A Case for Intelligence Reforms in India

IDSA Task Force Report

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES

A Case for Intelligence Reforms in India

IDSA Task Force Report

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES

ISBN: 978-93-82169-03-1

Disclaimer: The views expressed in this Report are of the Task Force members and do not necessarily reflect those of the Institute and the Government of India.

First Published: 2012

Price: Rs. 250/-

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

Layout & Cover by: Geeta Kumari

Printed at: M/s Printline
H-10, IInd floor, NDSE-I
New Delhi - 110049
Tel: (91-11) 24651060, 24643119
Email: printline2003@yahoo.co.in

Contents

Foreword

The unprecedented attack on Mumbai -on 26.11.2008 focused attention on the complex security challenges facing India, which have the potential to derail its economic and social progress. In the aftermath of that incident, the functioning of India's security and intelligence set-up and its ability to meet the new emerging challenges was extensively discussed in various circles. Even earlier, after the Kargil intrusions in 1999, the issue of intelligence lapses had been examined in depth and several recommendations made by the Task Force set up by the Group of Ministers were implemented. Nevertheless, doubts persist about the adequacy of intelligence mechanisms and the somewhat piecemeal or ad hoc nature of reforms being implemented. Besides, no less a person than the Vice President of India, Shri M. Hamid Ansari has also spoken about the need for the accountability of intelligence agencies and the necessity for them to function under some sort of legal cover.

The Institute for Defence Studies and Analyses (IDSA), on its part, has tried to look at the problem in somewhat broader terms and study the functioning of country's intelligence set-up; analyse the factors that impede good intelligence at various stages of collection, initial analysis, inter-agency cooperation and assessments and what can be done to improve assessments and human resources. It has also tried to examine the related issue of the necessity for the regular and periodic briefings of the political executive after they receive the intelligence inputs in a processed form.

A Task Force, consisting of S/Shri R. Banerji, Special Secretary (Retd.) in the Cabinet Secretariat, P. K. Upadhyay, (Consultant, IDSA), Harinder Singh (then Research Fellow, IDSA), have brought out the present report. It was assisted by Brig (Retd.) Rumel Dahiya, (presently the Deputy Director General, IDSA), Raj Shukla (then Research Fellow, IDSA), Alok R. Mukhopadhyay, and other experts. Colleagues from the diplomatic service provided some inputs on the interface between the intelligence agencies and the Ministry of External Affairs.

We were also fortunate to have the benefit of the advice from noted experts in the field, who participated in a round table discussion at IDSA in August 2010. These included the veteran security analyst (late) Shri K. Subrahmanyam, former National Security Adviser, Shri Brajesh Mishra, former intelligence professionals - Shri G.C. Saxena, Shri A.K. Verma, Shri Ajit Doval and experienced police and military officers like Shri Ved Marwah and Lt Gen (Retd) R. Sawhney.

The project also benefited from the advice provided by some other intelligence professionals like: Shri Kalyan Mitra, former Director General Security; Shri D. C. Nath, former Special Director, Intelligence Bureau; noted terrorism expert, Shri B.Raman; Shri K.

Santhanam, former Chief Adviser, Technology to the Government of India and ex-DG, IDSA; and Shri V. Balachandran, former Special Secretary, Cabinet Secretariat and co-author of the Pradhan Committee report on the Mumbai 26/11 lapses.

A report based on these consultations and discussions, stretching over a year-long period was drafted by Shri R. Banerji. Besides, the former Director General of the IDSA Shri N.S Sisodia not only provided valuable inputs, suggestions and directions from time to time, but also extensively vetted the report, which was finally given its present shape by Shri P.K. Upadhyay.

The key recommendations made by the Task Force in the report are: The intelligence agencies in India must be provided a legal-framework for their existence and functioning; their functioning must be under Parliamentary oversight and scrutiny; and extensive reforms must be carried out in the recruitment and training processes of their personnel, their pay structures and career progression to attract the best talent available in the country. It is only then that the Indian intelligence agencies would be able to meet the myriad challenges the country faces in the new millennium.

We believe that this report, which relies on inputs in public domain and does not reflect the views of either the Government of India, or the IDSA, will nonetheless promote an informed discussion on key issues affecting our intelligence set up and hopefully, set in motion the process for further reforms.

Arvind Gupta
Director General, IDSA

New Delhi

Executive Summary of Recommendations

Towards Reforms in the country's intelligence apparatus

- The paradigm shift in the nature of the security challenges facing the country lends urgency to the need for reforms in country's intelligence apparatus;
- There is a need for comprehensive, not adhoc and piecemeal, reforms;
- The focus of this exercise should be on removing the deficiencies within the system, improving coordination between intelligence agencies and ensuring better accountability and oversight.

Legal Status

- Introduce legislation in Parliament for laying down the charters, functions and duties of intelligence organisations;
- Provide a legal basis for different tiers of accountability – executive, financial and legislative;

Recruitment, Deputation, Promotion, Training

- Have open and separate direct recruitment mechanisms for different intelligence agencies - advertising for the best talent available, specifying the qualifications required, including linguistic abilities – by using the existing mechanism of the Union Public Service Commission;
- Use deputation slots to induct experts from the military and science & technology streams;
- Outsource to meet specialised needs;
- Improve training modules, including specialised training for analysts;
- Improve quality of trainers, bring in military trainers;
- Review the present system of writing Annual Confidential Reports (ACR) in intelligence agencies to eliminate subjectivity and bring about better objectivity;
- Review *in situ* promotions to improve morale at middle, mid-senior levels.

Analysis & Operations

- Improve training for analysts in tools of modern prescriptive work;
- Improve quality of supervision in operational branches of intelligence agencies, reverse drift in operational work, discard useless and profligate sources;
- Bring better financial probity in intelligence operations;
- Introduce concept of social welfare safeguards for assets who rendered valuable service for national security, but became casualties on the job.

Technology Upgrade

- Enhance in-house technical research and development capabilities- especially in relation to signals decryption work, and cryptography capabilities;
- Examine feasibility of outsourcing relevant tasks to experts for improving output;
- Fast track equipment procurement processes, with innovative association of financial experts at suitably high levels, so that balance is maintained between time frames and norms of financial propriety;
- Upgrade Open Source Intelligence (OSINT) capabilities; Use advanced commercial search engines;
- Upgrade offensive as well as defensive capabilities in cyber warfare.

Relations between Intelligence agencies & Ministry of External Affairs

- Introduce a system of inter-changeability between various intelligence agencies and the connected Ministries of the Government of India;
- In case of external intelligence, institutionalise cover assignments in consultation with Ministry of External Affairs to improve cooperation;
- Have regular inter-action between heads of intelligence agencies and Secretaries of the concerned Ministries, as also between their area desk officers;
- Resume the practice of posting a Joint Secretary level Foreign Service officer in external intelligence – for better coordination and liaison.

Coordination of Intelligence

- Appoint a National Intelligence Coordinator/Director of National Intelligence to bring about better inter-agency coordination, remove overlaps and duplications, end 'turf-wars' and ensure better utilisation of national resources. Alternatively, the National Security Adviser (NSA) may function independently under a Minister for National Security.

Accountability

- Strengthen financial accountability of intelligence agencies; annual reports to go to Comptroller & Auditor General (CAG)/NSA;
- Provide for an in camera audit of Secret Service Funds;
- Have a separate intelligence ombudsman for IB, R&AW & NTRO;
- Enhance staff support by posting intelligence professionals in external processing units serving the Cabinet Secretariat (for R&AW and NTRO) and MHA(for IB);
- Examine the option of having a Minister for National Security & Intelligence, who could exercise administrative authority on all intelligence agencies;
- Set up a Parliamentary Accountability Committee for oversight of intelligence

agencies through legislation;

- Provide adequate professional secretarial assistance to the oversight committee through the Intelligence Ombudsman and a professionally staffed unit in the Cabinet Secretariat;

Decision Points

- Whether line departments – Department of Atomic Energy, BARC, ISRO, DRI, the Economic Offences Wing, Department of Science & Technology etc - should have their own intelligence wings or appoint intelligence liaison or nodal officers to interact on regular basis with main intelligence agencies?
- Whether analysis and operations work should be completely separated in intelligence agencies and whether a Joint-Tactical Analysis Centre (J-TAC), on the UK model) should be established?
- Whether strategic military intelligence should be taken out of the charter of external intelligence and handed over to the Defence Intelligence Agency?
- To what extent should Heads of Mission of Indian legations abroad be kept in the broad loop of the operational initiatives of intelligence agencies? Should separate parameters or yardsticks be followed in neighbouring countries?
- What option of legislative accountability is to be chosen? Whether to have a separate Minister for National Security, answerable to the Prime Minister and Parliament, and/or to have a statutorily constituted Parliamentary Accountability Committee for oversight of intelligence agencies?
- What should be the boundaries of intrusive inspection and accountability of intelligence agencies on invasion of privacy or human rights violations under the Right To Information (RTI) Act? Should this be confined to personnel and administrative/ disciplinary matters only? Should the safeguard of the prior exhaustion of the Ombudsman process be prescribed before RTI can be invoked in respect of intelligence agencies?

ABBREVIATIONS

A

ACR	-	Annual Confidential Report
ACIO	-	Assistant Central Intelligence Officer
AEC	-	Atomic Energy Commission (India)
AIVD	-	General Intelligence & Security Service (Holland)

B

BND	-	Federal Intelligence Agency (Germany)

C

CAG	-	Comptroller & Auditor General
CCS	-	Cabinet Committee on Security (India)
CDS	-	Chief of Defence Staff
CEIB	-	Central Economic Intelligence Bureau (India)
CI	-	Counter Intelligence
CIA	-	Central Intelligence Agency (USA)
CID	-	Criminal Intelligence Department
COMINT	-	Communication Intelligence
CSIS	-	Canadian Security Intelligence Service
CYBERINT	-	Cyber Intelligence

D

DCI	-	Director Central Intelligence (USA)
DGS	-	Directorate General of Security
DGMI	-	Director General of Military Intelligence (India)
DIA	-	Defence Intelligence Agency (India)
DIA	-	Defence Intelligence Agency (USA)

DLB	-	Dead Letter Box (commonly called a "Drop Box')
DNI	-	Director of National Intelligence (USA)
DNS	-	Department of Nuclear Safety (USA)
DRI	-	Department of Revenue Intelligence
DRDO	-	Defence Research & Development Organisation
E		
ECOINT	-	Economic Intelligence
EIC	-	Economic Intelligence Council (India)
ELINT	-	Electronic Intelligence
ECHR	-	European Court of Human Rights
EOW	-	Economic Offences Wing (India)
F		
FICCI	-	Federation of Indian Chambers of Commerce & Industry
FIS	-	Foreign Intelligence Service (Russian)
G		
GoM	-	Group of Ministers (India)
GCHQ	-	Government Communications Headquarters (UK)
H		
HuJI	-	Harkat-ul Jihad-e-Islami
HUMINT	-	Human Intelligence
I		
IB	-	Intelligence Bureau (India)
ICG	-	Intelligence Coordination Group
IED	-	Improvised Explosive Device
IIF	-	International Islamic Front
IMINT	-	Image Intelligence
IPKF	-	Indian Peace Keeping Force
IPS	-	Indian Police Service
ISRO	-	Indian Space Research Organisation

J

JIC	-	Joint Intelligence Committee (In India, UK and USA)
JTAC	-	Joint Terrorism Analysis Centre (UK)
JUP	-	Jamiat-ul Ulema-e-Pakistan

K

KRC	-	Kargil Review Committee

L

LTTE	-	Liberation Tigers of Tamil Elam

M

MAC	-	Multi Agency Centre (Central, India) (State units known as SMACs - State Multi Agency Centres)
MASINT	-	Measurement & Signature Intelligence
MCI	-	Ministerial Committee on Intelligence (UK)
MI-5	-	Directorate of Military Intelligence, Section V (UK - Now Known as Security Service)
MI-6	-	Directorate of Military Intelligence, Section VI (UK - Now known as Security Intelligence Service)
MIVD	-	Defence Intelligence & Security Service (Holland)

