ORF ISSUE BRIEF
DECEMBER 2020
ISSUE NO. 428

India's Enduring Challenge of Intelligence Reforms

VINAYAK DALMIA
VRINDA KAPOOR
SAIKAT DATTA

ABSTRACT India's attempts at strengthening its intelligence infrastructure and capabilities have historically been reactive and incremental, rather than holistic and sustainable. This was seen, for instance, in the aftermath of the Kargil War, and following the terror attacks on Mumbai in November 2008. India has rarely undertaken proactive reforms and done little to implement corrective measures subsequent to these crises. This brief offers recommendations for a concrete framework in transforming the country's intelligence capabilities, highlighting the role of technology.

Attribution: Vinayak Dalmia, Vindra Kapoor and Saikat Datta, "India's Enduring Challenge of Intelligence Reforms," *ORF Issue Brief No. 428*, December 2020, Observer Research Foundation.

INTRODUCTION

A week after 20 Indian soldiers were killed[1] in clashes with China's People's Liberation Army (PLA) in the Galwan Valley in the Ladakh sector, India banned 59 Chinese apps[2] and began a process of implementing more punitive trade measures. Indeed, the crisis that began in May 2020 in the Ladakh sector was unlike other clashes that have taken place between the Indian Army and the PLA in the past. It was more aggressive, unlike the posturings that both armies have been engaging in every year; it was more widespread, and clearly the result of months of planning. In its aftermath, India's response has raised questions about the country's intelligence capabilities.

First, since the PLA's move was months in the making, how did India's intelligence agencies miss the signs? At the very least, sub-one-metre resolution satellite imagery is easily accessible to even armchair intelligence watchers. Second, even if India's intelligence agencies were aware that the PLA was planning some kind of action after India changed the status of the erstwhile state of Jammu and Kashmir (including Ladakh) in early August 2019, was such information shared with field commanders? Third, what assessments were made by India's intelligence community and the National Security Council Secretariat (NSCS) that fed a range of response options for the government? Moreover, while the ban on the numerous Chinese apps may not be directly related to the subject, the question does emerge that if these apps indeed pose a security threat, why did India wait for a crisis to impose the ban?

Even a cursory look at any crisis reveals that India's efforts to reform its security architecture and processes have historically been reactive, cautious, piecemeal and only incremental rather than holistic. The same was seen, for instance, in the aftermath of the Kargil War with Pakistan in 1999, and following the terror attacks on Mumbai on 26 November 2008. India has rarely undertaken proactive reforms and done little to implement corrective measures subsequent to these crises.

INDIA'S INTELLIGENCE LANDSCAPE

India has various intelligence agencies, of which the Intelligence Bureau (IB) is the oldest. Created in 1887, IB reports to the Ministry of Home Affairs and is responsible for India's domestic intelligence, internal security, and counter-intelligence. First named the Indian Political Intelligence Office, it was given its current name after Independence. The Research and Analysis Wing (R&AW), meanwhile, is the country's foreign intelligence agency. Formed in 1968, it comes under the direct command of the prime minister. Legally speaking, R&AW is a wing of the Cabinet Secretariat. Established in 2004, the National Technical Research Organisation (NTRO; erstwhile National Technical Facilities Organisation), is the technical intelligence agency of the Government of India. NTRO comes under the National Security Advisor and is part of the Prime Minister's Office. There is also the Directorate of Revenue Intelligence (DRI) that is tasked with anti-smuggling intelligence; it was set up in 1957, and falls under the Ministry of Finance.

In addition to NTRO, all intelligence agencies have their own technical wing under them as well. The "norms of conduct" of the IB, R&AW and NTRO are governed by the Intelligence Organisations (Restrictions of Rights) Act, 1985. Additionally, employees of Indian intelligence agencies are subject to the Official Secrets Act (first enacted in 1923) that governs, among others, the sharing of classified information.

At the apex level, the National Security Council Secretariat (NSCS), headed by the National Security Advisor (NSA), was set up by the NDA government following the 1998 Pokhran-II nuclear tests. In 2018, the Joint Intelligence Committee (JIC), a body created to aggregate and analyse all intelligence from the various agencies, was subsumed into the NSCS.

Joint Intelligence

India's existing intelligence apparatus comprises an assortment of agencies that have specific mandates. They do, however, tend to overlap in their functions, either by design or as a natural consequence of their activities. To be sure, having multiple offices dealing with various aspects of intelligence work is not unique to India. In the United States (US), for instance, there are some 13 agencies that work in gathering and processing intelligence in some form or the other.

