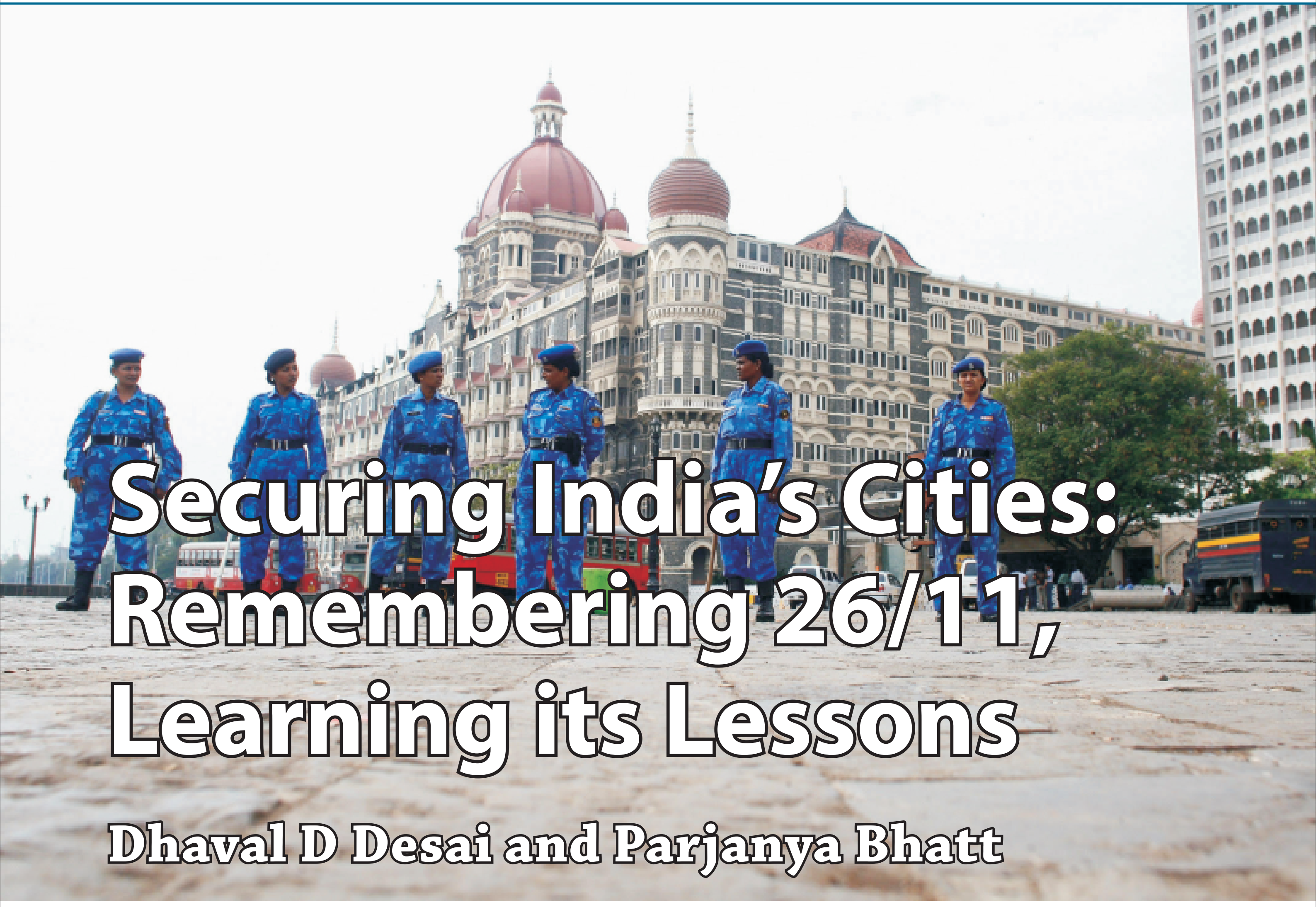
92

ORF SPECIAL REPORT

JULY 2019



Securing India's Cities: Remembering 26/11, Learning its Lessons

Dhaval D Desai and Parjanya Bhatt

Rapid Action Force personnel, 26/11, Taj Mahal Palace Hotel, Mumbai. Photo: Julian Herbert/Getty Images

Attribution: Dhaval D. Desai and Parjanya Bhatt, "Securing India's Cities: Remembering 26/11, Learning its Lessons", *ORF Special Report No. 92*, July 2019, Observer Research Foundation.