N

NCTC	-	National Counter Terrorism Centre
NIA	-	National Intelligence Agency (South Africa)
NIB	-	National Intelligence Board (India)
NIB	-	National Intelligence Bureau (Sri Lanka)
NIC	-	National Intelligence Council (US)
NGA	-	National Geographical Intelligence Agency (US)
NSA	-	National Security Agency (US)
NRO	-	National Reconnaissance Organisation (US)
NSC	-	National Security Council (US)
NSC	-	National Security Council (India)
NTRO	-	National Technical Research Organisation

O

OFC	-	Operation Forces Command (Indian Army)
OSINT	-	Open Source Information
ORBAT	-	Order of Battle
OSS	-	Office of Strategic Services (WW-II ancestor of CIA of USA)

P

POLINT	-	Political Intelligence
PSIA	-	Public Security Intelligence Agency (Japan)

R

RAS	-	Research & Analysis Service
RCMP	-	Royal Canadian Mounted Police
R&AW	-	Research & Analysis Wing

S

SANDF	-	South African National Defence Forces
SASS	-	South African Secret Service (External)
SB	-	Special Branch (In state police set-up in India)
SIGINT	-	Signal Intelligence
SIS	-	Secret Intelligence Service (UK -Erstwhile MI-6)
SPG	-	Special Protection Group
SS	-	Security Service (UK-Erstwhile MI-5)
SSB	-	Special Service Bureau (India)
SSF	-	Secret Service Fund

T

TACINT	-	Tactical Intelligence
TCG	-	Technical Coordination Group (India)
TECHINT	-	Technical Intelligence

U

UP	-	United Press (London)
UPSC	-	Union Public Service Commission

W

WMD	-	Weapons of Mass Destruction

Chapter 1

The Rationale For Intelligence Reforms

The need for reforms in the Indian intelligence set-up does not spring from any desire to ape the West, but from the fact that notwithstanding numerous failures so far, there does not seem to have been any broad-based exercise to reform the country's intelligence apparatus and make it more pro-active and in harmony with the pursuit of nation's internal and external policies. Whatever piecemeal restructuring that has been tinkered with from time to time, has mostly been crisis-driven and not a comprehensive need-based attempt to address the basic and structural flaws in the Indian intelligence set-up that appear to be a legacy of its origin as a branch of policing of the society. The Indian intelligence system did not evolve out of any detailed and well thought out administrative policy, but emerged as an extension of the Indian police system due to a need driven colonial decision making process, designed to meet the requirements of maintaining law and order and internal security. Its primary duty was to keep a check on the nascent ideas of modern Indian nationalism and counter them through police methods that were considered most effective and adequate.

According to Shri M. Hamid Ansari, the Vice President of India, "While intelligence information is at times incomplete, good intelligence often has made the difference between victory and defeat, life and death. By the same token, faulty intelligence leads to failures of varying degrees".[1] Despite some success stories, the Indian intelligence agencies appear to have failed on numerous occasions to perform by producing meaningful actionable and timely internal and external intelligence to safeguard national security and interests. The Bangladesh operations, the advance information given to Indian Air Force regarding Pakistani plans to launch a pre-emptive air-strike on Indian bases on or before December 3, 1971, the unearthing of plans by many modules of terror groups to hit at Indian interests both inside and outside the country, are some of the major successes of the Indian intelligence community. Yet, these have mostly been like flashes in the pan and not reflective of the general levels of performances. Even in those cases, where Indian intelligence apparatus has succeeded in busting terror and espionage rings, it has not been able to provide accurate information which could be developed into concrete evidence

[1] Kao Memorial Lecture by Vice President Shri Hamid Ansari, Jan 19, 2010.

able to stand judicial scrutiny (as was the case with MI-5's unearthing of the plot to blow-up trans-Atlantic flights over American cities).

Some of the major failures of Indian intelligence over the years have been:

1. Almost total ignorance about Chinese intentions and capabilities in Tibet and their designs against India in the 50s. (A case in point is the non-use of Indian Air Force to bomb Chinese positions on Indian side of the border during the 1962 Sino-Indian War, because of the fear that it could lead to Chinese retaliatory air raids against Indian cities in North India. This was a major intelligence failure since the PLA Air Force did not have large bases or aircraft in Tibet at that time, having the capability to launch raids across the Himalayas, bomb Indian cities and return to their bases);
2. Failure to assess the extent of popular alienation Centre's policies were creating in Kashmir through repeated changes in state governments since the early 1950s and, more specifically, during 1986-87;
3. Failure to predict Pakistani plans to infiltrate military personnel disguised as civilians into J&K in 1965;
4. Total ignorance about Pak plans to attack Chhamb in the 1965 war and the existence of an additional armoured division in the Pakistani Army;
5. The extent of the growing unpopularity of Sheikh Mujib government in the Bangladeshi armed forces and the plans for his ouster;
6. Pakistan's decision to initiate its nuclear programme in 1972 (The Multan conclave of Z.A. Bhutto, Pakistani physicists and nuclear scientists);
7. The extent of popular support enjoyed by movements like those for a separate Telangana state, or the growth of left-wing extremism in the post-Naxalbari phase;
8. The Samba spy scandal;
9. Pakistani plans to subvert Kashmiri Muslims in the name of religion in the 70s. Pro-Deobandi/Wahabi proselytising activities in the Valley in the mid-80s and recruitment of Kashmiri youth for arms training in Pakistan and their infiltration back into the Valley with arms to launch the 'Kashmiri Jehad' in late 80s;
10. The developing situation in the North-east from the early 80s; Links between Phizo and the ISI;
11. The growth of Sikh-separatist sentiments in the early 80s and, more specifically, the volume of the arsenal stockpiled inside the Golden Temple complex before 'Operation Blue Star';
12. LTTE's reaction to Indian peace making efforts in Sri Lanka and the extent to which its armed capabilities had grown to target Indian interests;
13. Kargil incursions; involvement of Pakistan Army regulars from Northern Light Infantry (NLI) in infiltrating deep into Indian territory, and construction of fortified 'sangars';
14. Various terrorist attacks in India either directly by Pakistani players, or their Indian proxies, specially the Mumbai

attack of 26/11 and those in New Delhi before that.

There are instances of intelligence failures of such magnitude in the developed world also. However, they have all been thoroughly enquired into, responsibilities fixed and remedial measures taken. However, this has not happened in India and the public impression persists that on most occasions the dirt was merely pushed under the carpet. After the Sino-Indian war of 1962, a review of performance of the Intelligence Bureau (IB) led to the creation of the Directorate General of Security (DGS). The Indo-Pak War of 1965 and the Mizo revolt in 1966, lead to the responsibility for external intelligence collection being taken away from IB and assigned to the newly created Research & Analysis Wing (R&AW). After the Kargil operations in 1999, an enquiry by Kargil Review Committee lead to the setting up of the G.C. Saxena Special Task Force which recommended the creation of the Defence Intelligence Agency (DIA) as the nodal point for processing all military related intelligence. The National Technical Research Organisation (NTRO) was also created to collect technical and communications intelligence. In June 2009, the Pradhan-Haldar-Narsimhan task force in the National Security Council (NSC) made suggestions for improving intelligence organisations in India. The Federation of Indian Chamber of Commerce and Industry (FICCI) also came out with a task force report on National Security and Terrorism (Rajeev Chandrasekhar report – Vol. 1, 2009), which made several suggestions for strengthening intelligence collection efforts and national security management.

However, most of these reports were crisis-driven reviews,[2] retrospective in nature, rather than need-based broad perspective plans to reform and revamp. They looked into what went wrong, examined particular lapses and suggested ways and means to prevent their recurrence. More often than not their suggestions were for setting up new agencies to plug the gaps, such as the one being presently discussed for setting up a National Counter-Terrorism Centre (NCTC); a new Maritime Intelligence and Coastal Security Centre; or a new Centre for Nuclear and Missile Intelligence, without clearly spelling out the ways and means to prevent overlaps or turf-wars. This persistent failure is, perhaps, significantly responsible for the tussle between the newly created NTRO and the Aviation Research Centre (ARC) over the use and bifurcation of expensive valuable assets and facilities. There is clearly a growing perception in the media and amongst an ever-widening spectrum of intellectuals and academics engaged in the study of national security related issues that a rigid and stodgy bureaucracy may have stood in the way of developing or enhancing the desired core competence in the field of intelligence operations and analysis. According to a leading intelligence expert, Indian intelligence set-

[2] B. Raman : Dimensions of Intelligence Operations: Maj. Gen. Sinha lecture at USI, New Delhi,26.4.2004;

up is like an aircraft that can fly at a maximum height of only 10,000 feet. If the nation has a need for an aircraft to go up to the height of 15,000 feet, no amount of overhaul and up-gradation of the old aircraft's systems would make it attain that height. There would be no alternative then but to develop an entirely new technology and have an aircraft that can go up to 15,000 feet and beyond.[3]

However, apart from the natural inclination not to risk or gamble, three factors seem to have conspired against the adoption of an imaginative and unconventional approach to equip and improve capacities of the intelligence agencies to meet new threats, commensurate with India's emerging responsibilities as a global power:

i) Conflicting motivations of those considering reforms;

ii) Environmental challenges at initiation of reform; and

iii) Failure of leadership.

Understanding these factors and seeing where gains have been made despite handicaps may lead to the realisation that real change may still occur, but only if difficult choices are made while opportunities exist.[4] Any quest for meaningful reform in the intelligence machinery would necessarily bring up issues uncomfortable to the intelligence establishment in the country, such as, whether intelligence should remain the preserve of the police; whether recruitment and lateral intake policies should not be adopted to take advantage of the available immense cross–cultural talent in the form of political analysts, legal experts, linguists, financial wizards, social scientists, journalists and domain specialists, who could be roped in to provide valued inputs based on the acuity, ingenuity and contextualised insights of their own experience and wisdom .

A broad consensus that is apparently shared by a wide section of Indian intelligence professionals presently, underlines the need for the following:

i) A focus on "improvement of capabilities, or removal of deficiencies, within the agencies themselves, whether in terms of manpower or quality of assessments";

ii) "Co-ordination amongst various agencies- there must be someone who knows everything that is happening and who can go and report to the Prime Minister frequently", i.e. a "Minister for National Intelligence";

iii) "Thirdly, how do you manage Parliamentary oversight?"[5]

---

[3] Views of Shri A. K. Verma expressed in the round table at IDSA on August 6, 2010

[4] Patrick C Neary, *Intelligence Reforms*', *Studies in Intelligence, Vol*. 54, No. 1 (Extracts, March 2010

[5] The consensus view of intelligence experts expressed in the IDSA Round Table, August 2010. Brajesh Mishra ,former National Security Adviser & Principal Secretary to PM, strongly underlined the need for a "Minister for National Intelligence".

Shri M. Hamid Ansari has expressed concern about the nature and extent of supervision over intelligence agencies by the political executive and the possibility and scope of misuse of these agencies by that authority. He has also highlighted the issue of accountability and oversight as these measures were being undertaken in various modern intelligence organisations.[6] Clearly, the time has come for the political executive to confront these issues head on and not skirt around them.

[6] M. Hamid Ansari: Kao Memorial lecture, R&AW: Jan 19, 2010;

Chapter 2

New challenges of national security management

The five components of national security management presently relate to diplomacy, economy, military, internal security, and intelligence. In the US, the Hoover Commission report of 1953 defined intelligence as the collection, collation, analysis and assessment of information pertaining to national security or having a bearing on formulation of national strategies. Intelligence services the world over have faced difficulties in meeting these tasks due to the constant emergence of newer conventional and non-conventional threats to security. Conventional threats are defined as "offensive armed postures by hostile powers, subversion, nuclear, biological and chemical threats, as also terrorism" while, "non-conventional threats could extend to include migration, epidemics, natural disasters, human trafficking, trans-national crimes (e.g. drug smuggling or trade in counterfeit currency) and environmental security".[7]

The concept of national security itself has changed dramatically. Till the First World War, it was viewed largely in military and political terms, and was mainly concerned with the armed forces of known adversaries. The ideological impetus of USSR-backed communism for causing political destabilisation in other countries was recognised as a major threat during the Cold War years and was often covertly exercised.

