needs to be replicated and not duplicated across agencies and the country.

An additional challenge that has come to the surface over the last year is the use of social media for extremist propaganda, especially the threat of the terror group ISIS.

Chapter 5

Social Media and The Extremist Challenge

5.1 The ISIS 'Virtual' Threat to India

The arrest of a Bengaluru executive in November 2014, accused of allegedly running a pro-ISIS Twitter handle, threw open a Pandora's box on the use of social media by extremist groups for radicalisation and recruitment of youth in India. The 24-year-old Bengaluru-based engineer, Mehdi Masroor Biswas, "confessed" that he was handling the pro-jihad twitter handle, "*@ShamiWitness*, which became "a source of incitement and information" for new ISIS recruits.[1]

It was then that the repercussions of the news of four Mumbai youth, who had gone to Iraq-Syria in May 2014 to join ISIS, began to be felt. While one of them returned a few months later, it was his confession to the National Investigative Agency (NIA) that revealed the extent of his radicalisation. The youth claimed he had come back home succumbing to parental pressure and if given a chance would rejoin the ISIS and fight for the cause.[2] "This despite the fact that ISIS leadership made him clean toilets, indulge in construction work and provide water to those on the battlefield, instead of being pushed into the war zone," said authorities as quoted in media reports.[3]

[1] "Police Arrest Bengaluru Exec behind ISIS Twitter Handle @ShamiWitness", *firstpost.com*, accessed on URL: December 14, 2014, at http://www.firstpost.com/india/police-arrest-bengaluru-exec-behind- isis-twitter-handle-shamiwitness-1848493.html, on 15 January 2015.

[2] "Will rejoin ISIS if I get a chance: Kalyan boy Areeb Majeed", *Zee News*, 1 December 2014, accessed on URL: http://zeenews.india.com/news/india/will-rejoin-isis-if-i-get-a-chance-kalyan-boy-areeb-majeed_1507651.html, on 15 January 2015.

[3] Ibid.

Then in January 2015, a US educated Indian techie was apprehended in Hyderabad by security agencies after it was found that he was joining his partner in the UK and then travelling to Syria, ostensibly to join the ISIS.[4] Local police said that in one of the three Facebook accounts opened by the techie, all peddling the ISIS cause, over 180 messages were posted by followers from India, as the engineering post-graduate had taken on the task of recruiting local youth from Hyderabad.[5]

Next, in September 2015, an Indian woman allegedly involved in recruiting people for the ISIS was deported by the UAE and subsequently arrested in Hyderabad. The 37-year-old, Afsha Jabeen, alias Nicky Joseph, had been portraying herself as a British national while luring youth for ISIS through social media.[6] This was followed by news of the arrest of Muhammed Abdul Ahad, a US-educated computer professional from Bengaluru, who was intercepted by Turkish authorities on the Syrian border and deported to India.[7] Most interestingly, he had barred his wife from contacting authorities about his disappearance or from locating him. There have also been reports of agencies monitoring over 150 youth from South India, who the agencies seem to be monitoring.[8] Those apprehended included a brother

[4] "Arrested ISIS recruit introduced to terror group by girlfriend", *The Times of India*, 18 January 2015, accessed on URL: http://timesofindia.indiatimes.com/india/Arrested-ISIS-recruit-introduced-to-terror-group-by-girlfriend/articleshow/45927316.cms, on 20 February 2015.

[5] Ibid.

[6] "Indian Woman Involved in Recruiting for ISIS Deported from UAE, Arrested in Hyderabad", *DNA*, 11 September 2015, accessed on URL: http://www.dnaindia.com/india/report-indian-woman-involved- in-recruiting-for-isis-deported-from-uae-arrested-in-hyderabad-2124378, on 20 November 2015.

[7] Josy Joseph, "Techie Left Note for Wife before Heading to Join IS", *The Hindu*, 20 November 2015, accessed on URL: http://www.thehindu.com/news/national/techie-left-note-for-wife-before-heading- to-join-is/article7897123.ece, on 20 November 2015.

[8] Josy Joseph, "150 IS 'Supporters' in South India", *The Hindu*, 22 November 2015, accessed on URL: http://www.thehindu.com/news/national/150-is-supporters-in-south-india/article7904410.ece, on 22 November 2015.

and sister who received over Rs 50,000 from a mysterious benefactor to prepare their travel documents, an MBA holder and his wife, a Google employee, brother of a SIMI activist killed by the police, and several engineering students.[9] Social media, here too, was acting as the via media for joining the cause.

In April 2016, media reported the killing of Mohammad Shafi Armar, the head recruiter of the ISIS in India, in a US drone strike in Syria.[10] According to media reports, Shafi, the chief recruiter for ISIS in India before being killed in a drone strike, was close to ISIS chief Abu Bakr al-Baghdadi. Intelligence agencies believe that Shafi was putting together an ISIS unit in every Indian state.[11] He had reportedly recruited 30 youngsters and was in touch with 600-700 potential recruits via Facebook, Whatsapp, and other social media platforms.[12] In fact, Muddabir Sheikh, the ISIS recruiter arrested by the NIA during its countrywide raids, was radicalised by Shafi, who promised a promotion and additional money for Indian operations if Sheikh successfully carried out his first assignment.[13] Sheikh reportedly had been unemployed since October 2015 and spent most of his time on the internet, combing through ISIS propaganda.

As this paper goes into publication, there was news of 15 people going missing in Kerala, including two women and three infants, allegedly to join the cause of the ISIS in Afghanistan and Syria.[14] While investigations continue in the case, families of the missing have revealed

[9] Ibid.