ISBN 978-93-89094-55-8

INTRODUCTION

The terrorists who attacked Mumbai on 26 November 2008 (or 26/11) came via sea, taking advantage of the gaps[1] in India's national security ecosystem. Over ten years since, India's policymakers are heeding the lessons of 26/11, and constant changes are being undertaken to strengthen the country's security systems. At the same time, however, the manifestations of terrorism have evolved.[2] Terrorist groups are making effective use of technology,[3] social media and other innovative tactics not only to evade arrest and prosecution but to disseminate their propaganda and recruit foot soldiers.[4] Recognising the difficulty of militarily defeating state forces, terrorists are aiming to create spectacle.[5]

The challenge for India's security organisations, therefore, is to combat an enemy whose aim is not only to kill, but to win minds. Cities, by their supposedly cosmopolitan and inclusive nature, provide the theatre where terrorists can garner their global audience.

This special report builds on the insights shared during a conference organised by the Observer Research Foundation (ORF)–Mumbai. The conference gathered key stakeholders, principally in the country's security matrix, who exchanged views on the question of whether or not the country is prepared to deal with increasingly unpredictable and deadlier forms of terrorism in the urban landscape.

INDIA'S COUNTERTERRORISM APPARATUS POST-26/11: KEY CHALLENGES

1) Intelligence capabilities and inter-agency coordination

Reliable and actionable intelligence is a pillar of any effective counter-terrorism apparatus. Following the 26/11 Mumbai attacks, it was discovered that there was a failure of intelligence and a lack of ability to communicate information to the relevant stakeholders. The weaknesses of India's intelligence are three-fold. The first is when there is no intelligence at all. Second, the available intelligence is too general, vague in nature and not actionable.[6] Across the world, law enforcement agencies blame the lack of actionable intelligence as a major obstacle to the prevention of terror attacks. The third challenge is that different agencies fail to effectively communicate the details of the intelligence received by them to the relevant law enforcement agency.

Such a pattern is repeatedly seen amongst the security forces and intelligence agencies of many different countries. For instance, in the case of the 9/11 attacks in the United States, the Central Intelligence Agency (CIA) had some knowledge about the presence of hijackers within American territory, but the information was not communicated to the Federal Bureau of Investigation (FBI).[7] Indeed, intelligence agencies are today dependent on technical intelligence on non-state actors. There is also a huge volume of information which cannot be deciphered.

In the decade following the 26/11 Mumbai attacks, the Government of India has taken important measures to improve the state's intelligence gathering mechanism and enhance inter-agency coordination amongst the various security agencies. These measures have resulted in a marked reduction of terror attacks in urban centres. India's security apparatus has been reinforced with the establishment of Multi-Agency Coordination Centres (MACCs) and Subsidiary Multi-Agency Coordination Centres (SMACCs).

Although these steps have led to a qualitative improvement in combating terrorism, there is limited coordination amongst intelligence agencies, security forces, and the bureaucracy. India also suffers from inadequate inter-agency coordination which, in turn, leads to lack of effective intelligence monitoring and security response. Concerns also exist over the fact that the information is not disseminated to the security forces at the tactical level at the speed and effectiveness with which it should ideally occur. To improve the level of coordination, inter-operability amongst the agencies must be enhanced and military officers must be periodically sent on deputation to cooperating agencies to ensure that the country's entire intelligence apparatus precisely understands the specific requirements of the consumers of their intelligence.

