



ORF ISSUE BRIEF

JULY 2015

ISSUE BRIEF # 98

India's Intelligence Agencies: In Need of Reform and Oversight

Manoj Joshi and Pushan Das

Introduction

The national security threats that India confronts today are much more diverse and complex than ever before. These threats range from nuclear-armed adversaries like China and Pakistan, to Maoists, and militancy and terrorism arising from within its borders and beyond. The question that we must ask is whether the country has a strategic measure of these challenges and the willingness and ability to confront them and, if required, pre-empt them. The tasks before India's intelligence community are similar to those that are confronted by their counterparts across the world: they relate to strategic intelligence, anticipatory intelligence, current operations, cyber intelligence, counterterrorism, counter proliferation and counter intelligence. The objectives require integrated mission and enterprise management, and innovation.¹ They are contingent upon the security challenges faced by a nation at a given time and necessitate reform and reorientation to meet evolving threats. Historically, intelligence agencies have been forced to reform and restructure because of failure. In India, too, reforms in intelligence agencies have occurred, primarily after wars and crises.

This report shall highlight the tasks before the Indian intelligence agencies in implementing reforms and restructuring. It will seek to highlight the lack of political guidance and, in this regard, examine why recommendations made by previous task forces and committees have not been implemented.

The Conference

The report draws considerably from the conference on *The Future Challenges to India's Intelligence System*, organised by the Observer Research Foundation on 24 February 2015, which featured discussions

Observer Research Foundation is a public policy think tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics and business leaders.

involving serving and former Intelligence officers, research scholars and specialists interested in intelligence affairs.

The discussions at ORF were divided into three broad themes: External intelligence; internal intelligence; and technical intelligence. The key issues that emerged from the discussions are the following:

- Co-ordination and tasking in need of improvement amongst intelligence agencies and between state and Central agencies
- Intelligence collection is ad-hoc in the absence of clear-cut requirements from the consumers of intelligence
- Poor cadre management and inability to recruit qualified language specialists and technical skills result in a shortage of personnel
- Lack of intellectual capacity and investment in education system exacerbate recruitment shortfalls in intelligence agencies. Engaging private players for specialist tasks is therefore necessary.
- Agencies suffer from chronic shortage of military expertise Big data analytics capabilities need to be commissioned and customised for the Indian context
- Special forces capabilities need to be ramped up and their concept of use 'married' with the capabilities of intelligence agencies
- China's growth and the multiplication of its capabilities requires a more focused effort in TECHINT (Technical Intelligence) and HUMINT (Human Intelligence)
- Parliamentary statute is the key for creating accountability in intelligence agencies
- Lack of political attention and effective guidance has prevented reform and optimal functioning of the intelligence system

An Overview

There are currently 14 intelligence agencies operating in India with different and sometimes overlapping mandates. Most of these 14 intelligence agencies have come into being as a response to changing strategic environment and shortcomings in the intelligence framework on several occasions. Following the debacle of the 1962 war with China, the Directorate General of Security (DGS) was set up within the Intelligence Bureau (IB), with its operational unit, the Aviation Research Centre (ARC), tasked with obtaining intelligence on China. Following the failure of IB in the 1965 war against Pakistan, the government decided to hive off external intelligence under a new agency, the Research & Analysis Wing (R&AW) and linked the DGS with it.

Though there were various measures of internal reorganisation and restructuring, the next wave of reforms came after the 1999 Kargil war, when there was a colossal failure on the part of various

security agencies in detecting Pakistani incursions across the Line of Control (LOC). The Defence Intelligence Agency (DIA) was set up in 2002 and tasked to collect, collate and evaluate intelligence from other service directorates and other agencies. The DIA was to control inter-service technical intelligence (TECHINT) assets primarily in Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT). In 2004 the National Technical Research Organisation (NTRO) was set up to be the premier TECHINT agency of the country with the mandate to collect communications intelligence (COMINT), electronic intelligence (ELINT), IMINT and cyber intelligence. The NTRO's mandate created quite a storm, since it was given tasks already being done by other intelligence services, resulting in inter-agency turf battles that led to problems in its functioning for nearly a decade.