[10] For more, see Shruti Pandalai, "ISIS in India: The Writing on the (Facebook) Wall", *The Diplomat*, 6 May 2015, accessed on URL: http://thediplomat.com/2016/05/isis-in-india-the-writing-on-the-facebook-wall/, on 15 May 2016.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] "Kerala's missing 17: How a complex web of conversion and radicalization led them out of India", *The News Minute*, 9 July2016, accessed on URL: http://www.thenewsminute.com/article/keralas-missing-16-how-complex-web-conversion-and-radicalization-led-them-out-india-46218, on 12 July 2016.

to investigators that their kin were radicalised through a complex web of conversion in a systematic way and led out of the country to live under Sharia law.[15] All these cases point to the fact that ISIS has spread its tentacles far and wide into the Indian subcontinent.

5.2 ISIS releases first propaganda video Targeting Indian Muslims

The spate of arrests of Indian sympathisers has proved that 'Brand ISIS' has found its foothold in India. The threat is manifold because the Islamic State is winning supporters via social media. The Indian government too, after the 2015 Paris attacks, has moved beyond treating the rhetoric of ISIS as a distant problem. With the latest propaganda video of the terror group released in May 2016, directly targeting potential Indian recruits, the writing clearly is on wall.[16] The video showed off a large group of Kalashnikov-wielding jihadists, allegedly from India, fighting against the Syrian forces in the Homs province and urging Indian Muslims to avenge the Babri Masjid Demolition and atrocities on Muslims in Kashmir by joining the holy fight.[17] The NIA officials, analysing the video, say media reports have conclusively identified from the video one engineering student, Fahad Tanvir Sheikh, a resident of Thane who had travelled to Syria in 2014.[18]

[15] Ibid.

[16] "Islamic State releases video allegedly showing Indian jihadists fighting in Syria", *The Indian Express*, 25 May 2016, accessed on URL: http://indianexpress.com/article/india/india-news-india/isis-releases-video-showing-indian-jihadists-fighting-in-syria-2810827/#ifrndnloc, on 26 May 2016.

[17] Ibid.

[18] "NIA analysing IS video featuring purported Indian fighters", *India Today*, 23 May 2016, accessed on URL: http://indiatoday.intoday.in/story/nia-analysing-is-video-featuring-purported-indian-fighters/1/675627.html, on 26 May 2016

5.3 NIA Investigations reveal worrying trends

India has trouble on its hands. Media reports on data of NIA investigations of ISIS India sympathisers reveal that 70% of the 152 Indians arrested, detained or counselled for links to ISIS were from middle and upper middle class families, with half of them holding graduate degrees and 23% completing their masters.[19] Only a quarter of them had religious degrees. In contrast, an overwhelming majority of 645 terrorism suspects interrogated between 2000 and 2014, before the rise of ISIS, were from poor families.[20] More than 90% of them had not completed school, and the trigger for their radicalisation was mostly perceived victimisation at home, not a desire for global jihad."[21]

This, according to the agencies, marks a possible class shift among those attracted to violent groups in India, where religious radicalisation is thought to be more prevalent among the poor and illiterate.[22] Educated, middle-class youngsters in India appear to be more drawn to ISIS, moved as much by the terrorist group's brand of global jihad as by perceived injustices against Muslims at home. [23] Once again social media propaganda has been identified as the medium driving this online radicalisation and puts emphasis on controlling the narrative on the perception wars of communities on sensitive issues. The data suggests a direct correlation between key events with religious undertones in India and spikes in internet traffic from the country to jihadist websites over the past two years.[24]

[19] Appu Esthose Suresh, "Educated, middle-class Indian youngsters drawn to Islamic State" *Hindustan Times*, 13 June 2016, accessed on URL: http://www.hindustantimes.com/india-news/educated-middle-class-indian-youngsters-drawn-to-islamic-state/story-hJxNUrsBOvTEFb5e9d8E4O.html, on 13 June 2016.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

Reports quote, "The National Technical Research Organisation and Intelligence Bureau detected that such traffic peaked between July 23 and 29 (2015) coinciding with the hanging of 1993 Mumbai bombings convict Yakub Memon. Many believed him to be innocent, triggering a media debate. Again, more people logged into jihadist websites from India between April 17 and 23 (2016) – around the time as a controversy over the National Investigation Agency softening its terrorism charges against people linked to Hindu radical groups."[25] It is no wonder then that the propaganda video released by the ISIS targeting Indian Muslims, plays on these perceived insecurities. While India is trying to buff up its capacities to build effective counter narratives, it is imperative to understand and respond to the scale and volume of ISIS propaganda online.

5.4 Understanding ISIS social media modus operandi

ISIS has mastered the art of selling terror and ideology instantly. Today the group's "lone wolfs," armed with smart phones, run "DIY(Do It Yourself) Terror forums," virtually scouting for recruits across the globe. Many in India may not know much about ISIS ideology or the rank and file, but most would have heard of "Jihadi John," the now deceased British Arab, who became infamous for beheading ISIS captives in the group's propaganda videos, which were viewed millions of times across the globe. Interestingly, in the current propaganda videos, an Indian-origin ISIS terrorist from Britain, Siddhartha Dhar, has been dubbed as the "New Jihadi John," and allegedly is a senior commander of the dreaded outfit.[26]

ISIS has made brutality fashionable by exploiting the medium. YouTube videos edited in fancy Hollywoodesque sequences show jihadis as regular Joes, interested in sports and movies — while unflinchingly

[25] Ibid

[26] "Siddhartha Dhar, the "New Jihadi John" of IS: report", *The Hindu*, 3 March 2016, accessed on URL: http://www.thehindu.com/news/international/siddhartha-dhar-a-top-commander-of-is-report/article8548219.ece, on 15 May 2016.

posing with the decapitated heads of victims who went against ISIS decrees. These videos use gaming language, graphics, and effects coupled with trending hashtags, to target their global audience — disenchanted youth who are spoiling for a fight. ISIS speaks to them in a language they understand. This explains the shift in the target audience ISIS seems to be attracting in India, the educated middle-class youngsters, wanting the ISIS global identity while assuaging perceived grievances of their communities back at home. A toxic mix of ideology and technology that makes for a potent challenge.