The creation and evolution of intelligence agencies in India is chequered, with instances of good intentions being poorly implemented, or else the original vision and intent getting lost. Much of India's challenge emanates from the fact that many of its intelligence agencies are created not as part of a deliberate strategic vision, but merely as a response to a crisis. Further, some of them were simply copied from existing models in Western countries, leading to mismatches with India's political and bureaucratic systems, resulting in below-par capabilities.

In 1968, the foreign intelligence division of the IB was hived off to create the R&AW. This was a result of two crucial lapses by the IB: its failure to make a correct assessment of China's intentions that would eventually lead to the 1962 war with India, and Pakistan's Operation Gibraltar that led to the 1965 war. These were primarily cited as the reason for needing a dedicated external intelligence agency along the lines of the American CIA and the British MI6 (Secret Intelligence Service).[3,4] However, the implementation of the vision left much to be desired. While it sought to have an open recruitment system that would eventually lead to the creation of a dedicated intelligence cadre for India, the plan failed to take off. While policymakes did not intend for the Indian Police Service (IPS) to have overarching powers over the intelligence agencies, both external and internal, such was what happened eventually.

The different branches of the military have their own intelligence wings. The Indian Army (IA), for instance, has a cadre of military intelligence officers comprising former high-ranking, intelligence officers with decades of experience in the field. The question, however, is whether this has led to significant gains for the IA's intelligence capabilities. The other two services—the Indian Air Force and the Indian Navy—also have intelligence wings, but they

do not have a cadre; instead, they field personnel on a rotational basis. The result is that these efforts remain largely tactical and focused on day-to-day operational requirements; larger issues of strategic intelligence are left largely to the civilian agencies.

Following the Kargil War of 1999, the government sanctioned the Defence Intelligence Agency (DIA) of the Integrated Defence Staff under the Ministry of Defence. However, it failed to address the strategic gaps of the military dimensions of intelligence, struggling to remain relevant with India's intelligence community. Like the creation of the R&AW, that of the NTRO was also a result of a particular crisis (i.e., the Kargil War). The failures in intelligence—whether in collection, analysis or processing—led to a recognition of the need for a dedicated technical intelligence agency modelled after the UK's Government Communications Headquarters (GCHQ) or the US National Security Agency (NSA). This led to the creation of NTFO, which later became NTRO, meant to be an agency comprising a dedicated technical intelligence cadre. This, too, fell short of the desired objectives and was soon mired in controversies, including those related to personnel policies and acquisitions.[5,6,7,8] The fact that a technical intelligence agency needed a dedicated and capable cadre was virtually ignored, leading to crucial obstacles during its formative years.

Over the years, the impact of these efforts at fortifying India's intelligence capabilities has been limited. Even at the apex level, where intelligence collation and analysis need to take place, the results have been far from desirable. Repeated failures following the reports of the Kargil Review Committee and the Group of Ministers point to a deeper and systemic failure. For instance, although there was available intelligence on possible terror attacks on Mumbai in 2008, India's intelligence agencies and networks failed to identify the threat and prevent the attacks. Therefore, an evaluation of India's intelligence capabilities can only be done by measuring the reasons for its repeated failures to reform its agencies. While incremental changes have been accepted occasionally—either the Kargil Review Committee or the Group of Ministers' report, or even the Naresh Chandra Committee—all of them failed to modernise India's intelligence apparatus.

A HISTORY OF MISSED REFORMS

The Kargil Review Committee (KRC) was set up by the Government of India on 29 July 1999, three days after the end of the Kargil War. The Committee found serious deficiencies at various levels of intelligence collection. It noted, for instance, thus: "There is no institutionalized mechanism for coordination or objective-oriented interaction between agencies and consumers at different levels. Similarly, there is no mechanism for tasking the agencies, monitoring their performance and reviewing their records to evaluate their quality. Nor is there any oversight of the overall functioning of the agencies." Two decades later, it is apparent that little has changed since the KRC's observations in 2000. India remained unable to detect, let alone prevent the PLA's build up in Ladakh in 2020.

Owing to the weaknesses in India's security establishment, the country has failed to marshal its Comprehensive National Power (CNP). To begin with, the public is unable to even see the entire picture of India's past military crises. Most of the KRC report on the Kargil War, for instance, is redacted and its substantive parts have never been released to the public. Chapter III, in particular, which delves into the Intelligence Apparatus, remains classified. Similarly, the report of the Naresh Chandra Task Force on National Security, constituted by the then UPA government in 2012, have still not been made public even after a succession of governments.