The biggest problem has been the lack of co-ordination amongst the intelligence community in India. Each agency looks out for itself and guards its turf zealously. There is need for strict guidance and supervision to ensure that there is cooperation and coordination. Former Union Home Minister P. Chidambaram enforced co-ordination at the apex level after the Mumbai attacks of 2008, but after his departure, the new Home Minister has not kept up the process. Since the Home Minister has a vast repertoire of responsibilities, there is need for a Director National Intelligence, or a Minister, to arbitrate between agencies and promote greater collaboration between them.

The question of accountability in the Indian context is no less important. Hardly anyone, if at all, is held accountable for serious failures on the security front—the inability to assess Chinese intentions during the 1959-1962 period, to pinpoint Pakistan's additional armoured division in 1965, or the plans for Operation Gibraltar, the LTTE's reaction to the India-Sri Lanka Accord of 1987, the Kargil incursion, or the Mumbai attacks of 2008. This has led to a culture where no person or agency is held responsible for major intelligence failures and hence the intelligence agencies have had little or no accountability. This is only partly due to excessive secrecy within which intelligence organisations and processes work. It is more part of a systemic flaw where authority and accountability do not go together.

The Mumbai attacks in 2008 resulted in the implementation of further reforms at apex level co-ordination. The attack, while not a failure of intelligence gathering, was a failure of timely action and co-ordination. However, the Indian experience of reform and restructuring has, till now, been visited by only limited success. The reasons for this have been many and will be laid out in the conclusion.

Internal Intelligence:

India's internal security environment is fraught with a number of challenges. They range from cross-border terrorism, a Maoist rebellion, insurgencies in North-east India, violent Islamic extremism, communal and sectarian violence, as well as illegal migration, human trafficking, narcotics smuggling and money laundering. Such a wide gamut of threats requires a multi-pronged approach to intelligence gathering which would be beyond the remit of a single agency.

The Indian intelligence system emerged as an extension of the police system to track and counter the Indian national movement during British rule. This is a legacy and structure that it has not quite broken out of to meet the challenges of modern intelligence-gathering. It carries the burden of an intellectual infrastructure that has failed to build competencies essential to intelligence operations in a vastly different environment than the pre-Independence era. The lack of a dedicated intelligence cadre and the continuing practice of staffing intelligence agencies with police officers has resulted in agencies playing down the importance of language specialists, social scientists, technical specialists and cyber analysts.

The IB has over the years become a reporting arm of the government, often treated as an appendage of the Ministry of Home Affairs (MHA). Its location at the MHA, meant for convenience of administration, has resulted in supervision of the IB by the Home Ministry. The tight political control by the MHA made IB focus more on domestic and political matters at the expense of other security challenges. The agency also has responsibility over local police functions in the form of verifications and background checks, which further ties down its already-limited manpower. All these factors put together have drastically compromised the IB's capabilities especially in the area of counter-intelligence, which is one of its primary mandates, to begin with.

In 2001, a Group of Ministers (GoM) had recommended an end to this practice and sought to confer the rank of Secretary to the Director of IB, on par with the status of the R&AW counterpart. On the GoM advice, the IB was designated as the premier Counter-Terrorism agency and authorised to create Multi-Agency Centre (MAC) and Subsidiary Multi-Agency Centres (SMACs) to collate and process intelligence inputs from various sources. These were to be located in state headquarters comprising representatives from various agencies from the state and the centre.

External Intelligence:

The R&AW is the sole agency tasked to gather external intelligence. The organisation was created by an executive order and not by parliamentary statute. It was interpreted, at the time of the R&AW's creation in 1968, that it would provide HUMINT and TECHINT to fulfil its mandate. Over the years there has been criticism that the R&AW relies too much on TECHINT and Open Source Intelligence (OSINT), and does not pay enough attention towards developing human intelligence (HUMINT). The blame for this deficiency should be shared equally, if not more, by the political leadership which, often, chose to limit R&AW's critical operational mandates.