Terrorism has moved beyond the physical space to the digital space. In this context, the gathering of intelligence needs to become multi-faceted as well. The old debate on whether human intelligence is better than technical intelligence is no longer relevant. It would be a more effective strategy for India to complement efforts of information gathering through technical means with human intelligence to enhance the state's capabilities in meeting the evolving challenges posed by terror groups.[8]

2) The role of social media

Individuals and groups with terrorist agenda are making use of social media platforms to widen their reach, spread their ideology, and recruit followers and cadre. For instance, Al-Qaeda's websites carry manuals on how to construct explosive devices.[9] Social media also provides anonymous avenues for terror groups to communicate with each other. Indeed, terrorists have been proving themselves adept at using technology for a long time now. During the 26/11 Mumbai attacks, all the 10 terrorists involved, were in constant communication with their handlers in Pakistan through satellite phones.[10] Those handlers in Pakistan, in turn, were using the live television coverage of the state response to pass on messages to the terrorists, almost in real time.[11,12]

The impact of social media on the spread of terrorism can be seen in the conflict in Kashmir, where there is a growing trend of increased radicalisation[13] especially amongst the youth.[14] India's security forces must create effective counter-narratives and build an environment that does not lead to marginalisation and radicalisation as is increasingly seen in the case of homegrown jihadis in the Valley.

This increased radicalisation is one aspect of the Kashmir conflict that is more difficult to counter than combatting terrorism by military means. For instance, in the case of Sri Lankan suicide bombers of 2019, some of the bombers were foreign educated and came from affluent backgrounds.[15] In India, there exists a large grooming infrastructure which is involved in "talent spotting" and radicalisation activities. These talent spotters, it was observed, work openly, yet are not easy to prosecute owing to lack of clear "criminality" in their actions. Radicalism must be dealt with by intelligently balancing "soft" and "hard" approaches.

3) Vulnerabilities of India's maritime and coastal security architecture

In the last few years, the thrust of India's maritime strategy has been to leverage the advantages of the country's vast coastline for economic activities.[16,17] For instance, a substantial portion of India's domestic energy production comes from the Mumbai High offshore fields on the western coasts.[18] There are similar endeavours underway to extract energy from offshore oil and gas fields on the eastern coasts. With these economic activities in mind, the Government of India has initiated the Sagarmala Programme[19] to enable port-led development by devoting significant fiscal resources for the modernisation of existing ports and the establishment of new ones.[20] Additionally, under this programme, 14 coastal economic zones have been identified to promote port-led industrialisation in different maritime states and Union Territories.[21] The Sagarmala Programme, when combined with Bharatmala[22]— the ambitious centrally-sponsored roads and highways project—will facilitate trade and the movement of resources between ports and mainland cities and thus bridge the regional economic disparities across the country.

Trade between India and other countries is largely conducted through sea routes. India's ports handle 70 percent of its external trade in terms of value.[23] As the value and numbers of India's maritime assets increase in the coming years, their vulnerability to attacks by terrorist groups will also heighten.

Maritime and coastal security has its own set of challenges. The 26/11 Mumbai attacks and the 1993 serial bomb blasts in Mumbai[24] in many ways exposed the vulnerabilities in India's maritime security architecture. To begin with, given the nature of the seas being porous, policing is difficult. As multiple agencies are trying to get into the domain of coastal security there is a need to ensure that their duties are spelt out and there is a clear-cut sense of command, control, responsibility, and coordination.

One significant reform undertaken post-26/11 was the clear designation of coastal security responsibilities to different agencies. The Indian Navy would be primarily responsible for ensuring security of areas beyond 12 nautical miles, assisted by the Coast Guard. The Coast Guard would be responsible for ensuring the coastal security between five to 12 nautical miles, while the marine police will ensure security between the base-line to five nautical miles. At an organisational level, the Indian Navy has been designated in-charge of all aspects of maritime security.[25] Coordination between various agencies has improved, joint exercises are being regularly conducted to familiarise with the standard operating procedures (SOPs), and the levels of surveillance has been enhanced as well.[26] Joint trainings are also integral to this effort.

Another challenge related to coastal security is that the perception of coastal states on matters pertaining to their security varies. Many of the port or maritime-based infrastructure coming up in India's coastal cities are largely technology-dependent. This means their vulnerability to cyber-attacks increases substantially.

The fleet strength of the Coast Guard (ship and air elements) has been enhanced to ensure increased coastal security. The Coast Guard is employing electronic means to increase maritime surveillance.[27] They have also increased their joint exercises with the relevant agencies and state marine police forces.

After 26/11, countries around the Indian Ocean Region have expressed willingness to work with India on the aspects of maritime and coastal security.