This ideological pull beyond the Middle East is further explained by some of the numbers that the Brookings[27] ISIS Twitter census came up with: 1) Almost one in five ISIS supporters selected English as their primary language when using Twitter while three-quarters selected Arabic. 2) ISIS-supporting accounts are among the most active and on an average had about 1,000 followers each, considerably higher than an ordinary Twitter user. Much of ISIS's social media success can be attributed to a relatively small group of hyperactive users, numbering between 500 and 2,000 accounts, which tweet in concentrated bursts of high volume. 3) And, finally, perhaps the most important finding – suspension of accounts by Twitter didn't result in a drop in the frequency of messages, in fact new users cropped up in no time. This highlights the need for not just monitoring and surveillance of social media platforms by security agencies, but also the creation of comprehensive content to build effective counter narratives – both by civil societies and governments across the globe.

[27] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter",The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper | No. 20, March 2015, accessed on URL: http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf, on 20 December 2015.

If one looks at the new tools in the ISIS arsenal, Twitter remains its most powerful weapon. However, the Islamic State's online diaspora spans several major sites according to an investigation by The Washington Post (see Table 5.1)

Table 5.1: The ISIS Social Media Arsenal—ISIS Propaganda Tools

Twitter	The microblogging site has likely been the most successful platform for the group.
Facebook	The social network allows the selective sharing of graphic content if the user posting the content is condemning it, but not if the content is being celebrated or glorified. This makes it difficult for militants to post there.
Youtube	The video-sharing website allows the group to upload professionally produced propaganda videos of executions, captured territory, and promotional pieces about life in the Islamic State.
Kik and other messaging apps	The recruiters prefer such apps to speak with would- be members. They often ask newcomers they find on other services to move their conversations to Kik.
Ask.fm	AQ-and A site, where militants and other Islamic State members answer questions about their motivations and religion.

Source: Scott Higham and Ellen Nakashima, "Why the Islamic State Leaves Tech Companies Torn between Free Speech and Security", The Washington Post, 16 July 2015.

In India too, agencies see a similar pattern with IS recruiters scouring social media to identify possible candidates who 'share' or 'like' pro-IS literature. They then encourage them to share more content before trying to inveigle them into travelling to IS-controlled areas in Iraq and Syria.

Table 5.2: How ISIS Recruits in India: Online Radicalisation Trends

Step 1:	Posting messages on Facebook, requesting ‘likes’ and ‘shares’
Step 2:	Develop contacts with person who has ‘liked’ or ‘shared’ the post
Step 3:	Getting them to share more radical content
Step 4:	If seriousness is shown, explaining the route and logistics to reach Islamic State
Step 5:	Exchange of phone numbers, Skype IDs and other means of communication
Step 6:	Meeting in person with the intermediaries
Step 7:	Further action based on the willingness and abilities of the subject to join the ISIS.

(***Source:*** Fighting The Islamic State: Centre plans anti-terror cyber-push, 11 April 2016, The Hindu)

5.5 Dangerous Fallout on National Security

In addition to this, Indian security agencies are also worried that the brazen use of social media by the ISIS to establish itself as the global face of "jihad" has had other troublesome spin offs.[28]

5.5.1 ISIS Propaganda Fuelling Competition between Terror Groups on Social Media

Firstly, ISIS propaganda on social media has made other transnational terror groups like al Qaeda more competitive and resorting to more sensationalist and ruthless styles of propaganda. Over the last two years, we have seen many propaganda messages on social media directed towards the "Indian Muslim" by both these groups. This naturally is a big cause of concern for investigating agencies.

5.5.2 Bandwagoning by Terror Groups in India

Perhaps the biggest threat that the success of ISIS poses to India is, the bandwagon effect that it seems to have inspired in local terror outfits. Irrespective of whether or not they agree with the ISIS ideology, groups like the Indian Mujahideen and other extremist outfits have been seen as eager to latch on to brand ISIS in a bid to garner attention. Media reports quoted intelligence agencies saying that "Instead of forming its sleeper cells, the Internet and social media has become another platform for the terror outfit to scout for vulnerable youth belonging to the minority community. All agencies are keeping a close tab on the suspect areas where the IM was most active."[29] The outfit had also uploaded a video of the ISIS Chief, Abu Bakr al-Baghdadi, with Hindi, Urdu and Tamil subtitles.

[28] This section is based on the author's paper: "Armed with a Tweet: The Islamic State's Virtual Propaganda Wars, Its Appeal and Looming Threat to India" in *Asian Strategic Review 2016 -Terrorism: Emerging Trends*, edited by S. D. Muni and Vivek Chadha, IDSA and Pentagon Press, New Delhi, 2016.

[29] Ibid.

5.5.3 Inspiring "Overt War of Ideas" and Recruitment by Indian Insurgent Groups

One of the spin-offs of the blatant use of social media propaganda by the ISIS is that insurgent groups in India are catching on to the potential of social media to attract recruits. Social media was flooded with photos of militants in the North East, posing in the forests with assault rifles. This group NSCN-K was responsible for an ambush on the Indian Army that had killed 18 soldiers in Manipur. The message was clearly signalling that the "war of ideas against the establishment" is no longer covert, but aims to inspire recruits overtly.