The R&AW is faced with a number of challenges which have constrained its ability to deliver external intelligence in a rapidly evolving world. The organisation often works under embassy cover which limits its ability in generating human intelligence. The Aviation Research Centre (ARC) gathers signals and image intelligence on China, a task which overlaps with the mandate of the National Technical Research Organisation and the Defence Intelligence Agency. The IB too has recently set up a China Desk, though its functions are not quite clear but presumably relate to counter-intelligence. While

overlapping of mandates is natural, there is a need to clearly articulate the principal focus of each of the agencies to yield optimal output and avoid failures.

Recruitment to the R&AW is still dependent on deputations from other central agencies especially the Indian Police Service. Its intake of scientists, cyber analysts and linguists is below required levels. The lack of lateral entry options reduces the agency's ability to recruit off the market. Elsewhere, intelligence agencies have moved much faster and much further in recruiting experts from private sector and academia to support intelligence operations.

Over the years, R&AW's efforts towards seeking 'outside' expertise have been few and erratic, at best. The agency is also faced with intelligence requirements being framed in an ad-hoc manner. Consumers are reluctant to clearly spell out their requirements, in part because they have not applied their minds to the task, and in some measure because they have not worked out just how intelligence can be applied to enhance their own effectiveness. There is need for a better mechanism for tasking and fusion of intelligence with policy. Both the Joint Intelligence Committee (JIC) and the National Security Council with a well-staffed secretariat are mandated to fill this very gap, have not measured up to expectations, particularly in dealing with asymmetric threats like the Mumbai attacks of 2008.

Technical Intelligence:

In view of the significant role of technology in intelligence collection, analysis and dissemination, an important development was the creation of the National Technical Research Organisation (NTRO). The NTRO's mandate was to plan, design, and set up and operate major new TECHINT facilities. It was tasked with the establishment of secured digital networks to disseminate TECHINT to all the agencies as well as to enable information flow between agencies. As part of this, the NTRO is to host a common database of information so that it could be easily and quickly disseminated to other agencies. The agency is tasked with monitoring missile launches in countries of interest and responsible for defensive and offensive cyber operations. Another agency that was created was the tri-Service Defence Intelligence Agency (DIA). It controls the TECHINT assets of the three armed services, primarily the Army's erstwhile Signals Intelligence Directorate and the Defence Image Processing Analysis Centre (DIPAC) in Delhi and the Defence Satellite Control Centre (DSSC) in Bhopal. There have been issues between DIA and NTRO over space-based assets and their control.

The creation of a new agency in the form of the NTRO resulted in predictable resistance, especially since it was given tasks which were being done by others. Creating facilities anew would have been an expensive proposition, and so, the obvious way was to transfer assets being held by the others. Strangely enough, this problem was not anticipated and addressed by the government. Subsequently, a committee was set up by the National Security Advisor (NSA) to come up with proposals and the NTRO came up only in April 2004, though its Chairman, former ARC head RS Bedi, had been appointed a year earlier.² Another issue has been the overlap between NTRO and the ARC. This has created a situation where NTRO controls high-resolution satellites and is responsible for space- and

ground-based COMINT, while the ARC is responsible for collecting IMINT and COMINT through aircraft mounted sensors.

The notification establishing the NTRO stated that its task was to gather COMINT, ELINT, IMINT and cyber intelligence and termed it as the premier technical intelligence agency of the country. There was some criticism that the agency's task was to merely collate and make the information available to other agencies, but when it was set up, it was clearly given an analysis role as well.

Poor management and turf battles have, however, led to the agency over-exceeding its capacity and thereby failing to meet some important target areas.

Issues for reform

First and foremost, the Indian government needs to decide what challenges must be addressed by its contemporary agencies. What kind of an intelligence system would best serve internal and external security requirements? How best to strike a balance between traditional politico-military intelligence operations in target countries and working on pre-empting and containing non-state actors? How much emphasis should be laid on economic, commercial and scientific intelligence?