This development must be strengthened by putting more thought into bilateral and multilateral scenario-building exercises. Civil servants posted in coastal districts should have more maritime consciousness, and retired experts must get involved in capacity building within the maritime domain.

4) Cyber security

There has been an increasing trend towards cashless modes of financial transactions in recent years.[28] This is amongst the Indian government's policy priorities,[29] as citizens are being encouraged to conduct cashless transactions to ensure greater transparency and accountability.[30] Additionally, advances in information technology have enabled various infrastructural and industrial capacities to become technology-driven. The government is also putting greater emphasis on expanding the coverage of digitisation across the country to enable the central and state governments to deliver their services and ensure governance.[31,32] The increasing dependence on technology for governance, delivery of services and financial transactions will bring in transparency, swiftness and increasing accessibility to services. It also brings its own set of vulnerabilities.

Indeed, the digital domain has become a target for India's adversaries in the last few years. To ward off these threats, India should build robust systems to ensure uninterrupted and safe operations of the country's digital infrastructure. Many other countries are also grappling with the threats posed by state and non-state actors by using technology-driven information warfare. The multiple challenges emanating from the cyber domain include interference in elections through the use of propaganda in social media, fake news leading to panic, and digital disruption of energy assets and transportation systems.

Tackling these cyber challenges will require a great deal of coordinated effort as well as innovative approaches at the inter-agency level. To begin with, it is imperative to address the structural and organisational issues pertaining to the country's cyber security apparatus. The challenges are enormous, and greater financial investments are needed. India must tap into its rich pool of human resources in the domain of information technology, data science and cyber issues.

Some states have already initiated concerted steps to ramp up their cyber capabilities. Besides enacting cyber legislations, the government has also undertaken organisational measures by establishing new centres for cyber security such as the National Critical Information Infrastructure Protection

Centre and the National Cyber Coordination Centre; creating a division covering Cyber and Information Security within the Ministry of Home Affairs; and improving institutional capacity building through training of personnel and generating awareness.[33]

RECOMMENDATIONS FOR THE WAY FORWARD

1) Collaboration between government, media and public

There should be greater cooperation and dialogue between the public and decision-makers. It is time for India to give serious thought to the idea of creating neighbourhood 'Awake Cells' comprising youth activists and concerned citizens. These 'Awake Cells' would ensure that citizens who are conscious on aspects of security would act as feeders of information to the security agencies – particularly on any unusual and suspicious activity in their areas. Inputs from these sources would enable the security agencies to have better domain awareness. It is also important for law enforcement agencies to acquire information from the people in proximity of the attack site. Here, the media can play an important role in providing critical information at the site of a terrorist attack. Given that media practitioners reach a terror-attack site faster and interact with people around the area, it is important to quarantine such early information and pass them on to the security forces that have been deployed to respond.

2) Containing the attack and the perpetrators

The first response during a terrorist attack is to contain the terrorists. Till the time the specialised forces reach the site, the local police forces must be capable and equipped to engage the terrorists through the use of force. In this regard, following 26/11, state forces in Mumbai have substantially improved their capabilities. The local police stations, combat vehicles and the Quick Reaction Teams (QRT) are all available to provide an immediate and a "graded" response to any future incident.

3) Enabling timely transportation of security forces during terrorist attacks

It is essential that responders are able to reach the site of the attack in the shortest time. This is a serious challenge in India's urban spaces, given the heavy congestion and their haphazard layouts. The imperative is for the seamless movement of forces and their equipment through planning and physical power to manage, restrict and divert traffic movement. In turn, traffic management faces challenges owing to budgetary constraints and lack of human resources. The problems are compounded by jurisdiction issues caused by a multiplicity of controlling agencies within the state and city administrations.

The current investments in mass public transport systems such as Mumbai's Metro are a step in the right direction. It is also pertinent to consider creating infrastructure such as water transport to ferry people, ponder disincentivising the purchase of more cars, and phase out old vehicles.

4) Increasing the capabilities of security forces

The National Security Guard (NSG) has been involved with capacity building of different state forces, including conducting joint exercises with various agencies. There is a need to consolidate their efforts and graduate from single-agency, standalone exercises to multi-agency ones. The NSG exercise held in 2017 at Jamnagar, where 12 agencies participated in elaborate exercises over two days, is a good model to scale-up and replicate across the country. Continuous and incremental improvement in the availability of firepower and protection equipment across all police stations must be considered with adequate funding for such capacity building. India must integrate all its resources for deployment to combat any future contingency. Essential equipment and weapons systems must be acquired.