Contrast India's landscape with that of the United States, for example. Following 9/11, a 10-member commission created to investigate the attacks released the 9/11 Commission Report.[9] Originally, the final section of the report (titled "The 28 pages") was classified. However, in 2016, the Obama Administration approved the declassification of the section, albeit in a partially redacted form.

Not only is India's intelligence processes moribund, they have also failed to grapple with the impacts of internet-based technologies that are fundamentally altering how the world currently works. India's lack of a credible technology and security industry leaves gaping holes in its ability to manoeuvre modern-day security challenges.

THE AGE OF TECHNOLOGY

Technology has always mattered[10] in building strong nations, in particular, sophisticated militaries and intelligence agencies. In recent years, the relevance of technology has come to the centrestage, amidst the Cold Tech war[11] between the US and China. The imperative is for India to nurture a national intelligence strategy for this technology era. In 2019, what is now known as the Pegasus malware attack managed to breach the WhatsApp communication platform's end-to-end encryption protocol across several countries. The incident brought out in the open another set of questions[12] regarding India's intelligence capabilities. By relying on foreign vendors and third-system integrators, India could be compromising and diluting its national security.

India would do well to have its "Make in India" initiative reach the country's intelligence agencies. This brief is not suggesting for India to unlawfully spy on its own citizens. The challenge is for India to finally muster a vision for the development of its indigenous capability.

Vannevar Bush, the first scientific adviser to a US president, wrote in his 1945 magnum opus report, *Science: The Endless Frontier—an*[13]—-"new frontiers of the mind" were essential "to our security as a nation, to our better health, to more jobs, to a higher standard of living, and to our cultural progress." There always has been an intimate relationship between technology and intelligence work. While "HUMINT" (human component) will continue to be a crucial component of the job, continuous technological advancements[14] have led to sophisticated forms of "SIGINT" (signal intelligence). As a *Foreign Policy* report[15] summarises: "the most crucial element of the technological storm engulfing intelligence agencies is the mobile phone."

Modern SIGINT traces its origins to the Russian-Japanese wars of the early 1900s, with further advancements in interception and code-breaking during the two World Wars. The Cold War also pushed the boundaries with two great rivals battling for global domination. Yet, 9/11 might be the real watershed moment. In its aftermath, the surveillance industry went through radical changes, spending billions of dollars every year to procure new technologies and gear.

It is here where India is terribly lagging. According to the 2019 Council on Foreign Relations Task Force on Innovation and National Security:[16] "..the intelligence community will fall behind potential adversaries if they do not rapidly access and deploy technologies developed in the private sector." Consider these statistics: India was the largest buyer of arms from Israel in 2017, with purchases worth US$715 million; nearly 9 percent of India's defence imports was Israeli between the years 2009-18. Not to mention that majority of the technology in this sector is imported into India; the country imports disproportionate volumes of intelligence tech and gear from countries such as Israel. The foreign original equipment manufacturer (OEM) lobby in India is notorious and will not cede space so easily.

On intelligence technologies, India's domestic capability is sorely missing. The country is almost exclusively dependent on foreign imports from countries such as Israel and the US. With the increasing commercialisation and privatisation of espionage, technology providers are going to be the biggest beneficiaries. If India continues to lag, it will lack the smart power it so desires. It is also less likely to have an influence in how new technologies are deployed and regulated around the world. Indeed, cutting-edge technology companies in the defence and intelligence sectors have become the modern-day equivalent of the East India Company—able to create dependencies and diminish strategic agency.

A robust base in technology and innovation can strengthen national security, which in turn bolsters the economy. This intimate cycle is best witnessed in the US which has been an economic and security powerhouse since the Second World War owing to its investments in science, and Research and Development (R&D). The same can be seen with Israel, which has built a global reputation and significant exports on the back of its security and surveillance-based deep technologies. China is fast catching up, and by 2030 is poised to be the world's biggest R&D spender with a significant portion going to intelligence and national security-based applications.

RECOMMENDATIONS

India needs a national security innovation strategy based on three pillars of reform: people, *paisa* (money), and processes. Such a framework will need a tripartite partnership between government, private sector (including young companies and non-traditional suppliers), and the academia. Best practices from other countries have shown how much of innovation emerges from regional ecosystems made up of networks of technology firms, capital markets, and research institutions.

The first step is to identify specific technology pathways and create a concrete

five-year plan to swiftly build local capacity. This entails a targeted approach that encourages accountability, as opposed to a diffused one.[17] All efforts must converge within the stipulated period and towards a common goal: building Indian capability in a set of technologies that will serve the intelligence community.