5.5.4 The Case of "Facebook Militant" Burhan Wani

This overt war of ideas has serious consequences for India's national security as seen in the resurgence of unrest in the state of Jammu and Kashmir in July 2016. The case in point is the mass violence that was triggered in the aftermath of the killing of Burhan Wani, the Hizbul Mujahideen commander who was infamous as the "Facebook Militant" in mass media.[30]

Burhan Wani's story was no different than that of the many youth who take to militancy in the valley. Wani had taken to militancy after 2010, as a teenager, to avenge the brutalities committed on his brother allegedly by the Indian state, which has been battling for decades the cross border fuelled insurgency in the valley.[31] Considered reticent, Wani, the son of a school principal, ironically became the new face of Kashmiri militancy by adopting the overt war of ideas and used social media to campaign for his cause.

During the summer of 2015, Burhan became an unparalleled icon of Kashmiri rebellion using technology to access extraordinary media coverage and reach. A picture of Burhan with a dozen of his comrades

[30] "Burhan Wani: Kashmir's Facebook militant", *The New Indian Express*, 11 July 2016, accessed on URL: http://www.newindianexpress.com/nation/Burhan-Wani-Kashmirs-Facebook-militant/2016/07/11/article3524242.ece, on 12 July 2016.

[31] Ibid.

posing in army-style combat fatigues, went viral on social media and signalled the brazenness with which the new-age militants were willing to be identified.[32]

He followed this up by a video where he addressed the Kashmiri youth directly and spoke of "Khilafat." The idea of Khilafat, a clear departure from demands made by separatist leaders in Kashmir, placed the Kashmir rebellion in the larger discourse of Islamist movements across the world.[33] It urged the youth to join his outfit and asked the Kashmir police to shun their fight against the militants. The video saw Wani speaking to the camera, flanked by two gunmen in military fatigues, with a Kalashnikov, a pistol and a Quran in front of him. The production, high on its symbolism was clearly inspired by propaganda styles of the Islamic state as discussed previously.[34]

In his videos, he was shown playing cricket or eating with his friends; and with these images he was able to humanise the rebel, clearly adopting techniques used by the ISIS propaganda machinery.[35] From backing radical islamic preachers linked to terror attacks in Bangladesh or tapping on polarising sentiments against re-establishing of townships for the returning Kashmir Pandits in the valley, Wani's propaganda videos managed to exploit the fissures on controversial issues in the valley.[36]

[32] Sameer Yasir, "Hizb-ul-Mujahideen's Burhan Wani takes to social media to influence youth in Kashmir", www.firstpost.in, 23 May 2016, accessed on URL: http://www.firstpost.com/india/the-virtual-world-hizb-ul-mujahideens-burhan-wani-innovates-to-influence-youth-in-kashmir-2794392.html, on 12 July 2016.

[33] Ibid.

[34] Ibid.

[35] Samanth Subramanian, "Burhan Wani: The rise and fall of the Kashmiri militant and social media star", *The National*, 26 August 2016, accessed on URL : http://www.thenational.ae/world/south-asia/burhan-wani-the-rise-and-fall-of-the-kashmiri-militant-and-social-media-star, on 27 August 2016.

[36] Prabha Rao, "Online Radicalisation: The Example of Burhan Wani", *IDSA Issue Brief*, 16 July 2016, accessed on URL: http://www.idsa.in/issuebrief/online-radicalisation-burhan-wani_prao_160716, on 28 August 2016.

According to experts Wani's social media outreach had created a hype in the press, both in India and Pakistan. With a majority of the Valley's population being below 30, often unemployed and hyperactive on the social media, gave Wani a receptive target audience.[37] Top police sources, quoted in the media, admitted that Wani had remained elusive because of his "tremendous following" online and on the ground. "Every time an operation was launched against Wani, our movement was reported to him by his huge network of young supporters and fans," said a top police officer.[38] Wani, according the police, played a key role in making Hizbul Mujahideen stronger than the Lashkar-e-Taiba in the Valley. Most of Wani's recruits allegedly came from a middle-class background with good academic records. They would snatch weapons from policemen and receive training in orchards.[39] "Since 2010, he must have influenced more than 60 youths in south Kashmir to join militancy. He received training locally without crossing into Pakistan-occupied Kashmir," said a police source to a national publication.[40]

While data linking Burhan Wani's social media outreach to the rise of militancy in the valley is purely causal at this point of time, it does indicate disturbing trends. The violence that erupted in the valley post his death, the outpouring of grief across Kashmir and the unprecedented crowds who attended his funeral defying curfew are proof of his popularity among the masses and underscore the alienation in the valley. His death will be used by anti-India elements across the border to revive the armed resistance in the valley. Social media seems to be their weapon of war. Indian agencies need to take guard.

The ISIS inspired overt war of ideas is here to stay.

[37] Ibid.

[38] Peerzad Ashiq, "Burhan Wani, Hizbul poster boy, killed in encounter", *The Hindu*, 9 July 2016, accessed on URL: http://www.thehindu.com/news/national/other-states/burhan-wani-kashmir-valleys-most-wanted-militant-commander-killed/article8824756.ece, on 28 August 2016.

[39] Ibid.

[40] Ibid.

5.6 India's Push back against ISIS Virtual War

The Indian authorities are clearly concerned with ISIS recruitment via social media. A Ministry of Home Affairs (MHA) advisory released after the Paris attacks reiterated that the Islamic States "success of online radicalization of youth (…) and the possibility of piggybacking on terror groups operating in India, opened up the possibility of IS-sponsored terrorist action on Indian territory."[41] While Indian agencies are aware of the looming challenge, we need to buff up capacities to match the scale of the challenge. Dedicated Social Media Labs, focussing just on ISIS and al Qaeda recruitment attempts online could perhaps be the first step in that direction. These concerns were reflected when the MHA announced in December 2015,that it is examining the feasibility of a multi-agency 24/7 Social Media Analysis Center to monitor online recruitment.[42] A recommendation which was first made by the author as part of policy papers submitted to the MHA on the subject.