The support given to Islamic fraternal forces to push back or counter Soviet expansionism in Afghanistan gave rise to an even more dangerous force with extra-territorial powers. Today, non-state actors, aided and abetted by the establishments of some states, pose major threats to national security. This has made the task of national security management increasingly complex, requiring knowledge, expertise and organisational infrastructure of a kind that is qualitatively different from what has been available hitherto.[8]

---

[7] According to Amy Zegart, organisational pathologies do require urgent attention even as risks emerge, adding new layers of bureaucratic complexity. *'Spying Blind: The CIA, the FBI, and the Origins of 9/11'*, Princeton University Press, 2009

[8] B. Raman, *National Security Management & Pakistan*, South Asia Analysis Group, Paper No. 507, August 16, 2002.

The view that terrorism is a threat to law and order and can be controlled by the police alone itself has started changing since:

- Terrorism began to be used by certain states to achieve perceived 'strategic objectives';
- Terrorists started resorting to hijacking, hostage taking, using improvised explosive devices (IEDs) to intimidate civilian populations;
- Suicide terrorism, first used with devastating effect by the Liberation Tigers of Tamil Eelam (LTTE) has since been adopted by Islamic terrorists. This has contributed exponentially to raising the threat to national security;
- Easy availability of modern arms and ammunition, and technological innovations to terrorists of different affinities.
- Informal cash flows directed to sustain terror modules, including, through drug trade, in terrorism affected areas;
- Terrorism has been buttressed by the building up of regional and trans-national networks e.g. between jehadi terrorist groups owing a mixed degree of ideological allegiance to organisations like Al Qaeda.
- Organisations like the International Islamic Front (IIF), (formed in February, 1998) that are revanchist in character, medieval in their objectives, yet modern in their methods of operation. They espouse trans-national or pan-Islamic goals.[9]
- Cyber terrorism, and remote controlled missile attacks could be other new threats;
- Maritime terrorism, such as the attack on *USS Cole* in October 2000 and thereafter, the incidents of piracy mainly off the Somali and Ethiopian coasts. The Mumbai attack of 26/11 has also raised the level of such threats and taken them to an entirely different level;
- The Maoist movement has emerged as the single most serious internal security threat to India in terms of the levels and spread of violence, extending across a wide swathe of almost contiguous territory in West Bengal, Bihar, Jharkhand, Chattisgarh, Orissa and Andhra Pradesh. Here the Naxals have consolidated their position and battle capability by exploiting the societal grievances of backward tribal communities and stoking antagonism against the state to their advantage;
- Globalisation, networking and easy access to information technology have

[9] Two of the original signatories of the IIF were Pakistan's Fazl-ur Rahman Khalil of Harkatul Jehad-e-Islami (Huji) and Mir Hamza of Jamiat-ul Ulema-e-Pakistan (JuP). Later 13 other Islamic organisations from different countries also joined - five of which were from Pakistan. In the face of subsequent concerted efforts to search attack and decimate IIF's leadership, through intensified drone operations by USA in recent years, it has adopted several manoeuvres to develop regional linkages and ever expanding networks with new disenfranchised or embittered groups, mostly in Muslim majority countries.

given terrorists an awesome power for economic disruption and destruction;

These developments have had an effect on counter-terrorism as well. In the past, counter-intelligence in its traditional sense could be defined as the pre-empting of threats by hostile countries in espionage, subversion or sabotage. Today counter-intelligence has to perforce focus more on constantly denying tactical victories to terrorists and frustrating the plans and capabilities of non-state actors. This has to be achieved through "smart counter-terrorism", which has four components: better intelligence, better security, better coordination between different agencies on the ground for attending to the above tasks, as also better investigation and crisis management when incidents occur. It also entails a capability for deniable retaliation.[10]

Present capabilities, deficiencies and gaps

In keeping with the British model of police administration in India, the intelligence collection cells of the police were the Special Branch (SB) or the Criminal Investigation Department (CID). The armed forces and national level intelligence agencies played a back-up or support role. As more and more serious incidents of terror confronted the state, they came to be viewed as a threat to national security as a whole - internal as well as external. It was seen that national intelligence agencies were good at investigation or detection work after an incident occurred but they were found wanting in prevention or in the precise prediction of a planned attack. More often than not, this was not always due to lack of precise intelligence inputs. The lapse was more on account of inadequate follow up action or close monitoring, lack of coordination at different levels at the centre and the states or the concerned implementing agency.

In the context of internal security, where Naxalism has assumed priority, the inadequacies of the central and state intelligence apparatus became apparent in the most active hubs of Maoist activity in remote tribal areas of Chattisgarh, Jharkhand, Bihar and parts of south-west Bengal. Some superficial political inputs may be available but they are not enough to provide access to hard-core operational information for storming their hideouts. On the other hand, Maoists more often than not have a string of local informers giving them advance information about troop movements and plans of operations. This can be illustrated further by studying examples of some major intelligence lapses:

Intelligence Lapses

Serious breaches of national security have an intelligence related cause and effect. Five such causes include:

- zero intelligence (The Falklands invasion by the Argentine army in1982; and the Mumbai blasts in March 1993),

[10] B. Raman, "Countering Terror: Challenge of 21st century, Paper available at the South Asia Analysis group Website.

- inadequate intelligence: Rajiv Gandhi's assassination, May 1991 and Kargil in 1999,
- inaccurate intelligence: Assessments, both in UK & USA about Iraq's WMD capability; IB reports of 12 Naga insurgent groups going to Yunnan in 1968 via Kachin state in Myanmar to establish contact with China; R&AW report in 1980s about Chinese troops stationed in Tibet,
- excessive intelligence or overload of often irrelevant intelligence faced by most modern intelligence agencies due to increase in inputs, mainly through technical inputs (TECHINT) and a plethora of open source inputs(OSINT), *and*
- inadequate follow up action on available intelligence.[11]

A study of some past cases of intelligence failure may help identify in broader terms issues that impede good intelligence at the level of collection and analysis, the level of human resources, in inter-agency co-ordination and in the quality of the final assessments.[12]

The Falklands enquiry in the UK highlighted the importance of the physical presence of an intelligence agency in a target country, either under diplomatic or non-diplomatic cover. There were enough open source inputs regarding Argentinean intentions including press reports and British Embassy dispatches, but these do not seem to have been appropriately analysed to arrive at the right conclusions.

The enquiry identified three major gaps: the absence of systematic dissemination and analysis of open intelligence having a bearing on the issue; the absence of the practice of reverse analysis to look at things from the perspective of the adversary; and the absence of independent thinking at the level of the joint intelligence committee.

An evaluation by R&AW in 1989 of the likely threats to Rajiv Gandhi's security, as the then Leader of the Opposition in Parliament, did focus on the threat from Sikh extremists in his travels in north India and from Sri Lankan Tamil terrorists during travels in south India. The Verma Commission of enquiry found this R&AW assessment fairly accurate. However, this general warning proved inadequate. There was no specific alert to find out if the LTTE was doing anything to prepare for an assassination attempt. TECHINT means were not effectively utilised before the assassination. A few days after the event, R&AW did track the minute-to-minute movement details of the surviving perpetrators of the attack. Communications from LTTE headquarters were intercepted and their codes successfully broken, but questions over why this capability could not help detect the arrival of the assassination team in Chennai, its subsequent movements and preparations, continue to linger.[13] The Jain Commission found that the IB was

[11] B.Raman, "Maj. Gen. Sinha memorial lecture at United Services Institute", April 26, 2004

[12] N. S. Sisodia, "IDSA Round Table on Intelligence Reforms", August 6, 2010

[13] B.Raman, op cit: paras 39-42;

intercepting the coded messages of the LTTE but did not have the capability to break their codes. The IB did not inform R&AW about these un-deciphered messages while the R&AW also did not indicate that it had the capability to break the codes.[14]

There have been innumerable instances where intelligence agencies have played a stellar role by gathering correct preventive intelligence, but this advantage was frittered away due to lack of effective coordination between various agencies. The Rajghat incident of October 1986 is the best example of that. The R&AW passed on a specific input, based on HUMINT, about the possibility of a Sikh terrorist hiding in the bushes near the *samadhi-sthal* at Rajghat, during a VIP visit. This information was passed on to the Delhi police directly and to the Special Protection Group (SPG). Searches were conducted but the intruder was not detected. The lack of adequate coordination between IB, R&AW and Delhi police came up for criticism during the post-mortem of this case

The Sri Lanka operation, which was the Indian Army's first ever overseas force projection operation, also underlined lack of adequate coordination between various agencies. India's military intelligence (MI) had limited HUMINT capability. The then available ELINT (Electronic intelligence) and SIGINT (Signals intelligence) were primitive by modern day standards. When the Sri Lankan army crackdown on Tamil militants in the Jaffna peninsula had reached a vital stage, a small MI directorate team was moved to Chennai to cover Sri Lanka. Till the IPKF (Indian Peace Keeping Force) moved into Sri Lanka, this MI team was the DGMI's sole source of intelligence. Of course, it had some access to IB and R&AW inputs. The IB was keeping an eye on the activities of Tamil refugees from Sri Lanka. It also had very good knowledge of LTTE's activities in Tamil Nadu. The state police Special Branch was another good source, but the DGMI had no direct access to any of them.

When India decided to send troops to Sri Lanka following the July 1987 Indo-Sri Lanka agreement, the Army's Southern Command based in Pune established an Operational Forces Command (OFC) in Chennai to oversee the operation. The DGMI attached Tamil speaking Intelligence Corps officers to the OFC. Later, the 57 Mountain Division Intelligence Company was moved to Palaly, Sri Lanka to augment MI resources.

Several coordination problems between the MI and civilian intelligence surfaced during this period. The R&AW claimed that the Army Headquarters did not take it into confidence or seek its advice prior to the Jaffna operations. During the operations, there was no advance planning for the interrogation and screening of suspected civilians and prisoners, either at the OFC HQ or at the divisional HQ.

[14] B.Raman, op cit: paras 43-44;

After initial hiccups, coordination between R&AW and the advance HQ of the OFC improved. However, the MI perception remained that R&AW's inputs on LTTE's military capabilities were not specific or detailed enough. Neither could their future actions be accurately anticipated. No accurate maps of the theatre of operations were made available by R&AW to MI. Deliberate LTTE leaks (on TECHINT) about Prabhakaran's possible hiding places proved inaccurate. There was a view that success of interaction between the Army and R&AW often depended too much on the personal equations between officers on the spot as, there were no standard operating procedures for intelligence sharing, in absence of which, both sides lived in 'a culture of denial'.

The IB too was found to be focused on gathering internal political intelligence, whereas once the Indian Army went in to the Sri Lankan mainland, the fine line dividing political and operational inputs got blurred during counter insurgency operations. The MI officers felt the IB was unable to appreciate the needs of forces operating in an alien environment.

The DGMI could not provide "top down" assessments during the course of the operations, which hampered MI planning at the Advance HQ OFC. The frontline troops' requirements of tactical intelligence from OFC MI units could be met to a certain extent wherever there was close coordination, notably in the Jaffna, Trincomalee and Batticaloa sectors, but unfortunately this could not be achieved fully in the jungle terrain of Vavuniya and Mullaitivu districts due to lack of good enough HUMINT.