To identify the areas of technology that intelligence agencies should focus on, one can learn from others such as the Five Eyes or the Chinese,[18] both of whom have the same goals. These examples illustrate the fundamental principle that any intelligence work is done using two basic senses: of seeing and of hearing. The technology needs will be shaped around these senses, to both detect threats as well as deceive adversaries. For example, it is essential to build local capabilities in cyber-offense and interception of satellite calls.

Richard Aldrich's book, 'GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency'[19] reveals how other intelligence agencies have developed their technology capabilities, from satellite call interception by aircraft flying overhead the city of Birmingham, to call-spoofing to confuse eavesdroppers. The agency completes 100 years[20] in operations in 2020 and is in the midst of a revamp.

The second step is to unleash a host of policy levers that will converge in the same singular goal. Some of these policies will be designed for short-term reforms, and others for longer-term structural changes. If India is keen to develop a technology base to further its intelligence capabilities, it needs to nurture a culture of technology and innovation. This goal has the following elements:

1. **Government as investor.** It is time for India's intelligence agencies to act as venture capitalists and take ownership in the companies they will nurture and support. For example, In-Q-Tel is the CIA's venture arm, and has been investing in young companies since 1999. The US NSA has also experimented with the same. More recently, the famed Israeli spy agency, Mossad, has launched an incubator, inviting applications from all over the world (in select technology areas).

2. **Rapid experimentation.** It is important to better leverage existing funding platforms such as the recently launched "Innovations for Defence Excellence" (IDEX[21]) (to fund innovative ideas and startups) of the Ministry of Defence.

3. **Create a Future Technologies Unit.** This is a multi-agency federal body representing the future technology needs of the main intelligence agencies at the national level. One percent of the budget from each agency should be channeled to this office for fast technology development and integration.

4. **Establish a Digital Academy.** This could train serving intelligence officers in the chosen technology domains.

5. **Technology Fellows Programmes.** A lateral entry program of a few years can be offered to domain experts who work closely with intelligence agencies. This is one way to attract young technical talent. The CIA and FBI ran the Cybersecurity

Talent initiative which included two-year placements. Similarly, in the UK, the GCHQ has started a cyber programme for high school students.

6. **An R&D charter for the intelligence community.** One cannot expect the current operations and procurement teams to also focus on R&D. A separate parallel team has to be created, capable of risk-taking and experimentation, that will work closely with the operations team.

7. **INT R&D lab / Science Park.** Create an R&D lab focused on SIGINT within a leading engineering university.

8. **Create international alliances.** These collaborations will focus on development exercises akin, for example, to the Indian armed forces' collaboration with the US under the DTTI charter.

9. **Create a dedicated unit on Open Source Intelligence (OSINT)[22,23] to collect and analyse the vast volumes of data that are now publicly available in the open domain.** Commercial sensors and the internet have made this possible and it can often prove to be a treasure trove for intelligence operations.

10. **Shift the status quo by creating a healthy competition between the private sector and the DPSUs / DRDO.** A challenger from the outside could create better results than what is being seen from the current near-monopoly of public-sector units.

11. **For India to build an industrial base**, it needs a clear method of security clearances similar to those of the US and UK, and even of the North Atlantic Treaty Organization (NATO) for private citizens. Otherwise, the industry side will fail to find solutions to problems that they do not completely understand.

12. **Greater participation of the private sector in technology assessment.** The US, for example, routinely seeks the assistance of the private sector in assessing technology. The large defence contractor, Booz Allen Hamilton, helps the government evaluate new technology and obtain pricing for their development. This proves important even for framing of Request for Information (RFI) / Request for Proposal (RFP).

13. **A separate budget for R&D exclusively for the Indian private sector.** With the large procurement orders create a "small business set aside" (instead of offsets). This will compel large foreign original equipment manufacturers (OEMs) to bring along Indian Small & Medium Enterprises (SME) / startups, without which they cannot bid on tenders.

CONCLUSION

India's national security challenges make it imperative for the country to develop a technology-centric intelligence cadre, and nurture this cadre's capabilities. Substantial reforms are needed to improve the collection, processing and dissemination of intelligence on a real-time basis. A prerequisite is to pass specific legislation that would give India's intelligence community a statutory basis and a charter, and provide it with institutional levels of accountability.

India inherited its intelligence structures from its British colonisers. The UK has moved on to creating a similar sound legislative basis and charter for its intelligence agencies, while also ensuring that they are technologically advanced and accountable to its citizens through Parliament. In the US, the CIA and its sister agencies were created through Acts passed by Congress and has seen periodic reforms, including in the aftermath of the Watergate scandal, or the failures to detect the Indian nuclear tests of 1998, and the attacks on the twin towers in New York on 11 September 2001 by the *al Qaeda*.