Second, specialisation is important in the modern era and multiplicity of agencies is inevitable. Quite often, the issue of turf war is over-blown. In fact, a certain level of redundancy among intelligence agencies can prevent a systemic failure in one outfit from becoming a catastrophic, all-round failure.

Oversight

Amongst democracies, India alone lacks any oversight of its intelligence agencies. As previously mentioned, its agencies do not have any constitutional authority. The problems with oversight and accountability are many. Intelligence agencies are reluctant to submit to any oversight as it is. In addition, intelligence agencies are equally concerned with the level of inexperience and ignorance among the political class with matters relating to security. The agencies have to contend with the very real worry of information leak if every action of theirs becomes subject to parliamentary scrutiny. However, given the fact that there are several senior politicians who have served government in key ministries, it should not be too difficult to construct an oversight mechanism comprising a mix of former members of the Cabinet Committee for Security (CCS) and serving ministers. Alternatively a small ministerial committee, aided by external experts, could monitor issues related to performance, finance and privacy.

Successive governments have historically been reluctant to create oversight mechanism for intelligence agencies. One reason could be the manner in which the governments use the Intelligence Bureau in domestic political espionage—in clearer terms, spying on political rivals. This is a widely known fact, yet politicians conveniently overlook it when they take charge of the government.

However, there is another kind of oversight which can be introduced—an office of the Inspector General who could be from the intelligence services or a security professional reporting to the top intelligence coordinator or the National Security Advisor.

For the present, however, the more practical method seems to be the oversight provided by the National Intelligence Board (NIntB) comprising of the NSA (Chair), the Principal Secretary to the Prime Minister and the Cabinet Secretary who in their own way separately report to the PM as well.

Apex level management

At present, presumably this is being done by the NIntB, and the Chairman Joint Intelligence Committee (JIC) functions as the member-secretary of the unit. But the question that repeatedly comes up is whether the NSA, Cabinet Secretary and the Principal Secretary to the PM have the necessary time and attention span to provide the kind of supervision and leadership needed for the task of high-level direction to the intelligence apparatus—oversight, apex level tasking, supervision of agency and coordination between agencies. The government could consider a full-time intelligence adviser to do so, or even appoint a Director National Intelligence to do the task and place him under the NSA and make him a member of the NIntB.

Coordination and tasking

Coordination between the Centre and the states, and within states at district and thana (local police station) level remains deficient even after setting up new mechanisms like Multi Agency Centres (MAC) and Subsidiary Multi Agency Centres (SMAC), to enable intelligence sharing and coordination amongst multiple agencies. There is need for higher level coordination which involves the Home and Police departments working together with their Central counterparts. This is unlikely to come through an administrative fiat, and would need to be subject to legislation. The Defence Intelligence Agencies (DIA) offers an apt illustration. Its principal infirmity is the absence of the person or position at the top of the pyramid—the Chief of Defence Staff. This has created several problems for the organisation which was otherwise robust and has potential. The experiment with annual tasking done through the NSCS came to a halt in 2008, after two cycles. Thereafter, the agencies have been doing “self tasking” based on their respective charters. Given the complexity of the security environment facing the country, single-point tasking is neither adequate nor reliable.

Self-tasking has its own problems since it puts the agency in policy-maker's role, which is not an ideal solution. It is up to the consumers and policy-makers to decide what they want from an intelligence agency and, for coordination purposes, this should be mediated at the apex level by the NIntB and at a lower level by the JIC or NSCS. There is need for a sharper look at the Intelligence Cycle which moves from tasking and planning, collection, processing, analysis in terms of original tasking, and dissemination back to the original task giver. The system needs to be sharply defined and degrees of separation need to be maintained between collection and analysis.