Though OFC MI had established useful links with Sri Lanka's National Intelligence Bureau (NIB), some of its inputs were misleading. Constant vigilance had to be maintained to prevent efforts to thwart operations, particularly between 1988-89. The overall paucity of intelligence staff and lack of inputs from air or naval Intelligence sources were also limiting factors.[15]

Apparently, the failure to initiate remedial measures in the light of the above incidents and their post-mortems, greatly contributed to the Kargil incursions. The Kargil Review Committee (KRC) found serious deficiencies at various levels of intelligence collection, operational processes and coordinated sharing of inputs but stopped short of deeming it an intelligence failure. This was more a case of inadequate intelligence. For one, the armed intrusion by Pakistani Army regulars remained undetected and came as a complete and total surprise. This had more to do, perhaps, with a practice that had developed over the years, of leaving some particularly hard or inaccessible sectors in the Kargil-Dras-Batalik area unpatrolled, which was well known to the armies of both India and Pakistan. The Pakistanis tried to exploit this situation with a somewhat harebrained, albeit bold scheme, hatched between a small group of four top generals who had served in

[15] Col (Retd) R. Hariharan: Presentation at Centre for Joint Warfare Studies (CENJOWS) seminar, New Delhi,Sept15-16,2008.

these forward areas at some stage in their early careers. These included the Pak Army chief Gen Musharraf, the Rawalpindi based Commander of the X Corps Lt. Gen Mehmood Ahmed, Divisional Commander FCNA (Force Command, Northern Areas) Maj. Gen. Javed Hassan and the Chief of General Staff, Lt Gen Mohammad Aziz.

The Director General of Military Operations (DGMO), Maj. Gen. Tauqir Zia was kept completely out of the loop in the initial stages of planning. He also acquiesced but much later. Generals Aziz and Mehmood Ahmed in particular, presented the plan as an opportunity to take advantage in this 'no man's sector' and settle scores with India for Siachen, 1984.[16] The usually powerful collegiate body of other Corps Commanders was informed much later. One of them, Lt. Gen. Tariq Pervaiz, GOC XII Corps, Quetta openly criticised the strategy in his discussions with his juniors, leading to his subsequent sacking by Musharraf.

The Kargil Review Committee found R&AW's HUMINT to be quite weak. It had some graziers or shepherd assets who traversed this terrain but not in the winter months. Ultimately, in early May 1999, just before an Army patrol sent to look out for intrusions was attacked, one such shepherd alerted the Army about the sightings of suspicious intruders in the 'sangars' (stone hutments on Kargil heights). Apart from that, there were some sporadic reports about purchase of unusually large quantities of winter boots by the Pak Army and some logistic buttressing of forces in the Gilgit - Olthingthang region across Kargil. However, none of this was considered good enough indication of the Pak Army's Kargil plans. Ideally, there was need for much higher levels of penetration within the Pak Army hierarchy, for sounding the alert through HUMINT, which was lacking.

Nonetheless, the R&AW got some very good TECHINT breaks during the Kargil standoff. The interception of a telephone conversation between Gen Musharraf, during his visit to China, with his Chief of General Staff, Lt Gen Aziz, provided crucial evidence to international interlocutors and media, worldwide that the intruders were Northern Light Infantry 'regulars', whose 'jugular' (*tooti*) was being controlled throughout by the Pakistan Army .

This helped turn the tide of world public opinion in favour of India, though the subsequent casualty of the concerned technical intelligence link had to be endured. The KRC report also acknowledged the work of the Aviation Research Centre (ARC), which produced excellent aerial intelligence after the intrusion, was detected. The question as to, why the ARC was not deployed for similar aerial surveillance in this area before the conflict broke out, particularly after some trans-border sources of the IB and the R&AW had reported heightened ground

[16] Shuja Nawaz (2009), "*Crossed Swords: Pakistan, its Army and the Wars Within*", Oxford University Press: Karachi, pp 512-513.

level activity in some military formations on the other side, however remained unanswered.[17]

Though lack of coordination between the R&AW and the Army, especially DGMI was highlighted in the Kargil Review Committee report, shortcomings in this regard persist and cannot be addressed simply by the creation of a separate Defence Intelligence Agency (DIA). The DIA has functioned so far as a collation agency for tactical intelligence whereas the responsibility for strategic intelligence remains with the R&AW. Yet the defence services are generally believed to be lukewarm to R&AW's indent for serving officers to meet its job requirements.

Mumbai attacks

The 26/11 Mumbai incidents, which should have been studied as a national intelligence and security lapse, was the subject matter of a limited probe that was confined to the Mumbai police's reaction to the terrorist attack. The Maharashtra Government classified the report denying their own police officers or other departments the opportunity to study it for better future action. Even legislators were not allowed access to it for a long time. The enquiry committee received no help from the Central Government despite many requests. Central intelligence reports were made available only to the local Director General of Police's (DGP) office. However, even within the limited mandate, the committee discovered grave lapses in the response to central intelligence pointers in building up of resistance capability, in assessing the overall picture and transmitting the pointers to the ground forces for adequate action. During our enquiries we were told that the Multi-Agency Centre (MAC) and its state-level compartments - State Multi-Agency Centres (SMACs) were doing only the collation work by pooling available intelligence with the members. There was no "intelligence arbitration" with different agencies to analyse intelligence and arrive at a common threat perception. The Mumbai police also neglected the OSINT although similar terrorist attacks had taken place on the Serena Hotel, Kabul (January 14, 2008) and the Marriott Hotel in Islamabad (September 20, 2008). In fact, in March 2007 the local press had reported that the Coast Guard had apprehended a suspected Lashkar-e-Taiba (LeT) boat heading towards the western coast but had allowed it to get away. These LeT cadres were later arrested by Rajouri police (J&K). Had the local police been sensitised to these developments they could have had a better appreciation of the threat from the LeT to Mumbai. Intelligence for ground action can thus originate not only from secret sources but also from the open media.[18]

Counter-intelligence lapses

Not much data is available in the open domain about counter-intelligence lapses. However observations, albeit guarded, can

[17] B.Raman: op cit: para 51.

[18] V. Balachandran, Special Secretary (Retd.), Cabinet Secretariat & co-author, *Pradhan Committee Enquiry Report*, in a note for IDSA Round Table, Aug 2010.

be made about a case where a senior intelligence officer in one of India's intelligence agencies was compromised and eventually detected before too much damage could be done to India's national security.

Early detection in this case happened due to the determination of a relatively junior surveillance officer. Despite instructions to 'lay off' a foreign operative engaged in liaison contact, the surveillance official detected rather elaborate warding off measures being taken by this foreign intelligence operative. This eventually led to the identification of the vehicle of the contacted Indian official used for their meetings. Though the ownership of the vehicle could be traced, the first laxity in the enquiry took place at this stage because of the diffidence of the junior level officers to undertake follow up actions in a case where one of their very senior officers was involved. Surveillance continued in fits and starts over the next six months or more, during which period there were fresh sightings to confirm the link between the foreign operative and the concerned official. A decision then had to be taken to summon the officer before his seniors and confront him with evidence about his complicity. At this stage too, damage control actions were marked by considerable diffidence. For instance, though it was decided to search the officer's residential premises, the search itself was conducted somewhat perfunctorily - cupboards, which the officer claimed, contained only his personal belongings were not searched. After three days of strenuous denial and outrage, an eventual lucky break helped break down the suspect. One of the officers in the interrogation team was carrying a packet of magazines meant for the senior officer which would have been delivered at his residence in the normal course. The officer mistook these for audio and video recordings confirming his guilt and confessed his involvement but maintained that he was doing so only to further psy-war objectives, in India's national security interest. This defence was not accepted as convincing enough and the officer had to quietly accept retirement with some dishonour, despite his earlier exemplary record and high profile career.[19]

Public discussion of intelligence failures almost invariably follows the slip ups, real or perceived, of the intelligence community, who try to balance out such perceptions by claiming and publicising, at times over publicise, their successes. The propensity of the media and the academic community to dissect the performance of intelligence agencies with their limited understanding of the realities of intelligence work, or on the basis of such overly publicised successes, or the not so highlighted failures, has the potential not only to demoralise the hard-core intelligence activists, but also to an erosion of public trust in their capabilities.[20]

---

[19] Though no attributions can be made, the above account is based on first hand knowledge of some serving intelligence professionals whose names cannot be disclosed, for obvious reasons. Those in the intelligence community would be able to identify the case in question.

[20] Nigel Inkster, "Review Essay: The Protecting State", *Survival* –Oct-Nov,2010, IISS: London

Timely intelligence can do much to reduce risks to national security. But the limitations of this capacity need to be clearly understood. Intelligence cannot predict the future. It can, given time and luck, reveal secrets. It cannot provide foolproof pointers to the thought processes of particular leaders or the outcome of complex and dynamic situations. It can however serve to reduce uncertainties for policy makers by making them confront uncomfortable realities.[21]

How to create these capabilities

Intelligence agencies must be clear about the challenges to the security of the state. Their ambit will perforce need to extend to the entire gamut of collecting intelligence on internal security, external security, military intelligence – both tactical and strategic, economic and commercial intelligence as well as new data in science and technology related issues.

The creation of a world-class intelligence set-up to meet these requirements will necessarily have to be taken up over the long-term, with the short term and medium term objectives clearly identified. While the main role of intelligence collection will remain focused on collection of inputs (operations), compilation and assessment (analysis) would be equally important but the kind of intelligence needed and the speed in obtaining it would be crucial.

One question that needs to be asked is whether some of these requirements are better left to the exclusive domain of line departments: e.g. the Department of Revenue Intelligence (DRI), or the Economic Offences Wing (EOW) under Ministry of Finance, Department of Science & Technology, the Atomic Energy Commission (AEC) and the Defence Research & Development Organisation (DRDO)? A related question would be whether these departments would at all care to assign such intelligence collection tasks to agencies that are bereft of specialists? Alternatively, if they want to do these tasks themselves, then the question may well be posed whether their own specialists have the requisite training or aptitude to handle this type of work? This question is particularly relevant for collection of science and technology intelligence, being undertaken by agencies like the Bhabha Atomic Energy Commission (BARC) or the Indian Space Research Organisation (ISRO).[22]

There would also be a need to take cognizance of the many non-traditional areas of intelligence – financial transactions, technological transactions, large company manoeuvres, organised crime etc. Connecting the dots in these specialised areas of intelligence collection, would make the process of intelligence collection far more complicated. Two suggestions that could be considered in this context are: every major economic department may need an intelligence

---

[21] David Omand (2010). "*Securing the State*", Hurst: London

[22] Authors interview with Shri K. Santhanam, former Scientific Adviser to Govt of India: discussions with author-07.01.11

wing, and increased outsourcing from intelligence agencies to think tanks may become necessary.[23] In practice, such cooperation is already underway in the day-to-day functioning of government departments; but it has not always been uniform or regular, being dependent on the rapport between personnel involved. These arrangements need to be institutionalised.

Another question which must be tackled in any worthwhile exercise on reform of Indian intelligence set-up, would be to examine whether only personnel from the police can be considered fit for intelligence operations and organisations? What makes them more suitable for analysing intelligence inputs, than say an economist, academic, area expert, or scientist? Or should India cast its recruitment net wider, to include the sizeable national talent pool of technocrats and specialists of different hues to assist in the task of intelligence gathering. Given the intricacies and specialisation now required for intelligence collection in the modern era, the number of police officers involved in intelligence collection, as opposed to counter-intelligence, has to be not as pervasive as so far it had been. This suggestion has already been made in the FICCI task force report[24] that advocates developing a special cadre of trained personnel for national security management. After 9/11 and Iraq, Western intelligence agencies have begun the process of grappling with the demands of "post-modern Intelligence". The sheer pace of change, not only because of the technological and information revolutions, has left many in the intelligence community struggling to update their practices and prescribe better practical solutions, to avoid the tendency to lurch from crisis to crisis.

The US intelligence community's traditional model was secret and "collection–centric", and prized classified data. It was driven by data availability while analysis remained secondary. It was context-minimal, with analysts staying close to the data, in "narrow account lanes". It was 'current' oriented, with no collectible facts about the future and warning focused. It emphasised alarm ringing, remained product centric, measuring success as being relative to the "finished intelligence" provided to policy makers, rather than on its utility or service. This model resulted in compartmentalisation and, inevitably, reduced distribution. In today's complex strategic environment, access is largely unrestricted and threats or opportunities can emerge from almost anywhere in this 'information–rich' world. This argues for a more "cognition–centric" model that prioritises sound thinking ahead of mere secret data collection and moves towards a synthesis of facts and analysis which is what is needed today.[25] The intelligence

---

[23] K. Subrahmanyam, Op cit – pg. 8 of transcript, IDSA Round Table, Aug 6, 2010.