The Sputnik satellite launch by the Soviets on 4 October 1957 catalysed the US to invest heavily in R&D for its intelligence and security community. As a result, for three-quarters of a century the world has witnessed unparalleled American hegemony in the field of science and technology. India is facing massive challenges in filling the gaps in its intelligence systems; will the intrusions in Ladakh serve as India's Sputnik? ORF

ABOUT THE AUTHORS

Vinayak Dalmia is an entrepreneur and national security and foreign affairs analyst. **Vrinda Kapoor** is a deep technology entrepreneur who runs a Data Analytics Company. **Saikat Datta** is a Strategic Advisor at *The Dialogue* and NullCon, and is former South Asia Editor for *Asia Times*.

ENDNOTES

1 "India-China clash: 20 Indian troops killed in Ladakh fighting," *BBC News*, June 16, 2020, https://www.bbc.com/news/world-asia-53061476

2 Shruti Srivastava and Bibhudatta Pradhan,"After Banning Chinese Apps, India's New Trade Barriers With China", *NDTV*, July 24, 2020, https://www.ndtv.com/india-news/india-builds-new-trade-barriers-with-china-amid-border-row-2268160

3 Jayshree Bajoria, "RAW: India's External Intelligence Agency", Council on Foreign Relations, November 7, 2020, https://www.cfr.org/backgrounder/raw-indias-external-intelligence-agency

4 Srinath Raghavan,"After 50 years of RAW, there are still no declassified documents or an official history", *The Print*, September 18, 2018, https://theprint.in/opinion/why-was-raw-formed-and-what-has-india-learnt-after-50-years-of-its-existence/119811/

5 "Scams galore in nation's top intelligence outfit", *New Indian Express*, April 22, 2012, https://www.newindianexpress.com/thesundaystandard/2012/apr/22/scams-galore-in-nations-top-intelligence-outfit-360870.html

6 "Make public details of probe in corruption charges in RAW: CIC", *Times of India*, January 13 2011, https://timesofindia.indiatimes.com/india/Make-public-details-of-probe-in-corruption-charges-in-RAW-CIC/articleshow/7276527.cms

7 Saikat Datta, "Double Checking", *Outlook*, January 28, 2008, https://magazine.outlookindia.com/story/double-checking/236599"

8 Saikat Datta, "Inside, RAW", *Outlook*, July 02, 2007, https://magazine.outlookindia.com/story/inside-raw/235003

9 Steve Blank, "The Secret History of Silicon Valley", November 20, 2008, https://www.youtube.com/watch?v=ZTC_RxWN_xo

10 Adam Segal, "The Coming Tech Cold War With China", *Foreign Affairs*, September 09, 2020, https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china

11 Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms", *Foreign Affairs*, May/ June 2019, https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms

12 Vinayak Dalmia, "The rise of Pegasus and why India should know the problem with hiring 'internet mercenaries'", *The Print*, November 01, 2019, https://theprint.in/opinion/rise-of-pegasus-india-must-know-problem-with-hiring-internet-mercenaries/314457/

13 Vannevar Bush, "Science The Endless Frontier", A Report to the President, by Director of the Office of Scientific Research and Development, July 1945, https://www.nsf.gov/od/lpa/nsf50/vbush1945.htm

14 Edward Lucas, "The Spycraft Revolution", *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/

15 James Manyika, William H. McRaven and Adam Segal, "Innovation and National Security", Independent Task Force Report No. 77, Council on Foreign Relations, 2019, https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf

16 Harsh V. Pant and Ambuj Sahu, "Israel's arms sales to India: Bedrock of a strategic partnership", ORF Issue Brief No. 311, September 2019, https://www.orfonline.org/wp-content/uploads/2019/09/ORF_Issue_Brief_311_India-Israel.pdf

17 Yuki Okoshi, "China's research papers lead the world in cutting-edge tech", *Nikkei Asia*, January 06, 2019, https://asia.nikkei.com/Business/China-tech/China-s-research-papers-lead-the-world-in-cutting-edge-tech

18 Richard Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency (HarperCollins Publishers UK, 2011)

19 "GCHQ Looks Toward 'Unique Challenges' On Centenary", *Forces Net*, November 01, 2019, https://www.forces.net/news/gchq-looks-toward-unique-challenges-centenary

20 https://idex.gov.in

21 "NATO Open Source Intelligence Reader", February 2002, http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf

22 https://www.bellingcat.com/tag/satellite-imagery/

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