Shortage of personnel and recruitment

One of the major problems with all intelligence and specialised agencies in government is the challenge of addressing personnel issues. Some of the personnel shortage arises from the inability to recruit the right kind of people for specific tasks—technically skilled staff or linguists for instance. Equally important is the issue of cadre management—ensuring that the personnel are able to progress through the bureaucratic system in an orderly and productive manner and that no morale issues crop up because there is bunching of ranks at a particular level.³

Intelligence agencies also suffer from a chronic shortage of military expertise. While a system of deputation exists, military officers are reluctant to be posted to these agencies. In the absence of equivalent rank in the agencies, the military officers are compelled to work at a level which is often lower than their Service rank. Persistent staff shortages have raised a debate about a distinct cadre for the intelligence agencies with independent recruitment and promotion system similar to the civilian bureaucracy. The obvious answer for technical issues is for the agencies to think in terms of getting private contractors to work for them. But India has no system for providing non-government personnel security clearances that would be required for such work.

In the current framework, for there to be meaningful and long-term reform there needs to longer tenures for key personnel and chiefs like they have in western nations. There needs to be discussion on the time periods required to implement institutional reforms.

Open Source Intelligence

The internet has ushered in an information revolution beyond the traditional mediums of open source information like newspapers and television. At present the NTRO handles Open Source, mainly through the monitoring of TV and radio channels. It has often been indicated that the R&AW too draws a lot of information from open sources. Open source information now emanates not only from traditional media sources but also social media and other internet-based applications apart from professional journals and technical literature. The internet has also become one of the primary sources of communication all over the world for governments and non-state actors and people. There is a need for one agency to focus on open source information and internet-based communications which will cover all mediums, including newspapers, radio, the internet and social media sites like Twitter and Facebook.

Legislation

There are two reasons why the intelligence agencies need to be governed by laws framed by the Parliament. First is the need to strengthen their accountability. The Indian agencies function outside the purview of any legislation, making it difficult to implement administrative, operational or financial accountability. The IB was established by the British in December 1887 as a part of the Indian Special

Branch, but it has no legislative authorisation. The other agencies have come up through executive orders as well. Given the enormous power these agencies wield, it is important to legislate their functions and provide for means to guarantee the citizens against their misuse.

The second reason is the need for clarity in the functioning of various agencies. By definition, legislation is precise because its words have legal implications. The enormous powers provided to the agencies should be carefully spelt out in a legislative format to ensure that they are viewed with all the seriousness they deserve. There should be no room for misinterpreting authority or tasks of the agencies. A quick look at the US Intelligence Reform and Terrorism Prevention Act of 2004 will reveal precise and detailed wording, spelling out duties, responsibilities and authority.

In March 2011, Manish Tewari, who also subsequently served as a minister in the UPA government introduced a Private Member's Bill “to regulate the manner of functioning and exercise of powers of Indian Intelligence Agencies”. The Bill will have authority within the country and outside of it, and aimed at providing “for the coordination, control and oversight of such agencies.” One of the aims of the Bill was to provide legislative authority for the functioning of the agencies, another was to ensure against the misuse of their powers. The section “authorisation and procedures” specified that any kind of interception of communication or break-in could be conducted without a warrant issued by a designated authority.

The Bill also provided for a National Intelligence and Security Oversight Committee headed by the Chairman of Rajya Sabha, Speaker of the Lok Sabha, the PM, Home Minister, Leader of the Opposition in the two Houses of Parliament, and two MPs nominated by the Chairman RS and Speaker LS. The Cabinet Secretary would be the secretary of the Committee. This Committee would draw up and table an annual report, appoint an Intelligence Ombudsman to deal with staff grievances and administrative issues of the agencies and constitute a National Intelligence Tribunal to investigate complaints against the agencies. The Bill remains in the long queue of legislations waiting to be put to vote.

HUMINT and TECHINT

The world is going through a proliferation of information. Big data analysis in India is still in its infancy, but clearly it is the trend of the future. Documents that came out about the Boundless Informant programme of the US' NSA indicated that the agency collected almost 3 billion bits of intelligence from US computer networks, and 97 billion worldwide, in a 30-day period in 2013.⁴

According to a report, India's Central Monitoring System and National Cyber Coordination Centre will, between them, enable government to access all phone calls and internet-related data 24x7 and on a real time basis.⁵ Some of the physical elements of these systems are already in place, but there is, as yet, no legislative authorisation for this large-scale invasion of privacy, penalties against the misuse of data thus obtained, or any guarantees against misuse.