[24] FICCI *Task Force Report on National Security & Terrorism*, Vol.1, 2009

[25] Josh Kerbel, "For the *Intelligence Community, Creativity Is the New Secret, "World Politics Review,* Vol. March, 2010, URL: *http: //www. world politics* review.com/articles/5329/for-the-intelligenced-community-creativity-is-the-new secret

community in India too will have to take note of these 'multiple, overlapping and often contradictory narratives to successfully cope with the challenges it faces from multiple directions.[26]

In other words, there is an urgent need for a significant paradigm shift in the focus of intelligence agencies in India. A justifiable case can be made out for the widening of their charters to include subjects like environmental security or energy security, demographic change, climate change etc. Internal security responsibilities today are integrally enmeshed with the security clearances for public sector projects or even private sector projects in the telecommunications sector. Perhaps, an empowered ember in the Planning Commission could oversee security related issues.[27] It is necessary to acknowledge that intelligence has gravitas and is not a dubious calling but an essential component of statecraft, with covert capacities inherent to its domain expertise. If this is accepted then the road map for any intelligence overhaul has to be appropriately designed to meet the modern day challenges facing India as an emerging global power. This would make it necessary that for an effective coverage of intelligence requirements in the 21st century India, the intelligence apparatus should be based on a system created by Parliament that clearly mandates the charters, functions and duties of each organisation, and it should be autonomous in the conduct of its operations, strategies and tactics. The appointment of the heads of these organisations should be the prerogative of the political executive and, finally, the performance of these intelligence organisations should be broadly monitored by oversight committee/s set up by Parliament, while keeping operational matters outside their ambit.

---

[26] *Andrew* Rathmell, 'Towards Post-modern Intelligence', *Intelligence and National Security*, 17(3), Sept.2002, pp.87 – 104.

[27] D. Nath, Special Director, Intelligence Bureau (Retd), Paper for IDSA Round Table: "Thoughts on Intelligence Reform", IDSA: New Delhi.

Chapter 3

Legal Status

It has been customary - ostensibly to maintain secrecy and in the interest of national security - to deny the existence of intelligence organisations. In the United Kingdom for many years, the MI 5 was seen as a deeply mysterious organisation. Successive governments intended it to be so. The intelligence community, though it existed, was meant to stay as far away from the public view as possible.[28] India's intelligence organisations were a colonial heritage and thus they endorsed this legacy of anonymity and denial. Till recently, questions in Parliament pertaining to the legal architecture under which the Intelligence Bureau (IB) functions elicited the response that it figured in Schedule 7 (Entry 8) of the Union List in the Constitution of India.[29] This does not make IB into a statutory body, but merely an *adhoc* administrative arrangement by the Executive.

The end of the Cold War and the disintegration of the Soviet Union gradually transformed public perceptions about the functioning of security services. The advent of international terrorism also contributed to the changed priorities in recognising the role and resources of intelligence agencies the world over. As British society became more open and less deferential, the security services realised that levels of secrecy that went beyond their operational needs actually eroded public confidence and bred conspiracy theories about their functioning and capacities.

In 1989, the Security Services Act placed MI-5 on a statutory footing. Three years later, Stella Remington, its first female chief was publicly acknowledged as its Director General. She very seriously undertook the task of demystifying the service for the public and the media and touted this as one of the main achievements of her term. This demystification was further encouraged by the establishment of a parliamentary oversight committee as well as the legal recognition of the external intelligence organisation - The Secret Intelligence Service or MI-6, under the Intelligence Services Act, 1994.

---

[28] Christopher Andrew (2009*), The Defence of the Realm: The Authorised History of MI5* Allen Lane, London

[29] Manish Tiwari, *"Legally Empowering the Sentinels of the Nation, Issue Brief #20,* Observer Research Foundation, New Delhi, August 2009.

In the *Harman & Hewitt vs. UK* case which came up before the European Court Of Human Rights (ECHR) in 1992, the lack of a specific statutory basis for MI-5 was held to be fatal to the claim that its actions were "in accordance with the law" for the purpose of surveillance and file keeping, contrary to safeguards provided by the convention on the right to privacy.[30] The ECHR later further specified that observing the rule of law by maintaining a simple veneer of legality would not suffice, a 'Quality of Law' test would have to be met , which required any such legal regime to be clear, foreseeable and accessible.

In India too, the Kargil Review Committee (KRC) took note of the legal vacuum in which both IB and the R&AW were working. The Task Force on Intelligence formed by the Group of Ministers recommended specific and formal charter of duties for both external and internal intelligence services of the country.

According to this report, the R&AW was assigned the role of being the primary intelligence agency for collecting and analysing all forms of external intelligence, while the IB was earmarked for a similar role in domestic matters. The IB was also designated the nodal agency for counter–terrorism within the country. It was further clearly mentioned that the IB would liaise with foreign agencies dealing with counter-terrorism "in consultation and co-ordination with R&AW", after obtaining permission from the government at the highest level.[31] These charters have now been codified but they still lack the sanction of specific legislative enactments. Even earlier, after the 1975 emergency, the L.P. Singh Committee had gone into the working of the IB and recommended a written charter for it. It is imperative in a democracy that every organisation of the government draws its powers, privileges and authority from clearly defined legal statutes as laid down by the supreme legislative body in the country. The legal basis must be clear to obviate any obfuscation about both the intent of the legislature and the mandate it seeks to bestow.[32] Not only should such laws spell out the charters and authorise the Central Government to fix broad goals within the charters, they should also hold intelligence agencies accountable. Absence of legislative cover can be a serious lacuna as all intelligence work is carried out under executive instructions. Some of this work, especially that pertaining to foreign intelligence operations, may involve violation of local laws in the target country. There is no legal protection for those who undertake such operations. A legal enactment could offer such protection to Indian intelligence operatives.[33] A case in

---

[30] Hans Born & Ian Leigh (2005), "*Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies,* Publishing House of the Parliament of Norway: 2005.

[31] The Group of Ministers' (GoM), Report on the Kargil Review Committee referred by Mr Satish Chandra, in *AGNI*, *Studies in International Strategic Issue* Vol. 10(4), December 2007.

[32] A K Verma, "Intelligence needs a new order", *Indian Express*-10.2.2005.

[33] A K Verma, Intelligence Reforms, Paper No. 3277, June 26, 2009, South Asia Analysis Group (SAAG), URL:www.http://www.southasiaanalysis.org/%5Cpapers33%5Cpaper3277.html

point is the Lewis 'Scooter' Libby case in 2007, wherein the former Chief of Staff to the US Vice President, Dick Cheney was convicted on a charge sheet filed by a Special Counsel, for revealing the identity of CIA's "deep cover operative", Valerie Palme, a US foreign service officer in 2003.[34]

There is growing and across the board support for such measure with reference to the Indian intelligence agencies, especially among well informed retired intelligence professionals. A case could also be made out to protect intelligence agencies from excessive bureaucratic restraints and controls relating to financial management, without absolving them of the need to adhere to financial probity.[35] In the context of accountability to a political executive in a parliamentary form of government too, the legislative enactment of charters of duty for intelligence agencies could safeguard and protect an honest, upright and conscientious intelligence operative/ official. "If you have a Minister telling the intelligence man to go and do something, and for him to say I will not do it, he should have a piece of paper to say this is what the law says."[36] For the same reason, "the charter for R&AW must be legislated" asserts Brajesh Mishra, former Principal Secretary to the Prime Minister and National Security Adviser[37]

The Geneva Centre for the Democratic Control of Armed Forces [DCAF), the Human Rights Centre of Durham University, UK and the Norwegian Parliamentary Intelligence Oversight Committee undertook a joint exercise to draft legal standards for accountability of intelligence services in liberal democracies. According to them legal standards need to cater to four levels of oversight:

- Internal control at the level of the agency
- Executive control
- Parliamentary oversight &
- Oversight by independent oversight bodies.

Most modern intelligence organisations in the world today, function under the ambit of enacted legislation. The CIA in the US was created by the National Security Act of 1947. The Federal Intelligence Service (FIS) in Russia draws its legal basis from the Law on Foreign Intelligence Organs, 1996. The Federal Intelligence Service (BND) of Germany draws its legal status from the Federal Intelligence Service Law, 1990. In Japan, the Public Security Intelligence Agency (PSIA) is empowered by the Subversive Activities Prevention Law; in the Netherlands, both the General Intelligence & Security Service (AIVD) and the Defence Intelligence and Security

[34] V. Balachandran: Former Special Secretary, Cabinet Secretariat: A Paper on Intelligence Reforms sent to IDSA Task Force – June,2010.

[35] Op.cit.

[36] K. Subrahmanyam, IDSA Round Table on Intelligence Reform, August 6, 2010.

[37] Brajesh Mishra, IDSA Round Table on Intelligence Reform, August 6,2010

Service (MIVD) are mandated by the Intelligence and Security Services Act 2002, as amended in November 2, 2006.

A study of these legislations reveals certain key features. The role and spheres of operation of intelligence agencies should be clearly defined by legislation. In a democracy, the responsibility for delineating these tasks lies with the parliament. Threats to national security and the powers and mandates of officials entrusted to deal with organised crime, terrorism and espionage require careful definition and need to be specified. These may have variables that distinguish between internal and external services. The practice followed in Western democracies has been to refer to security services for internal threats and to intelligence services for external threats. Separate legislation has been drawn up for different agencies. The powers of the heads of the services are clearly delineated. It is clearly mentioned that they will report annually to the political executive – the Prime Minister, in a parliamentary model and the President in a presidential form of government. Other layers and institutions of oversight and supervision – internal, executive, judicial and legislative - are also defined in such legislation. Such a clear enumeration of duties at supervisory levels helps maintain accountability. Responsibility for misuse of office or secret funds can be fixed and allegations of misuse or other misdemeanours can be promptly enquired into by the competent legal authority, instead of their appearing again and again in the media and lowering the prestige of the government.[38] Thus, the very first reform recommended is to give Indian intelligence agencies the support of legislative enactments. The model of the UK Intelligence Services Act, 1994 could be followed to frame the provisions of an act to accord legal status to the R&AW while the Security Services Act, 1989 could serve as a model for the IB.

[38] V. Balachandran, Op cit, Pg 6

Chapter 4

RECRUITMENT

It will be difficult to bring about any effective intelligence reforms unless there is clarity about the fact that intelligence is a specialised activity in which excellence is at times achieved because of an inherent or individual knack but is generally built up and cultivated as a life long passion.[39]

Intelligence collection and operations are highly specialised skills, that include language skills, an in depth knowledge of strategic matters of target countries/areas, their cultural mores, computer know-how, technological skills, etc. These capabilities are not something that can be developed overnight by everybody, or by men and women who seek to join an intelligence agency as a temporary haven, or as an opportunity to treat these organisations merely as stepping stones to greener pastures.[40] In the past, persons recruited for intelligence agencies at various levels were not always ideally suited for intelligence work. The recruitment processes were often too general and bureaucratic. No attempt was made, on the pattern of Service Selection Board procedures, to find out if the applicants had any aptitude for this type of work. Perhaps too much faith was reposed in following the rather simplistic approach, of naively identifying intelligence collection capabilities with requirements of a 'law and order' or criminal investigation approach.[41]

Most modern intelligence services across the world have refined their recruitment processes over a period of time. In fact, an analysis of the careers of leading personalities from the field of intelligence world over would reveal that hardly anybody has been from the regular bureaucracy:

- Sir Maurice Oldfield: Legendary Chief of MI-6 (1973-78) on whom Le Carre had based the character of "Smiley" in his *Tinker, Tailor* series of novels, an academic from Manchester University, Army officer, MI-6 Chief and after retirement Chief Coordinator Intelligence & Security, Northern Ireland where he managed to exercise a marked control over IRA activities
- William Casey: Lawyer, US Naval

---

[39] D. Nath, "Thoughts on Intelligence Reforms", Paper for IDSA Round Table, August,2010