5) Institutionalising swift decision-making

There is a need for swiftness in decision-making on security issues. Decision-makers must be given the mandate to use their discretion while taking key and quick decisions. The rules, regulations, guidelines and circulars give broad outlines for the competent authorities and they must be empowered to interpret these rules and guidelines and proactively decide on the appropriate course of action. Counterterrorism strategies should be formed in an integrated manner. For example, terrorism cannot be seen from the perspective of whether the matter falls under the ambit of Home Affairs or Defence Ministry, or the state or centre.

The perception regarding India as a country being a "soft state" needs to be changed. The surgical strikes by India's special forces in 2016 and the air strikes on terrorist camp in Balakot in Pakistan following the attack on the CRPF convoy in Pulwama in February 2019 marks a change in India's strategy in responding to cross-border terrorism.[34,35]

6) Building the overall resilience of cities

The planned development of cities is a prerequisite for any sound internal security apparatus. Given the increasing clustering of populations in the cities as well as the concentration of economic output largely within urban areas, the terrorism landscape is also undergoing transformation. Security preparedness, therefore, needs to also evolve in these contexts. There is a need to think more about holistic urban planning as cities are places wherein development transformation can be made or disrupted. Historically, cities have demonstrated remarkable resilience and have bounced back from catastrophes.

CONCLUSION

Over ten years since the 26/11 Mumbai attacks, there has been a discernible improvement in India's counterterrorism mechanisms. Complex challenges, however, continue to confront India. These include the lack of inter-agency coordination and inefficient decision-making. As the manifestations of terrorism continue to change rapidly and become increasingly technology-centric, State forces responsible for the country's counterterrorism response will have to adapt to these shifts and build the resilience of India's security ecosystem.

ABOUT THE AUTHORS

Dhaval D Desai is Senior Fellow and Vice President at Observer Research Foundation, Mumbai.

Parjanya Bhatt is a Research Fellow at ORF Mumbai.

ANNEX

26/11 – REMEMBRANCE & RENAISSANCE

A conference organised by Observer Research Foundation-Mumbai

24 November 2018 / Mumbai

Participants

1. Vice Admiral Anil Chopra, PVSM, AVSM (Retd.); Distinguished Fellow, Observer Research Foundation (ORF)
2. Mr. Aromar Revi, Director, Indian Institute of Human Settlements, Bangalore
3. Dy. IG B Murugan, Chief Staff Officer (Ops), Coast Guard Regional HQ (West)
4. Maj. Gen. Bipin Bakshi, VSM; IG (Training), National Security Guards
5. Mr. Dhaval D Desai, Vice President and Senior Fellow, ORF
6. Col. Hemant Sahni, NSG, Mumbai hub
7. Rear Admiral K. G. Vishwanathan, VSM, Flag Officer Doctrines & Concepts, Western Naval Command
8. Ms. Prabha Rao, Former Senior Fellow, Institute for Defence Studies and Analyses
9. Dr. Ramanath Jha, Distinguished Fellow, ORF
10. Mr. Ravindra Kumar, DIG, Airport West Zone, Central Industrial Security Force
11. Commander Rohit Mishra, NM, Executive Officer, INS Abhimanyu, Western Naval Command
12. Commodore S. Kesnur, Director, Maritime Warfare Centre (Mumbai)
13. Brig. Sujit Narain, YSM, SM, Defence Intelligence Agency
14. Brig. Sunil Sheoran, SM, Indian Army
15. Mr. Sunjoy Joshi, Chairman, ORF
16. Mr. V. Balachandran, Former Special Secretary, Cabinet Secretariat, Government of India
17. Mr. Vivek Sahai, Distinguished Fellow, ORF

Observers

1. Col. Ashish Singh, NSG
2. Dr. Sanket Kulkarni, Research Fellow, ORF
3. Mr. Ameya Pimpalkhare, Associate Fellow, ORF
4. Dr. Ayjaz Wani, Research Fellow, ORF
5. Mr. Nilesh Bane, Research Fellow, ORF