Indian Government agencies have been working on plans to counter social media radicalisation in India. Apart from online surveillance to isolate influencers and prevent mishaps, emphasis has been made to institute a de-radicalisation programme. The programme, according to a government official quoted by the media, has tried to address the issue at three levels: At the first, macro level, through preventive arrests, at the second level, counter-narratives to discourage the youth and give incentives to renounce violence and, at the third, to work at the micro level with individuals.[43] However, this is no easy task. A government secretary was quoted saying, "It is hard to gauge the success of these

[41] For more, see Shruti Pandalai,"ISIS in India: The Writing on the (Facebook) Wall", n. 10.

[42] Ibid. Also see http://indiatoday.intoday.in/story/government-plans-social-media-scanning-centre-to-take-on-isis/1/554878.html, accessed on 15 May 2015

[43] This section is based on the author's paper: "Armed with a Tweet: The Islamic State's Virtual Propaganda Wars, Its Appeal and Looming Threat to India", n. 28.

programmes. But with this programme, disengagement from extremist groups has been managed but preventing re-radicalisation is proving to be difficult. Many jihadis go back to the vortex of terror."[44]

Attempts have already been made to reach out to the Imams of various Muslim communities in India, to use their Friday sermons to address the youth on why rejecting the ISIS-ideology should be their call of duty. In fact, over 1,050 Indian Islamic scholars and clerics have issued fatwa against the ISIS, describing its acts and actions as against the basic tenets of Islam.[45] In cities like Bengaluru, the Imam of the Jamia Masjid, has started an initiative to counter propaganda of the kind unleashed by the Islamic State by organising outreach programmes in colleges and using social media platforms, such as WhatsApp. A WhatsApp group of around 150 maulanas has been created to devise a communication strategy to prevent radicalisation of youths.[46] All these are great building blocks to a comprehensive effort to counter the ISIS ideology in India. The impetus has to remain in sustaining these efforts over time and to look beyond instant solutions.

As discussed in all of the cases above, from internal law and order challenges to threats from extremists, social media can be engaged with both to provide intelligence as we all as to create robust counter narratives, which make it a potent force multiplier in the hands of security and law enforcement agencies. However, this has been a challenge for the government in the past with activists criticising government's first response in emergency situations as curtailing freedom of speech and expression, and attempting to censor the internet. It is, hence, imperative that we next, discuss the legal challenges in dealing with cases arising of social media misuse.

[44] Ibid.

[45] Ibid.

[46] Ibid.

Chapter 6

Social Media and The Legal Challenge

In India, the effective use of social media by law enforcement and security agencies to protect internal cohesion have been hurt due to unfortunate incidents of misuse of current legal provisions, causing legitimate concerns over curtailing constitutional guarantees of freedom of speech and expression and created a threat perception of a "big brother" regime.

Pawan Duggal, a cyber law expert and advocate with the Supreme Court writes, "Social media as a phenomenon has grown by leaps and bounds in 2013. However, with the passage of time it is clear that the Information Technology Act, 2000, is not capable of effectively addressing the legal, policy and regulatory concerns generated by the use of social media in India."[1]

The following challenges need to be addressed immediately:

6.1 Fears of censorship of freedom of speech and expression

The Information Technology Act, 2000, and the amended IT Act of 2008 are the existent laws which provide the legal framework pertaining to issues of social media.[2] The questionable use of Article 66A of this

[1] Pawan Duggal, "The Face of Indian Cyber Law in 2013", *Business Standard*, 30 December 2013, accessed on URL: http://www.business-standard.com/article/technology/the-face-of-indian-cyber-law-in-2013-113123000441_1.html, on 5 June 2014

[2] IT (Amendment) Act, 2008 – DeitY, accesssed on URL : http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf. Also refer to "Short note on IT Amendment Act, 2008", *Centre for Internet and Society*, accessed on URL: http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008/, on 5 June 2014.

act, which now stands revoked after a ground breaking decision by the Supreme Court of India in March 2015, created lot of controversy.[3] In short, Article 66A prescribed punishment for "any person who sends, by means of a computer resource or a communication device, any information that is grossly offensive or has menacing character."[4] In a number of cases this provision was used to arrest individuals for their opinions on social media which were seen as critical of the government or political figures. The revocation of this provision was seen as upholding values of liberty and freedom, the two pillars of democracy by the Supreme Court. However, peoples' perceptions of the government attitudes to the same remain scarred.

6.2 Internet Traffic Monitoring and Privacy Concerns

The way in which the internet allows data to be produced, collected, combined, shared, stored, and analysed is constantly changing, and the need for redefining personal data and what type of protections personal data deserves and can no longer be a given.[5]

Police projects like *Social Media Labs* depend entirely on information available on public platforms and hence authorities must anticipate contestations to what constitutes public data in times ahead.

[3] "SC strikes down 'draconian' Section 66A", *The Hindu*, 24 March 2015, accessed online on URL: http://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional/article7027375.ece, on 15 May 2015.

[4] IT (Amendment) Act, 2008 – DeitY, n. 2. Also refer to Short note on IT Amendment Act, 2008", n. 2.

[5] Elonnai Hickok, "Internet Privacy in India", *Centre for Internet and Society*, 8 January 2014, accessed on URL: http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india, on 5 June 2014.

[6] For more, see: "Department of Electronics and Information Technology Framework & Guidelines for Use of Social Media for Government Organisations", p. 19, accessed on URL: https://negp.gov.in/pdfs/Approved_Social_Media_Framework_and_Guidelines%20_2_.pdf, on 1 September 2013.