[40] Vikram Sood, "Intelligence Reform", *Indian Defence Review*; Jan/Mar '2009

[41] P. K. Upadhyay, Concept Paper on Intelligence Reform, IDSA Round Table, Aug 2010

officer, OSS, Chairman of Securities & Exchange Commission, Reagan's chief campaigner, CIA Chief (1981-87)

- Richard Helms: Journalist with United Press in London during the pre-World War-II days, Indianapolis Times, Navy, OSS and CIA Chief (1966-73)
- William Colby: Academic from Princeton, US Army, OSS, law graduate from Columbia (1947), CIA Chief (1973-75)
- Prof. Joseph S. Nye: Harvard University, Chairman, National Intelligence Council 1993-94 (Like our JIC). Won Distinguished Service Medal for intelligence, now Dean, Kennedy School of Government (Harvard)

In most developed countries, the practice of utilizing university dons as talent spotters for campus recruitment is very common. If this approach has to be adopted in India, the focus would have to shift to merit based recruitment and promotion practices which can be de-linked from hierarchical equivalences. The ideas of hire and fire and even outsourcing for specified tasks have to be seriously considered. The United States introduced a new post of Director of National Intelligence (DNI) and set up the National Counter Terrorism Centre in 2004 after the Kean Commission of Inquiry submitted its report. In fact, the changes made within the US intelligence community, including the creation of a new Department of Homeland Security reflected a pre-disposition to respond to 'intelligence failure' with structural reforms, despite persisting scepticism among seasoned observers about the value of mere organizational reforms.[42]

Elsewhere in UK and Canada also changes have been implemented. In Britain, a new Joint Terrorism Analysis Centre (JTAC), has been established, which is housed within the Security Service (SS –old MI – 5) headquarters. A new Head of Intelligence Analysis has also been appointed.[43] On its part, the Canadian Security Intelligence Service (CSIS) undertook a study on the relationship between climate change and environmental degradation as far back as 2004. More recently, the John Major Commission inquiring into the bombing of the Air India Kanishka aircraft, revealed that divesting intelligence functions and responsibility from the Royal Canadian Mounted Police (RCMP) by creating a separate civilian agency –the CSIS– had not solved the problem of effective co-ordination of security intelligence.[44]

Intelligence agencies in various countries have from time to time undergone extensive restructuring to adapt themselves to the changing situations. Some examples:

UNITED KINGDOM:

In 1909 Capt. Vernon Kell (South Staffordshire Regiment) and Capt.

---

42 Len Scott & G. Hughes : *Intelligence & National Security in 21st Century* : Published by Routledge.

43 Peter Hennesssy : *From Secret State to Protective State* : *In The New Protective State: Government, Intelligence & Terrorism.* Continuum Books, 2007.

44 V.Balachandran : Paper on Intelligence reforms sent to IDSA –July 2010.

Mansfield Cummings (Royal Navy) established a "Secret Service Bureau" (SSB). Capt. Kell (known as "K") was in charge of counter espionage while Capt. Cummings ("C") dealt with foreign intelligence. In 1916 the SSB became part of military intelligence. The internal wing was designated MI-5 while the external arm was known as MI-6. However, in 1931 MI-5, later known as Security Services (SS) became independent and was placed under the Home Secretary. In 1992 the responsibility for coverage of Irish terrorism was taken away from the London Metropolitan Police and transferred to MI-5. The Security Services Act (1989 & 1996) placed it under parliamentary scrutiny.

MI-6 also became part of the War Office & Admiralty in 1916 but became independent in 1922 when it was designated as the Secret Intelligence Service (SIS). In 1940 Winston Churchill and Hugh Dalton set up the Special Operations Executive (SOE) known also as "Baker Street Irregulars" to conduct irregular warfare behind the enemy lines. After the war the SOE was merged with SIS in 1946. The Intelligence Services Act (1994) placed the working of the SIS on a statutory footing under the Foreign & Commonwealth Secretary. It is also under the watch of the Parliament's Intelligence & Security Committee and the Ministerial Committee on Intelligence Services (CSI) chaired by the PM.

The technical intelligence for the services was provided by the Government Code & Cipher School, which later became the Government Communications Headquarters (GCHQ) in 1946. Like the MI-6 the functions of GCHQ are governed by the Intelligence Services Act (1994) and supervised by the Foreign & Commonwealth Secretary.

Recruitment to MI-5, MI-6 and GCHQ:

These three organisations have considerable autonomy in recruiting staff and do not depend upon the general recruiting channels of the UK Civil Service. The MI-5 advertises vacancies on their website (www.mi5.gov.uk) and the candidates can apply online. MI-5's flexibility in recruiting senior management directly can be seen in the way Stella Rimington, the first woman MI-5 Chief (1991) was enlisted into the service in 1967 while her husband was posted in New Delhi as the First Secretary in the British High Commission.

Rimington gives a detailed account of the recruiting process in MI-5 in her book *Open Secret* (2001). Till the 1980s the channel for recruitment was either through Talent Spotters (not a great success) or from the Civil Services. In 1996 both these were given up and open advertisements started appearing from 1997. Her book is a treasure trove of information regarding the human resources' problem of motivation and performance assessment that bedevil a secret organisation, preventing it from imbibing good management practices from outside because of the need for secrecy.

Like the MI-5, recruitment to GCHQ is also done through their website. However prospective candidates for MI-6 have to apply by post to the Secret Intelligence Service.

USA

At the beginning of the 20th century, the

US Army's G-2 Branch performed the intelligence functions for United States. In 1942 the Counter-Intelligence Corps (CIC) and Naval Intelligence (ONI) took over this task. The Pearl Harbour experience led to the setting up of the Office of the Strategic Services (OSS) under Col. Donovan, a distinguished lawyer who had seen action during World War1. OSS began as a 'Research & Analysis Organisation' as part of the Library of Congress, handpicking some of the best historians and scholars to give strategic assessments. In 1942 the name was changed to OSS when it began to undertake activities behind enemy lines like the British SOE. After the War, President Truman disbanded the OSS in 1945 and handed over the intelligence functions to the Defence and the State Departments. However the compulsions of the Cold War led to a re-think. A New York businessman, Ferdinand Eberstadt was commissioned to prepare a blueprint for the setting up of a civilian intelligence agency. The National Security Act (1947) and CIA Act (1949) for setting up the National Security Council (NSC) and the CIA were passed as a result of this exercise. The Director Central Intelligence (DCI) was made responsible for intelligence coordination covering all the intelligence organisations including military intelligence, besides heading the CIA. After the passing of the Intelligence Reform & Terrorism Prevention Act (2004), a new post of Director National Intelligence (DNI) was created in 2005 in the White House to take over the coordination, previously under the DCI. The National Security Agency (NSA) and the National Reconnaissance Organisation (NRO) were formed in 1952 and 1962 respectively to collect technical intelligence. The Defence Intelligence Agency (DIA) was set up in 1961 while the National Intelligence Council (NIC) was established in 1980 to prepare and disseminate "Intelligence Estimates" (like the Indian JIC).

Recruitment to the CIA:

In the beginning CIA 'recruiters' used to visit universities including Ivy League Colleges for recruitment. Several graduates from these institutions joined the organisation in the early days. In addition, the organisation was able to attract intellectual giants like Prof. Willmore Kendall and Prof. Sherman Kant in the middle level management for the Analysis Desks during the 1940s and 1950s. Robert Gates, the youngest CIA chief in history who worked under five US presidents in different capacities, including, as the Deputy National Security Adviser was recruited in 1965 from Indiana University. He joined the CIA in 1968 after undergoing military training sponsored by the spy agency. Now advertisements are regularly placed for recruitment. An advertisement even appeared in *The Economist* in September 1999. Vacancies even in superior positions in these organisations are now advertised through the general federal employment website (www.usjobs.opm.gov). A prospective candidate can go to this general website, check his/her preferences and directly access the department concerned. For example "US Jobs" in July 2005 advertised various positions in CIA including that of Senior Intelligence Analyst (annual salary: $ 114,882). All these are for GS (General Schedule) jobs. The candidate can also access the websites of the concerned departments directly - even that of the CIA (www.cia.gov/employment). None of

these organisations depend upon the general federal recruitment procedure for recruiting their staff. The CIA website in July 2005 advertised for a Deputy Director (Technical Services), which is a very senior appointment on an annual salary of $149,200. There is no single civil service examination in the US and it is clearly stated that the candidate would not be required to take any kind of test at all for most federal jobs.

In July 2005 the CIA advertised for their 'Clandestine Services' with this job description:

> This is an elite corps that gathers the vital information needed by our policy makers". The requirements were a Bachelor's degree and an upper age limit of 35. The posts advertised were: Core Collector, Staff Ops. Officer, Collection Management Officer Ops., Targeting Officer, Language Officer etc., carrying an annual salary of $ 78,000 (*possibly, at entrance level*.)

In order to target the youth, the CIA offers Student Internship Programmes and Graduate Study Programmes whereby a recruit is allowed to continue his education with funds from CIA and later join the organisation.

However CIA does not encourage short term recruits or deputationists and has been following the policy of Allen Dulles, its pioneer:

> A sizable turnover of short term employees is dangerous because it means that working methods, identities of key personnel and certain projects in progress will have been exposed in some measure to persons not yet sufficiently indoctrinated in the habits of security to judge when they are talking out of turn and when they are not. (*The Craft of Intelligence*)

ISRAEL

Ben Gurion set up five intelligence and security outfits at the formation of the state of Israel:

(a) *Shai*: Intelligence Wing of *Haganah* (Jewish underground army)

(b) *Shin Beth*: internal security

(c) *Aliyah Beth*: To smuggle in Jews from other countries

(d) Foreign Ministry

(e) Police

In 1951 a reorganisation was effected and *Mossad* (Institution for Intelligence & Special Assignments) was created by combining *Shai*, *Irgun*, etc and placed under the Foreign Ministry. Later it started reporting to the Prime Minister. A new outfit – *Aman* - was created for collecting military intelligence while *Shin Beth* and *Aliyah Beth* continued with their original tasks.

For long Mossad followed the recruitment policy laid down by their legendary second chief Isser Harel (known as 'Isser, the Little', because he was short) who became famous for his 15 year manhunt for Adolf Eichmann. Isser who was the Mossad Chief between 1952 and 1963 did not allow a single volunteer into the service. He also cared little for seniority and promoted on merit. It was the official policy in the 1980s/1990s that recruitment to Mossad was always through talent

spotters or from among the relatives of serving personnel.

However, this started changing from 1998 following various controversies involving Mossad when there was a public outcry to introduce more transparency into its working. This dramatic change took place when Ehud Barak was the Prime Minister. Now an aspirant can apply directly on its website www.mossad.gov.il. All applications are handled by the Prime Minister's office only.

The working of Mossad is totally different from that of conventional intelligence organisations. Firstly, it believes in having a limited permanent cadre and more irregulars or retired persons who are paid out of secret funds. Operations abroad are mostly undertaken through the *Sayanim* (local Jewish volunteers) and the *Bodlim* (Safe House Keepers). At one time it was reported that there were as many as 2000 *Sayanim* in London alone. Most of the important operations are handled from the headquarters to ensure tighter control by the *Katsas* (Case Officers), while local units only play a supporting role. A *Yarid* (Security Officer) whose job is to provide facilities, cover, etc. is deputed for all important operations so that the local operative is not exposed. Secondly, Mossad personnel are not given any cover jobs while posted in their missions, or given only very light jobs with innocuous designations.

Canada:

For 120 years the RCMP (Royal Canadian Mounted Police) handled Canadian national intelligence functions. However various controversies about the excesses committed by the RCMP forced the government to set up the Mackenzie Commission (1960) and McDonald Commission (1981) which recommended divesting the RCMP of its role in national security intelligence and establishing a civilian intelligence agency under parliamentary control. "The Commission found that it was not appropriate for a law enforcement body like the RCMP to be involved in security intelligence work" (Mackenzie). McDonald believed that "Law enforcement and security work are incompatible". Following these reports, the Canadian Security & Intelligence Service Act (CSIS) was passed in 1984.

In 1987, the Osbaldeston Report on the staffing of CSIS recommended that recruitment be commensurate with the new requirements including counter-terrorism and counter-proliferation. The service was asked to recruit "high calibre university graduates to become intelligence officers". All vacancies are advertised on their website and prospective candidates apply on line.