The challenge of HUMINT remains, as intelligence agencies face critical shortages of skilled manpower. This is as much a problem of the lack of manpower as of the tendency to take the easy way out and rely on TECHINT to do the needful. The non-availability of personnel with the requisite language skills or aptitude for intelligence work is of serious concern. The system of time-bound deputation from the police and armed forces and the lack of an intelligence cadre make it tough for organisations to create and retain skill required for such specialised work. Military expertise in intelligence agencies needs to be improved by implementing a policy of giving equivalent rank to military personnel vis-a-vis their civilian counterparts.

Counter-Terrorism and Counter-Insurgency

The issue of an effective counter-terrorism and counter-insurgency system remains. The failure to create the National Counter-terrorism Center (NCTC) is one aspect of it. The government has to think hard and see how such a system can come up, even while meeting the requirements of federalism. In the wake of the 2008 Mumbai attacks, the government was able to push through legislation that created the National Investigation Agency (NIA) dedicated to investigating terrorism cases. Under the law the Agency can be invited by a state to investigate a case, or the Centre can direct it to investigate one. However, given the nature of power-sharing, it has inevitably come into conflict with state police systems. The best example is the conflicting claims and actions of the Maharashtra state police and the NIA on the German Bakery blast case.⁶ The Burdwan blasts in 2014 in West Bengal saw similar conflicts between the state police and the NIA.⁷

The big issue in counter-terrorism is the capacity of the various states to deal with terrorism, not only in terms of intelligence, but also dealing with a terror strike, as was evident during the Mumbai attack, besides investigation and prosecution of the case. The Centre has made great efforts to deal with the issue such as the creation of SMACs though proposals for fusion centres have yet to take root. The real problem is the extremely poor capacity of state police organisations to cope with even ordinary crimes, leave alone terror strikes. A lot of states also suffer from insurgencies of varying magnitude. The inability of state and central police forces to deal with these insurgencies reflects the poor state of policing in the country.

The problem of secrecy prevents us from assessing the effectiveness of counter-terrorism or counter-insurgency activities of Indian agencies. Agencies routinely claim that they have foiled several terrorist conspiracies and many arrests do indeed take place and are reported in the media. However, the gold standard—where the prosecution can actually obtain a conviction of those arrested—had not been achieved.

China

The rise of China poses all kinds of challenges to India. The opacity of the Chinese system makes it difficult for us to fathom its capabilities and intentions. China's military capabilities have shown an

exponential growth. In the last five years, China has astonished the world with the advances it has made in aerospace and missile capabilities. Its prowess in cyber-space is considerably advanced.

India's focus on China till now was primarily on the border, gathering military intelligence with regard to the potential threat of Peoples Liberation Army (PLA) forces in Tibet and Xinjiang. But China is making inroads into the Indian Ocean Region and reports of the PLA Navy operating and visiting regions around India are becoming all too frequent. As China expands across into the Indian Ocean and establishes strong economic and arms transfer relationships in the South Asian region, the dimensions of the challenge will change. This requires a much more focussed effort—through TECHINT and HUMINT to gather intelligence on Chinese military capabilities, scientific-technical capacities, politics, trade and economics. In turn, this requires the pooling together of specialist manpower—with requisite language and technical skills—and their effective utilisation. It also requires huge investments in TECHINT and cyber capabilities.

Conclusion

The Indian experience of reform and restructuring of intelligence agencies has, till now, revealed only limited success. The reasons for this have been many. Primary among them has been the lack of political guidance for the reform process. Task forces and committees come up with recommendations for reform, but implementing them requires the process to go through the bureaucratic maze and that is where resistance often happens. To overcome this requires political attention and leadership which is attuned to the security needs of the country, as well as possessing a nuanced understanding of the ways of bureaucracy.