ENDNOTES

1. Pushan Das, 'The chaos that is counter-terrorism in India' in '26/11: A decade after', Eds. Harsh Pant and Maya Mirchandani, *Observer Research Foundation*, ORF Special Report No. 77, December 2018, Accessed 22 April 2019, https://www.orfonline.org/wp-content/uploads/2018/12/ORF_Special_Report_77.pdf

2. James Miller, 'The Evolution Of Terrorism Since 9/11', *Radio Free Europe Radio Liberty*, 6 June 2016, Accessed: 23 April 2019, https://www.rferl.org/a/evolution-of-terrorism-since-911/27782825.html

3. Samir Saran and Kabir Taneja, 'Technology and Terror: A new era of threat in a borderless online world', *Observer Research Foundation*, 21 May 2019, Accessed 25 May 2019, https://www.orfonline.org/expert-speak/technology-and-terror-a-new-era-of-threat-in-a-borderless-online-world-51079/

4. Michael Sheetz, 'The rise of tech-savvy global terrorism networks', *CNBC*, 4 December 2015, Accessed 26 May 2019, https://www.cnbc.com/2015/12/04/the-everyday-technology-helping-terrorists-plot-evil.html

5. Op. cit, Samir Saran And Kabir Taneja.

6. Vappala Balachandran, 'Questions on 26/11 still not answered', *The Sunday Guardian*, Accessed 26 May 2019, http://www.sunday-guardian.com/analysis/questions-on-2611-still-not-answered

7. David Johnston, '9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses', *The New York Times*, 24 July 2003, Accessed 27 May 2019, https://www.nytimes.com/2003/07/24/us/9-11-congressional-report-faults-fbi-cia-lapses.html

8. N K Bhatia, 'Human Intelligence (HUMINT) as a Driver for Intelligence Operations', *Centre for Landwarfare Studies*, Issue Brief No. 79, June 2016, Accessed 25 May 2019, https://www.claws.in/images/publication_pdf/1646040662_IB79-Bhatia-09-06-16.pdf

9. ason Burke, 'Al-Qaeda launches online terrorist manual', *The Guardian*, 18 January 2004, Accessed 27 May 2019, https://www.theguardian.com/technology/2004/jan/18/alqaida.internationalnews

10. 'Handlers asked 26/11 Pakistani terrorists to identify themselves as Hyderabad residents', *India Today*, 26 November 2018, Accessed 28 May 2019, https://www.indiatoday.in/india/story/26-11-attackers-pakistani-handlers-hyderabad-mujahideen-1396371-2018-11-26

11. Rashmi Rajput, '26/11 handler had gone under scalpel to change look', *The Indian Express*, 28 November 2018, Accessed 28 May 2019, https://indianexpress.com/article/india/26-11-handler-had-gone-under-scalpel-to-change-look-5468060/

12. 'Headley reveals how Pak handlers used live TV to guide 26/11 attackers', *NDTV*, 26 May 2011, Accessed 28 May 2019, https://www.ndtv.com/india-news/headley-reveals-how-pak-handlers-used-live-tv-to-guide-26-11-attackers-456741

13. Amitabh Mattoo, 'View: Focus on stopping the radicalisation & alienation of Kashmiri youths', *The Economic Times*, 17 February 2019, Accessed 29 May 2019, https://economictimes.indiatimes.com/news/politics-and-nation/win-the-hearts-of-young-kashmiris/articleshow/68027557.cms?from=mdr

14. M.K. Narayanan, 'Adrift in the valley', *The Hindu*, 30 May 2016, Accessed 29 May 2019, https://www.thehindu.com/opinion/lead/Adrift-in-the-Valley/article14346052.ece

15. Jason Burke, 'Why Sri Lanka attackers' wealthy backgrounds shouldn't surprise us', *The Guardian*, 25 April 2019, Accessed 30 May 2019, https://www.theguardian.com/world/2019/apr/25/why-sri-lanka-attackers-wealthy-backgrounds-shouldnt-surprise-us

16. 'Maritime clusters & CEZ to bolster India's maritime sector growth under Sagarmala' *Press Information Bureau*, 31 August 2016, Accessed 31 May 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=149411