South Africa:

Far reaching intelligence reforms were introduced in South Africa after the apartheid regime ended. The National Strategic Intelligence Act (1994) gave the mandate for the new intelligence set up while the Intelligence Services Act (1994) lead to the creation of the National Intelligence Agency (NIA) for domestic intelligence and the South African Secret Service (SASS) for external intelligence, which included external military intelligence as well. The NIA and SASS were formed on Jan 1, 1995 after merging the following intelligence services:

(a) National Intelligence Service &

Department of Intelligence & Security of the former regime

(b) Pan-Africanist Security Service

(c) African National Congress

(d) Intelligence structures in Transkei, Bophuthatswana, Venda & coordinates with Ciskai

The NIA and SASS work under the Minister for Intelligence who coordinates with the Minister for Defence (South African National Defence Force-SANDF) and the Police Minister (South African Police Services-SAPS). In addition there is also an Intelligence Co--coordinator who heads the National Intelligence Co-Coordinating Committee (NICOC) for disseminating intelligence (like the JIC in India). Oversight and control are exercised by the Cabinet Committee and the Joint Standing Committee on Intelligence (JSCI). Besides there is an Inspector General to investigate any problems within the agencies whose annual reports are made public.

Over a period of time, many 'whites' took voluntary retirement from the NIA which was once a European dominated agency. The new recruits, mostly Africans, have now taken their places. Its present race-wise composition is as follows:

Africans: 62 per cent

Whites: 32 per cent

Coloureds: 4 per cent

Asians: 2 per cent

Both NIA and SASS allow direct recruitment to various posts such as intelligence officers, analysts, legal advisors, financial officers etc. Both services are exempt from the Labour Relations Act 1995, Basic Conditions of Employment Act 1997 and Employment Equity Act 1998.

SASS also has a student internship programme like the CIA. Such student internees are first trained in the South African National Academy of Intelligence (SANAI), which provides training for cadet intelligence officers in basic subjects like intelligence orientation, and report writing. After this they can continue education in regular institutions or pursue a career in intelligence by getting further training.

India

Research & Analysis Wing (R&AW)

The R&AW was not conceived as a central police organisation. The then Prime Minister, Smt. Indira Gandhi and the organisation's founding fathers, Rameshwar Nath Kao and K. Sankaran Nair repeatedly stressed that the R&AW should not become just another police organisation, but should draw talent from wherever it could be found, including from other services of the Government of India.[45]

Initially, the in-house slotting of IPS officers from within IB, the parent body, was undertaken partly on the basis of options and partly through screening. Recruitment

[45] V. Balachandran, Note on Recruitment Policy & other issues: restricted circulation: recorded-Aug,2005: made available on request , for IDSA report

to what would become a new service – the Research & Analysis Service (RAS) - began in 1971. Several lateral entrants got absorbed into this service in the first flush- from 1971 to 1977 -through an elaborate system of written examinations/ personality and psychological tests and interviews.

Detailed service rules were formalised somewhat later - in the mid-80s, during the tenure of G. C. Saxena - which spelt out job requirements and the required personality traits. Rigorous training, including physical toughening in the training institutes of various security forces, was also part of the training regimen, though it was subsequently discontinued. New recruits were also called upon to develop language expertise.

The second phase of direct recruitment began from 1985, through direct examinations and interviews for the first two years and then, from 1987, through the Union Public Service Commission (UPSC). This continued till 1992. Sections of media have strongly contended that many officers among the initial groups of lateral or direct inductees happened to be 'relatives and associates' of police officers, bureaucrats and senior serving or retired defence officers, who happened to be the colleagues of those at the helm in R&AW. These entrants, barring some exceptions, were unable to shed their own insecurities in the earlier phases of their careers, vis-à-vis their IPS colleagues, or hold their own among their peers in the Foreign Service while on cover assignments abroad. The quality was much better in the second phase of recruitment, with the new entrants displaying greater confidence in their own abilities and acquiring expertise over a period of time.

A combination of deputationists from the Police, mainly the IPS, and other Central services as well as direct recruitment through the UPSC continued to be the method of recruitment to R&AW for a fairly long time. However, this practice has suffered from the 'tail-end syndrome' in recent times. Only those at the bottom of the UPSC Combined All India Services entrance exam list, who get allotted to the not so popular, challenging or glamorous civil services, opt for R&AW and are interviewed and personality tested by a Screening Board set up for the purpose. The quality of these candidates has not always been up to the mark. Many of the candidates selected do not join, preferring to remain with the parent service they are already assigned to, instead of opting for further training or language training, which follows selection to the R&AW. The direct recruitments to RAS are understood to have practically been discontinued for the past couple of years, leading to the constant shrinking of the cadre. It would appear that the ultimate demise of the cadre in the course of the next few years due to retirement and other attritions is clearly on the cards now.

The confused cadre management and recruitment policies of R&AW become even clearer from certain reported moves, unique in nature, to directly recruit persons at the level of Deputy Superintendent of Police. It may be mentioned that persons staffing this level of appointments are usually from lower ranks, who move upwards in rank due to their substantial grass-root level experience. They, however, lack the wide vision and the in depth expertise to man senior positions. The composition of R&AW's senior positions is currently

believed to be from among those who came on short term deputation and then stayed on under the 'Permanent Secondment' scheme and/or persons recruited (including from within the department) from various other services/ cadres, apart from those promoted from junior ranks. Presence of personnel at senior positions belonging to a plethora of services and entry levels might further compound man-management problems and increase heartburn and internal tussles.

Recruitment to lower ranks in R&AW was initially an in-house exercise, without any reference to the Staff Selection Board (SSB), or the UPSC. This appeared to have been given up subsequently and such recruitments were channelled through SSB. However, the organisation reverted back to conducting its own examinations by advertising vacancies. Again, the route of recruitments from open market through normal processes of selection through UPSC/SSB has been avoided. How the aptitude of a selected candidate for intelligence work is determined, is not clear. Physical tests seem to have been abandoned for all ranks, nor there appears to be any specific medical fitness standards prescribed for any rank that could help in the selection of physically suitable personnel for future operational and fieldwork requirements of the organisation. The recruitment process at various levels in R&AW is clearly indicative of the nebulous character of policies regarding the organisation's composition and character. It also is indicative of the less than satisfactory functioning of the recruitment procedure followed by the organisation thus far - which requires a deeper analysis. While the underlying principle separating R&AW from IB and setting up a new organisation for external intelligence was to avoid making it just another 'police organisation,' in practice the primacy of the police officers in R&AW has continued unabated, leading to a constant and debilitating tussle between the directly recruited personnel and those on deputation. The loss of morale within the organisation, especially among the former, has been reported off and on in sections of the media and this has also possibly resulted in the low response from new All India Service applicants for joining the organisation.

Intelligence Bureau (IB)

Officers in the IB of the rank of Joint Assistant Director/Assistant Director used to be recruited through a special scheme known as the 'Ear-Marking Scheme (EMS)' from among successful IPS candidates. This was a planned process in which the toppers from amongst the IPS entrants were scrutinised to "earmark" candidates, who were then carefully vetted through an elaborate system of tests and personal interviews. Officers brought in under the scheme were given special pay and usually got faster promotions than their peers in most states. This was seen as an incentive for their tough and unglamorous work and the lack of the official perquisites enjoyed by the uniformed service in the states.[46]

[46] D. C. Nath, op cit.

At a junior level, Assistant Central Intelligence Officers-Grade-II (ACIOs-II) were recruited directly through a rather strict system of written examinations combined with a process of selection based on aptitude tests. The quality of intake was very good in the initial years after independence, with many meritorious double graduates, including Law Graduates making the selection. There were instances, albeit rare, when those who failed to make it as ACIOs later qualified for the IPS. The healthy practice of getting deputationists from the state police at the cutting edge level of Sub-Inspectors, Inspectors or Deputy Superintendents of Police has lapsed. This needs to be revived urgently, especially in larger metropolitan areas as the maintenance of an umbilical chord between field policing and internal security & intelligence work remains vital, particularly for effective counter terrorism tasks.

At both these levels, the old system of selection appears to have been diluted in later years with a concomitant decline in quality. Lack of incentives has contributed to a large number of vacancies. The concept of the central intelligence services being seen as elite organisations of excellence has suffered because of modern day values of perks and pelf so coveted by the uniformed services in states.

Deputation

Deputation slots in the central intelligence agencies have by-and-large remained confined to the IPS and a few other Central or All India Services. The induction of mostly police officers has helped in perpetuating the myth of close link between field policing and intelligence work, especially where domestic or internal security are concerned. However, the requirement of finding appropriate manpower to meet the specialised Science and Technology (S&T) needs or defence services personnel has hardly been met. Dependence on an ageing, depleting cadre of the earlier recruits with an S&T background has not helped. New recruitment, though attempted has not unearthed quality talent and the verification of antecedents takes so long that applicants interviewed and selected leave for better pastures.

The secondment of military personnel to these organisations occurs in fits and starts, and is delayed by the processing routine. The defence services today insist on proper equivalence of rank for serving officers who are spared for deputation to the intelligence agencies. This has become problematic as the old equivalence specified in rules of the Department of Personnel is not acceptable to them. Senior Colonels or Brigadiers do not want to come in as Directors. This has resulted in the induction of officers who are on the verge of retirement, or those who have missed due promotions in their own service cadres. (This aspect is discussed also in Chapter 9).

A more imaginative and well-regulated utilisation of deputation quotas is necessary to improve the quality of intake of defence service officers and experts in S&T, or economic intelligence. A suggestion worth considering in this context is to form a 'brains trust' of authorised personnel in government departments or public sector companies dealing with the electronics, nuclear or bio-technology matters, who could be designated either individually or jointly as

nodal points to whom raw data provided by intelligence agencies could be periodically referred for interpretation or assessment.[47]

Outsourcing

Outsourcing or intelligence contracting is another concept worth considering. An intelligence contractor can be defined as someone who provides analytical or technical support to the intelligence community in exchange for monetary compensation. They include authorised contractors who provide products or services which are not readily available but are relevant for national security. Historically, intelligence contracting is well known and was developed in the West during the two World Wars or even earlier (Pinkerton, Securitas, etc).[48] The Office of Strategic Services in USA used Standard Oil executives to obtain reports on the 'Axis Powers' fuel supplies. Goldman and Sachs were tasked to ferret out measures for funding of resistance groups. Specialists in major universities like Stanford, Berkeley, Columbia and Princeton were contracted to help in crypto-deciphering work. Military intelligence has also turned to private industry in the research and development arena (e.g. Lockheed Martin Advanced Development Projects Unit, etc).

In modern combat scenarios, the use of private enterprise has even extended to the sphere of covert action, as in Afghanistan and Pakistan (DynCorp, Black Water - now XE, Booz, Allen Hamilton, etc). After the unification of Germany, in the 1990s cryptologists who had earlier worked for the East German intelligence service, STASI, were recruited through an indirect process by the setting up of a private company-Rohde & Schwarz SIT Gmbh - who today do advanced cryptology and other connected technical interception work for NATO.[49]

Requisite Reforms

Studying the recruitment processes followed by the intelligence agencies of advanced or economically developed countries can be instructive. They have kept pace with advances in technology and have adopted flexible practices of recruitment not only to upgrade the technical skills of their operatives but to encourage area expertise and language skills.[50] In the UK, recruitment is direct. The element of secrecy has been relaxed somewhat to try and recruit the best young talent available from reputed universities. The intake also accommodates a flexible complement of referrals by university dons of talent banks of bright scholars, who are recruited after a prolonged scrutiny of their personal antecedents, social habits etc. Security

---

[47] K. Santhanam, during discussion with author: 07.01.2011;

[48] Ralph Cohen, "Putting a human & historical face to Intelligence Contracting, *Orbis*', *Foreign Policy Research Institute Journal*, Spring 2010, pp.240

[49] *Der Spiegel* online, 27.09.10

[50] P. K. Upadhyay, op cit

vetting is extremely thorough. Favouritism plays no role in such intakes. There are cases of bright professionally qualified executives from the private sector- in economics, marketing or business management - who have been attracted by the prestige and excitement of a career in intelligence. The CIA similarly absorbs the best talent from universities like Harvard, George Washington, Princeton, Stanford, Columbia and Berkeley. Attracting the best talent for Indian intelligence agencies is the most pressing challenge for the government. Even the FICCI task force report on *National Security and Terrorism* recommended the creation of a specialised cadre for national security management.[51]In India too, murmurs have begun to be heard about the need for 'public-private partnership' in security management.