Currently, provisions in IT (Reasonable security practices and procedures & sensitive personal data and information) Rules 2011[6] and the proposed Privacy Bill 2014[7] say that "Provided that any information that is freely available or accessible in public domain or to be furnished under the Right to Information Act, 2005, or any other law for the time being in force shall not be regarded as sensitive personal data for the purposes of this Act."[8] However, exceptions have been outlined under the privacy bill for security and law enforcement agencies in cases dealing with threats to the security and sovereignty of India.[9] Notwithstanding this, agencies must be aware that, for example, in the US, individuals have contested the use of their tweets without permission while courts in the US have ruled that tweets, private and public can be obtained by law enforcement with only a subpoena as technically the information has been shared with another entity, and is therefore no longer private.[10] Indian Courts have yet to deal directly with the question of social media content being public or private information. As use of social media evolves, for security and law enforcement agencies, questions regarding 'relevancy' of such data, and its 'admissibility' etc. will also be raised.

6.3 Inconsistencies in compliance review/due diligence in implementing filtering mechanisms for malicious content on the web

Under the existing legal frameworks, Sections 69 and 69(a) empowers the government of India to:[11]

[7] Elonnai Hickok, "Leaked Privacy Bill: 2014 vs. 2011", *Centre for Internet and Society*, 31 March 2014, accessed on URL: http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011, on 5 June 2014.

[8] Ibid.

[9] Ibid.

[10] Elonnai Hickok, "Internet Privacy in India", n. 5.

[11] IT (Amendment) Act, 2008 – DeitY, n. 2. Also refer to Short note on IT Amendment Act, 2008", n. 2.

1) issue directions for blocking of information for public access and to issue directions for interception or monitoring or decryption of information through any computer resource when circumstances threaten public order, defence, security, sovereignty and integrity of India, or friendly relations with other states or to prevent incitement to the commission of any cognizable offence relating to the above circumstances.

2) Article 69 (b) of the IT Act 2000 empowers agencies of the government of India, in this case the Dept. of Electronics and Information Technology, "to authorise to monitor and collect traffic data or information through any computer resource for cyber security" for cyber incidents and breaches.

Safeguards: Rules under 69 (a) of IT act 2000 (rule 7), authorises Secretary, DeitY as a competent authority to issue directions for blocking of information for public access after examining recommendations of a committee comprising of designated officer of DeitY, Joint Secretaries of MHA, Ministry of Law and Justice, Information and Broadcasting and ICERT. In situations of emergency, the competent authority may bypass committee examination, but rules require that emergency requests are examined within 48 hours by the committee. There are provisions for a Review Committee chaired by the cabinet secretary to review decisions taken by the competent authority for blocking of information for public access. In case inconsistencies are found, an order for unblocking of information will be issued.

Cyber law experts have said that while in the case of the Assam riots, the blocking of URLs by the government was a symbolic reaction, they say blocking en-masse of over 300 URLS exposed the ineffectiveness of safeguards as implementation of rules did not take place, says Pranesh Prakash, of the Centre for Internet and Society.[12] Recommendations have been made to make the process of blocking

[12] Pranesh Prakash, "Analysing List of blocked sites", *Centre for Internet and Society*, 22 August 2012, accessed on URL: http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism, on 5 June 2014.

of content less arbitrary and more transparent by "informing censored groups/individuals reasons for the block and allowing them to contest it and seek redressal from the relevant authority, as also informing the public about the reasons of the block after the emergency has been dealt with, to encourage openness."[13] Security and Law enforcement professionals on the other hand have said that a medium as fast and impactful as the social media, blocking, 48 hour time frames and committee decisions are futile. They have asked for real time redressal mechanisms which are legally sound and will make action effective.

6.4 Issues regarding liability of intermediaries

Section 79 of the IT Act requires intermediaries to advise users of its services not to post information which is harmful/offensive and violates the law of India. The rules further provide that intermediaries may remove on their own such type of information that is considered harmful or offensive.[14] Cyber law experts argue that ordering Internet service providers (ISPs) to block content and making them liable is largely ineffectual.[15] Instead, people and companies hosting the material on individual platforms should be targeted, since all sites have clear content removal policies and encouraging communal tensions and hate speeches generally would not be tolerated. They add that such provisions are misinterpreted by overzealous ISPs, who then act beyond the government's requirements.

6.5 Complications in jurisdiction with subsidiaries of foreign internet companies

Often during times of crisis, the governments find themselves in a spot, because social media service providers like Facebook, Google (YouTube, Blogspot), Twitter, etc., provide web and social media services from their servers installed in the US and hence say they will comply only with US laws. So far co-operation on matters happens only in good faith or with a letter from the government being sent to

[13] Ibid.

[14] Ibid.

[15] Ibid.

the US Department of Justice. Cyber security experts in India have been pressing the government to formulate laws that clarify the legal position on whether the law of the land or the law of the countries where the Internet companies are headquartered will take precedence in cyberspace. This is important because Indian authorities want the social networks to conform to local laws and sensitivities when it comes to blocking Web content.

The discussion above has barely scratched the surface in terms of the challenges that face decision makers vis-a-vis setting up a legal regime focusing on various aspects of social media. A high level meeting chaired by the NSA in September 2012 decided that "standard operating procedures will be put in place to set in motion response of the government and service providers in case of emergency and (...) to introduce predictability with regard to what kind of content is liable to be regulated and for how long."[16] The government is also said to be thinking on the lines of Mutual Legal Assistance Treaties between India and other countries like the USA.[17]

Experts interviewed for this project believe that the first step to deal with the multitude of challenges that have emerged with the rise of social media requires that it be legally viewed as a medium. Second is a complete rethink of the legal regime since the IT ACT 2000 conceived 16 years ago was meant to promote e-commerce and is incapable of resolving the challenges put forth by the rapid explosion of new technologies like social media. The National Cyber Security Policy doesn't have any provisions to deal with social media so the change has to come first at the Macro level. Even though the government,

[16] Thomas K. Thomas, "Intelligence agencies to keep an eye on social media content", *The Hindu Business Line*, 14 September 2012, accessed on URL: http://www.thehindubusinessline.com/industry-and-economy/info-tech/intelligence-agencies-to-keep-an-eye-on-social-media-content/article3897687.ece, on June 5, 2014.