Both internal and external intelligence agencies continue to face critical manpower shortages. The lack of a separate intelligence cadre and the lack of language and technical specialists have blunted the effectiveness of the Indian intelligence community. Agencies in India have not been able to keep up with the technical revolution that has taken place in collecting and analysing data. Indian public sector has not been able to meet the demands of systems that can handle big data. There exists a necessity to co-opt the private sector in intelligence work to make up for the shortfall.

India has in recent years become more adept at gathering and using IMINT gathered through satellites and aircraft. The Defence Image Processing & Analysis Centre (DIPAC) has acquired the capability to transfer imagery real-time over secure networks. The recent launch of the GSAT-7 satellite for the Indian Navy was another step in the same direction. A second satellite, GSAT-7A, is already in the pipeline.

There has been, over the years, a duplication of resources and capabilities, mainly because of ineffective coordination. The R&AW and the Aviation Research Centre (ARC) both are gathering electronic intelligence on China albeit on different platforms. The NTRO is now designated as the nodal agency for technical intelligence, but it is yet to gain control of all or acquire assets for other

agencies to carry out its mandate. While there exists a necessity to create additional capabilities, duplication of assets and capabilities must be rationalised given the economic costs.

It is imperative that intelligence agencies and the armed forces develop the capacity to deal with unpredictable threats. This calls for urgent and comprehensive reform and restructuring of the intelligence apparatus. The initiative must come from the political leadership committed to secure the country's strategic interests in the face of phenomenal and often unexpected challenges.

Endnotes:

1. The National Intelligence Strategy of the United States of America, 2014, p. 2
2. Satish Chandra, "National Security System and Reform," India's National Security Annual Review 2005, p 211
3. The IB's manpower is of the order of 25,000 plus personnel, but it actually needs double that number, primarily among intelligence collectors and technical staff. R&AW has some 9,000 personnel, but only about 3 per cent of these are posted abroad. Its officer cadre is even smaller than that. The issue of manpower actually runs across the intelligence services, whether it is the JIC, DIA or the economic intelligence agencies.
4. "Boundless Informant: the NSA's secret tool to track global surveillance data," <http://www.guardian.co.uk/world/interactive/2013/jun/08/boundless-informant-nsa-full-text>.
5. Sandeep Joshi, "India gets ready to roll out cyber snooping agency," The Hindu, June 10, 2013; Reuters, "India sets up nationwide snooping programme to tap your emails, phones", June 20, 2013. A smaller system called Network Traffic Analysis or NETRA system has been around since 2009 accessing Indian cyber traffic for the IB. Praveen Swami, "Hands tied on tech, India's digital eye is half shut," Indian Express, August 11, 2014 <http://indianexpress.com/article/india/india-others/hands-tied-on-tech-indias-digital-eye-is-half-shut/99/>. The big problem Swami, however, points out, is that lack of decryption skills results in a great deal of the intercepted material remaining unused.
6. Rashmi Rajput, "Maharashtra ATS contests Delhi police claim on IM operative," The Hindu September 9, 2014 <http://www.thehindu.com/news/national/maharashtra-ats-contests-delhi-police-claim-on-indian-mujahideen-operative/article6391728.ece>; Praveen Swami, "Pressure for results skewing terror investigations?" The Hindu September 15, 2011 <http://www.thehindu.com/news/national/pressure-for-results-skewing-terror-investigations/article2456267.ece>
7. Soumen Dutta, "Burdwan Blasts: Is Bengal Police Shielding Accused," Hindustan Times October 8, 2014 <http://www.hindustantimes.com/india-news/west-bengal-police-shielding-burdwan-bombers/article1-1272828.aspx>

ABOUT THE AUTHORS

Manoj Joshi is a Distinguished Fellow at ORF.

Pushan Das is a Research Assistant with ORF's National Security Initiative.



Observer Research Foundation,
20, Rouse Avenue, New Delhi-110 002
Phone: +91-11-43520020 Fax: +91-11-43520003
www.orfonline.org email: orf@orfonline.org