17. 'Address by External Affairs Minister at the 2nd Indian Ocean Conference', *Press Information Bureau,* 31 August 2017, Accessed 31 May 2019, https://mea.gov.in/Speeches-Statements.htm?dtl/28907/Address+by+External+Affairs+Minister+at+the+2nd+Indian+Ocean+Conference+August+31+2017

18. 'ONGC makes significant oil, gas discovery in Arabian Sea', *Live Mint*, 1 January 2018, Accessed 31 May 2019, https://economictimes.indiatimes.com/industry/energy/oil-gas/ongc-makes-significant-oil-gas-discovery-in-arabian-sea/articleshow/62325992.cms?from=mdr

19. 'Sagarmala: Concept and implementation towards Blue Revolution', *Press Information Bureau*, 25 March 2015, Accessed 31 May 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=117691

20. 'Sagarmala Programme', Ministry of Shipping, *Press Information Bureau*, 9 March, 2017, Accessed 31 May 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=159037

21. '14 Coastal Economic Zones being developed under Sagarmala', Ministry of Shipping, *Press Information Bureau*, 8 February 2018, Accessed 31 May 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=176381

22. 'Shri Gadkari says highways works worth Rs 8 lakh crore will begin before the end of 2018 under Bharatmala Pariyojana', *Press Information Bureau*, 25

October 2017, Accessed 1 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=171930

23. 'Year End Review 2018 – Ministry of Shipping, *Press Information Bureau*, 13 December 2018, Accessed 1 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=186373

24. 'Bombay Blast Cases', Central Bureau of Investigation, Government of India, Accessed 1 June 2019, http://www.cbi.gov.in/fromarchives/bombayblast/mumblast.php

25. 'Indian Navy Coordinates Largest Ever Coastal Defence Exercise Ten Years After 26/11', Ministry of Defence, *Press Information Bureau*, 22 January 2019, Accessed 1 June 2019, http://www.pib.nic.in/Pressreleaseshare.aspx?PRID=1560995

26. 'Initiatives to Strengthen Coastal Security', Ministry of Defence, *Press Information Bureau*, 25 November 2014, Accessed 1 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=111871

27. 'Measures to enhance Coastal Security', Ministry of Defence, *Press Information Bureau*, 5 March 2018, Accessed 2 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=176953

28. 'Current fraud trends in the financial sector', Joint report by Associated Chambers of Commerce and Industry of India and Price Waterhouse Cooper, June 2015, Accessed 1 June 2019, https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf

29. 'Digital Payment Revolution: Facts & Figures', *Press Information Bureau*, 14 April 2017, Accessed 2 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=161040

30. Ibid.

31. 'National e-Governance Plan', Ministry of Electronics & Information Technology, , Accessed 2 June 2019, https://meity.gov.in/divisions/national-e-governance-plan

32. Refer to Minister of State (Ministry of Personnel, Public Grievances and Pensions & PMO) Dr. Jitendra Singh's reply to a question by Shri. Konda Vishweshwar Reddy in Lok Sabha on November 30, 2016. For details: *Press Information Bureau*, 'E-Governance', 30 November 2016, Accessed 2 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=154617

33. For more details on steps taken to improve the cyber security ecosystem in India, see MoS (Home) Shri. Kiren Rijiju's reply on 18 December 2018 in Lok Sabha 'Cyber Security', *Press Information Bureau*, 18 December 2018, Accessed 2 June 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=186564

34. Nissar Ahmad, 'February 14, 2019: When a CRPF convoy came under attack in Pulwama on Srinagar-Jammu Highway', *The Hindu*, 16 February 2019, Accessed 3 June 2019, https://www.thehindu.com/news/national/february-14-2019-when-a-crpf-convoy-came-under-attack-in-pulwama-on-srinagar-jammu-highway/article26292339.ece

35. Arun Prakash, ‘India’s crucial security challenge is not external, but relates to maintenance of domestic harmony and unity’, *The Indian Express*, 4 May 2019, Accessed 3 June 2019, https://indianexpress.com/article/opinion/columns/india-national-security-defence-bjp-pakistan-china-5709644/

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000 Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org