[17] Interview conducted with Gulshan Rai, Director CERT-IN, on 8 August 2013 in New Delhi.

[18] "Centre plans anti-terror cyber-push", *The Hindu*, 11 April 2016, accessed on URL: http://www.thehindu.com/news/national/centre-plans-antiterror-cyberpush/article8459082.ece, on 26 May 2016.

after many recommendations including those from the IDSA task force report, has decided to push for a national social media policy, the blue prints are still being chalked out.[18]

At the more micro level, especially in situations where conflict is triggered with the misuse of social media, it has been suggested the government work with social media service companies to create mechanisms where in case of emergencies, provisions for 24x7 responses for complaints be available. This would not require new legislation but good communication skills and cultivating of relationships.

It has also been recommended that to make the process more transparent and prevent misuse of any information "an independent, autonomous and proactive privacy commissioner be established who will keep both private and state actors on a short lease.[19]

[19] Indrani Bagchi, " India for inclusive internet governance", *The Times of India*, 25 April 2014, accessed on URL: http://timesofindia.indiatimes.com/india/India-for-inclusive-internet-governance/articleshow/34170534.cms, on 5 June 2014.

Chapter 7

Recommendations for Future Frameworks and Scope of Challenges

This paper has provided a conceptual overview of the impact, opportunities and challenges thrown up by social media for security and law enforcement agencies. The focus has been to make a case for leveraging social media for engagement with citizens and securing communities, and also mining information available publicly for actionable intelligence to anticipate and prevent possible law and order situations in case there is a misuse of the medium. It has also laid emphasis on the use of social media to build effective counter narratives and combat the extremist challenge. The issues of engagement, process, technology and legal challenges posed for government agencies dealing with the medium will have to be tackled with a long term vision. However, a few concrete steps that could possibly be taken on immediately include:

1. *Institutionalise the blueprint for a National Social Media Policy*: The Indian establishment needs to recognise the medium and grant it a legal status if it needs to deal with the multitude of challenges that rise out of it effectively. The National Cyber Security Policy needs to be revised to include social media challenges which are distinct from the cyber security threats. While the government is working on a blueprint for a National Social Media policy to combat terror, it needs to institutionalise the blueprint for the same.

2. *Implement and institutionalise the Framework of Guidelines on social media engagement*: DeitY's Framework of guidelines has laid down elaborate guiding principles for engagement of social media by government agencies. It discusses objectives, engagement protocol, types of platforms, communication strategy, responsiveness criteria and legal limitations for agencies to formulate their respective strategies for engaging with the medium and stakeholders. The need is to ensure enforcement and institutionalisation of this policy

across the country with immediate effect. This has to be flexible and can be customised, depending the needs of each institution.

3. *Create awareness on the Challenges posed by social media*: Social media is really about interactive design. It is difficult to identify whether the other side engaging you is a person or a malicious actor. Same technology can be used for malware propagation, phishing, cyber-crime and misinformation campaigns. There exists a huge lack of awareness amongst citizens, law enforcement agencies and higher levels on the potential of misuse of social media.

4. *Create organisational ecosystems, circumvent hierarchies, encourage outreach:* Social media ecosystems are dynamic and hence pose a challenge for security and law enforcement agencies which work around established hierarchies. Considering the immense potential of social media as a force-multiplier, efforts have to be made up the ladder to change the approach to the use of social media by empowering personnel to engage proactively, and sustain channels of communication rather than looking at it from purely an observer/ monitoring perspective. Establishing a presence not only will help in disseminating of information and preventing misuse of the medium, but it will also build trust with the engaged communities, ensuring their support during times of crises. As an expert put it, "it will need the attitude of creating a small start-up within law enforcement agencies, which is a difficult thing to achieve."[1]

5. *Empower agencies, build talent, and use specialists*: If the medium is to be adopted into daily practice by all personnel, then agencies must be empowered technically, legally and financially to use the medium to their specific purposes. Decisions on dedicated teams, with talent specific to technical, legal and soft skill capabilities required for social media engagement, across centre and state levels need to be thrashed out. Inclusion of lateral entry specialists to handle specific requirements like 24x7 tech-support/or soft skills, etc., need to be debated. Practical solutions need to be pushed in line with the

[1] Nandakumar Sarvade, Former Sr IPS officer of Mahrashtra Police and Cyber Security Expert, interviewed on 18 February 2014 in Mumbai.

larger debate on police reforms. As an expert said, "One can't expect a baton wielding police official to suddenly master technology, when he/she doesn't even have basic computer skills. Building human resource capacity will be the big challenge. Curriculums in the National Police Academy and other training schools need to be revised to include the opportunities and challenges posed by social media."

6. *Replicate "Social Media Labs" across the country*: Use the success and work on the limitations of the social media labs experiment for the future and incorporate the best practices at the state and federal levels across the country. Target, specifically, issues relating to radicalisation and recruitment of youth by extremists.

7. *Demarcate budgets, standardise tools and platforms*: Currently, projects wanting to leverage social media are happening in isolation driven by individual or particular agency-led initiatives. There is a need to nationalise this effort and that will require demarcation of specific budgets, standardisation of tools and technology platforms for specific agencies and purposes.

8. *Expand and define scope of public-private partnerships:* The government has already recognised that since the private sector is a much larger user of the internet than the government, there is significant private sector participation in critical infrastructure and, most importantly, there exists a huge talent pool in the private sector is something that the government can usefully leverage.[2] There is a Joint Working Group already in place working out frameworks of engagement for cyber security initiatives.[3] Templates specific to PPP models for social media require directions on how agencies will decide on vendors offering technology, what will be the performance criteria, will there be a need for an oversight group etc.

[2] For more See Deputy NSA Nehchal Sandhu's address in *Report on CYFY 2013: India Conference on Cyber Security and Cyber Governance*, 14-15 October, New Delhi, organised by ORF-FICCI, accessed on URL: http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf, on 1 May 2014.

[3] Ibid.

9. *Frameworks must build capacity at local level and share information at federal level*: The framework to deal with social media challenges requires building capacity at local levels, since issues begin at this stage. However, the scope of building data bases and sharing of information should use existing mechanisms between state and federal agencies. For eg intelligence gathered on specific crimes using social media platforms can supplement information on national databases like Crime and Criminal Tracking Network System (CCTNS) which are being developed to share and analyse data between police agencies. Such practices can be further deliberated upon during DGP level conferences. Care must be taken to avoid duplication of infrastructure and turf wars within agencies.

10. *Outline standard operating procedures*:

    1) *for use of social media network analysis for intelligence gathering*: This includes a specific list of do's and don'ts regarding the use of social media data for generating actionable intelligence. So identifying the purpose, time frame, the type of tool, targets, duration of retention of information, compliance reviews and verification procedures etc. must be defined to ensure no misuse of data mined from social media platforms.

    2) *to be set in motion in case of a cyber-social media attack*: These operating procedures must define rules of engagement for all stakeholders involved in the situation. Provisions of 24x7 complaint review mechanisms with service providers during times of emergency, notification to concerned group/ individual to take down offensive content and instituting a redressal mechanism in case of contested blocking of content – are safeguards that need to be implemented. Quick decisions by an authority empowered to direct law enforcement agencies in a case of social media triggered cyber-attack that needs to be thought through.

    3) *for exchange of information with intermediaries / service providers of social media*: Since most social media content providers have headquarters outside India, the rule of the land at this point of time do not apply. So to avoid complications during

emergencies standard protocols for exchange of information with social media service providers must be developed to ensure no loss of time due to communication gaps.

11. *Re-haul legal regime: focus on loop holes and censorship and privacy issues:* It is imperative that the medium be given a legal status and thought be put into a new legal regime which can manage the gamut of challenges posed by social media. Obsolete laws, which are not up with the times including the many provisions of the IT ACT, 2000, need to be done away with. To have a more effective reaction to cases of conflict triggered by social media, political will is required to make intermediaries liable to India's legal requirements. Need for coming up with specific norms for internet service providers which will have consequences in case of non-compliance.

    Neither the courts nor the current legal regime have any precedence with respect to social media use or abuse in India. Hence, the government should expect many challenges to lie ahead including questions over the legality of what constitutes public data. Legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight are all issues which need to be debated in this realm. The suggestion for setting up an independent privacy commissioner to prevent misuse requires further examination. The balance between the requirements of national security and citizens' right to privacy will need to be navigated delicately.

12. *Continue awareness campaigns, build centres of excellence, create and exchange best practices:*

    Social media is an evolving field and governments and agencies the world over are still in the process of adapting to the phenomena. The National Cyber security Policy, 2014, while not directly referring to social media, envisions the creation of centres of excellence for various capacity building exercises including assistance to law enforcement agencies – some provisions could be expanded to include training personnel and developing techniques dedicated to social media technologies. At a more practical level, we have to recognise that data scientists who extract intelligence from the medium will not come up overnight. Thought needs to put into revised curriculum in universities to produce experts who will fulfil these demands

There is also a need to build a knowledge base of best practices and share them internally as 'lessons learnt' for institutional memory. Collaborations with likeminded international agencies to learn from their experiences must also be encouraged.

The adoption and use of social media for law enforcement and security is not purely a technological or engagement issue, but one which needs conceptualisation of policy and system designs at every level, while walking the tightrope on privacy concerns and balancing security imperatives. It will be a steep learning curve, but it is time to recognise our shortcomings and deal head on with the challenges and engage with the opportunities that technology has brought to our doorstep.

Social media - its reach, impact and potential in a globalised world is no longer contested. It is a fascinating phenomenon which presents both challenges and opportunities to governments and law enforcement agencies across the spectrum. An investigation into how India has grappled with the challenges posed by the medium as also whether social media can be harnessed to act as a force multiplier for our enforcement agencies is essential. Issues related to the inadequacy of the Indian legal regime in dealing with social media and fears relating to breach of privacy and censorship of the internet also need to be addressed. The author tries to investigate these concerns in the monograph and has attempted to evaluate the perceptions, current capacities and challenges faced by security and law enforcement agencies in India while grappling with the phenomenon. The monograph hopes to succeed in providing a conceptual framework to understanding this emerging challenge and draw up a set of best practices and recommendations for policy makers and law enforcement agencies to move forward with.

Shruti Pandalai is an Associate Fellow at IDSA, primarily working on issues related to India's national security and foreign policy. Attached with the military centre, she has worked on projects for the National Security Council Secretariat, Ministry of External Affairs and Ministry of Home Affairs. India's strategic thought and practice, India's military history - the wars of 1962 and '65 and their impact on contemporary foreign policy, Emerging challenges to national security and Forecasting and scenario projection are some of themes she has worked on. She has also published widely on the subject of Media and National Security at IDSA. Previously, Shruti was a broadcast journalist, a News Anchor and Senior Correspondent with a leading national English news network specialising in international affairs. She's regular commentator in national and international media on matters of national security and is the recipient of the IDSA President's Award 2016. She is an alumni of St Xavier's College Calcutta, The Asian College of Journalism, Chennai and The Centre for International Studies and Diplomacy, SOAS, University of London.

idsa
INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Institute for Defence Studies and Analyses

No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
E-mail: contactus@idsa.in Website: http://www.idsa.in