Ideally, an intelligence agency should be able to pay its personnel well. It should also be able to 'hire and fire' for non-performance, breaking out from the iron cage of bureaucratic rules and safeguards. Promotions would have to be on fast track, ultimately moving from seniority based structure to a merit oriented system. Flexible pay bands could be considered and equivalence with peer groups in other segments and routine government bureaucracies can be dispensed with[52]. However, given the past history of such discretionary recruitment practices in India, on balance, it may be better to opt for a variant of direct recruitment, through an established institution. The UPSC route has the advantage of transparency but seems increasingly unimaginative and inadequate to meet current needs. A modified system could be worked out in consultation with the UPSC and the Department of Personnel, to provide for specially designed parameters entailing an open, written competitive examination for intelligence services, which prescribes specialised papers like current affairs, international relations, history of modern India, nuclear disarmament etc. to be followed by initial screening and selection by the UPSC. Selected candidates could then be sent to a Screening Board established for the purpose of direct recruitment into intelligence agencies like R&AW, which comprises senior representatives from the Ministries of External Affairs/Ministry of Home Affairs, Department of Personnel and the Cabinet Secretariat**.** A representative of UPSC could also be an ex-officio member. These recruitments could be open to those also who are already working in the government in any capacity and in any service, and meet the requisite qualifying standards for employment with intelligence services. Keeping in view the functional requirements of the intelligence agencies, it may be mandatory for the candidates applying for a job at any level to have high level of computer proficiency. Possession of language specialisation and other technical qualifications could be given additional weightage during this screening. The present practice of

[51] FICCI report ibid

[52] Vikram Sood, op cit

recruiting candidates without these special attributes and then training them into them is neither satisfactory nor cost-effective, when persons with such skills can be easily found in the Indian job market. Separate aptitude tests could also be conducted for the shortlisted group of candidates for recruitment to different agencies, factoring in the requirement for the knowledge of additional Indian language/s, or a technical qualification in electronics, or Information Technology.

Three things are necessary to attract the best brains to intelligence organisations: The belief in the academic world that intelligence is merely 'dirty tricks' has to change. In the US, this has been sought to be achieved by introducing the practice of intelligence officers going back to teaching assignments in reputed universities (e.g. Richard Bundi at Harvard, Lincoln Bloomfield at the MIT). In India, hardly any ex-intelligence professional goes to teach, even as guest lecturer. Second, think tanks should be strengthened and promoted. The entire discipline of international studies/international relations has been developed in the United States through think tanks and universities. Intelligence agencies should start interacting with them to expand their capacities,. Thirdly, intelligence agencies should even outsource tasks to think tanks.[53]

ACRs & Career Progression

Annual Confidential Reports (ACRs) usually are the sole yardstick for assessing career progression in most government departments. Intelligence agencies are no exception. However, in the name of operational security, ACRs in intelligence organisations are written in rather general terms and are cloaked in secrecy. As a result, subjectivity often reigns supreme and ACRs are often at variance with the actual work done by the operative. There is a prescribed system of operational evaluation for field operatives, but instances abound wherein these assessments are disregarded or downgraded on other considerations. To obviate this flaw, the restriction on writing of self evaluation in totally bland terms has to be done away with. Instead, there should be a system whereby the ACRs of mid-level and above officers, should be in two parts – a general comments portion and a classified second part that details the actual work done with the comments of the Controlling Officer on the validity or otherwise of the claims made in this self evaluation. Gradings awarded should be communicated. In case of contested evaluations, a review board consisting of three senior officers- either in-house, or in case of more senior posts of the level of Joint/Additional/Special Secretary, even from outside (say the Cabinet Secretary, Foreign Secretary and Home Secretary) could be set up to reduce the impact of subjective assessments on senior appointments.

In an effort to counter stagnation at various levels, the concept of '*in situ* promotion' has recently been introduced, with newly specified yardsticks of

[53] K. Subrahmanyam, Observations at IDSA Round Table, Aug 06,2010

evaluation that are however discriminatory when compared to the prevailing norms for promotion in other services of Government of India at equivalent levels. This, coupled with the fact that deputation officers often earn promotions on the basis of work done by them in their parent departments in an entirely different environment, has led to needless heartburn and loss of morale at fairly senior levels of the intelligence services. This definitely needs to be reviewed to ensure a uniformity of practice and a balance between merit, objectivity and performance over a period of time.

Training

Personnel selected for intelligence services are being inadequately or incorrectly trained and are not being sufficiently groomed in academic and professional disciplines to successfully accomplish assigned tasks. The training curriculum remains archaic and too police-centric, relying on a heavy handed police approach rather than on human interaction. Tradecraft practices have not been adapted sufficiently to include modern technological advances in methods of communication for source running.

Some years ago, a special study was conducted by a senior retired Naval Officer regarding the training methods being used in the R&AW[54]. It recommended a wide-ranging overhaul and modernisation/upgrade of equipment, facilities and mechanisms to upgrade the quality of instructors. It is not known to what extent these recommendations have been implemented.

Though various intelligence agencies follow the Department of Personnel & Administrative Reforms (DP&AR) norms and provide 15 per cent training allowance to instructors, this does not seem to have attracted more competent persons to join the faculty and several posts remain vacant, or filled by persons with average skills. In many cases these slots in training establishments have been used to 'accommodate' either the 'inconvenient persons' or reward the 'favoured ones'. The healthy convention of assigning senior staff - with due weightage given to quality of the selected trainers - for supervising training at various levels has not been consistently followed. As a result, piquant situations develop of not being able to find proper replacements on the superannuation of some seasoned training instructors, or when some of them leave for other assignments. Moreover, there is a need to call in professionals - scientists, computer software and hardware experts - to impart up to date skills in computer hacking, cyber warfare, etc and to associate them integrally as nucleus of the training faculty with a major say in devising and updating curriculum content. These experts could be employed on contract basis after preliminary security vetting, if it is felt that an open door policy is not feasible.

Strategic military intelligence remains one of the important tasks in the charter of

[54] Admiral (Retd) Bangara report, Restricted circulation, not available in open domain

duties of intelligence agencies, yet not enough is being done to impart basic knowledge and skills to general duty officers who are given field assignments for this purpose. They do not know what to look for and where. This has led to faulty, inadequate and at times, misleading intelligence being sent to defence services.

The posting of military instructors in the training institutes becomes crucial in this regard. In the past this requirement was always met but in recent years there has been a dearth of staff or adequate numbers of trainers have not been made available. This has led to a marked deterioration in the quality of training imparted and the skills generated. Field officers engaged in trans-border military intelligence work have been found wanting in targeting proper quality assets and in tasking the narrow band of HUMINT assets available for meeting the needs of intelligence consumers – the defence services – whose needs and tasks keep expanding. Language training capabilities too have deteriorated in recent years. General duty field intelligence officers must be familiar with the language of countries where they will be posted, or the areas where they may have to work. This is especially essential in respect of the major neighbouring countries. Instruction facilities for languages like Chinese, Persian, Pashto and Arabic need to be upgraded. Instructors themselves have to be proficient. Intelligence agencies should not hesitate to utilise the services of experts from the private sector to impart training in these languages. Also, it is very important that career planning and postings take into account the training imparted. Cases abound where language experts end up doing their field assignments at a place where their language skills are wasted!

There could be no justification for truncating the time schedule for running various training programmes. Yet, this is often resorted to in intelligence agencies on the grounds of operational necessity. In the IB, ideally, the training period should be for about two years and include a compulsory attachment of about six months with the police set up in the states.[55] One of the suggestions put forward has been to set-up a common training centre for all intelligence agencies and to train instructors from the states. This recommendation has not found much acceptance among experts in the field.[56]

Leadership at the highest level would be required to implement these changes. Once the nation decides that it needs better intelligence, a case could be made out for an intelligence wing in every major economic department of the government. Once we have that and the broad structure is agreed on, the recruitment, training and the management of career graphs can be left to the concerned departments themselves. The main issue; however is to determine the role and need for intelligence and then build for the future.[57]

---

[55] D. C. Nath, op cit.

[56] S. D. Pradhan, IDSA Round Table, Aug 06, 2010

[57] K. Subrahmanyam, op cit;

Chapter 5

Content of Analysis & Operations

Most modern intelligence organisations in the world make a broad distinction between the 'analysis' and 'operations' functions. Operators collect intelligence while analysts assess its veracity – they have to weigh and sift the input in the light of all other reports. The aim is to give value and arrive, if possible, at a prognosis or trend.

Analysis

Many breaches of national security have occurred in the past and continue to occur today, not for want of intelligence, but because of the faulty analysis of available intelligence and inadequate follow up action thereon, and/or co-ordination of inputs.[58] This is not adequately highlighted in most post mortems of perceived intelligence failures surfacing in the media. Responding to the observations made regarding the Coomar Narain spy case and lack of intelligence specific to the Rubaiya Syed kidnapping in 1990, [59] the doyen of India's external intelligence, R. N. Kao said, "It is not enough either for the IB or the R&AW to send intelligence reports to the government. Someone with adequate experience has to interpret these reports to the government." He also referred to an observation made by late Smt Indira Gandhi earlier that intelligence organisations by themselves "did not see the wood for the trees."[60]

That has been reason enough for some other experienced and perceptive intelligence practitioners to suggest that intelligence reform should primarily focus on 'the improvement of collection, analysis and dissemination of intelligence' and not focus unduly on other related issues like 'recruitment or cadre management'.[61]

All secret intelligence collection, whether it is based on HUMINT or TECHINT, results from the penetration of the adversary's - a neighbouring state or an amorphous non-state actor - system. This collection is usually done by a variety of means – either through physical presence, or if that is not possible for hostile/historical factors, through trans-border or third-country intelligence collection efforts. There is, therefore a flood of inputs from

---

[58] B. Raman, SAAG paper on Intelligence & Counter –Terrorism, dated, 21.04.2004

[59] V. Balachandran, "Intelligible Intelligence", *Times of India*: 21.09.2000

[60] R. N. Kao, D. O. letter dated. 25 September 2000 to Shri V. Balachandran.

[61] R. Nagarajan, Special Secretary (Retd), Cabinet Secretariat, Observations sent to IDSA Task Force: July, 2010

different sources HUMINT or intercepted electronic inputs i.e. TECHINT to the analysis desks in any intelligence agency.

Given the information revolution and Internet communication, open source inputs provide more than 90 per cent of material relevant for any intelligence analysis. Monitoring and collation of Open Source Intelligence (OSINT) therefore becomes vitally important. A good analyst can only perform his function effectively if he can weld together inputs from HUMINT & TECHINT with OSINT without being dishonest to any particular aspect, thus achieving a balance, which is nearest to the truth.

This is a task easier said than done and requires backbreaking hours of sustained diligence, building up one's background on the subject, searching for grain in the chaff, with many mistakes in the course of learning on the job. Experience, area specialisation and the ability to read between the lines count for a great deal in this type of work, particularly in respect of the sensitive 'grey areas' of political or military related value judgments in respect of target countries where penetration of HUMINT is difficult. Yet the analyst is expected to come up with an accurate and timely prognosis of events affecting the security of nations.

Using modern tools of analysis for sifting of intelligence inputs becomes very important. The analyst should be aware of the pros and cons of any intelligence hypothesis. He must try to identify the major causal factors of the event being examined and familiarise himself with strains of divergent or convergent thinking connected to such a hypothesis. He should be able to sort out chronologies or time-lines while analysing an incident or while assessing prospects.

One of the methods used for this is to have a 'decision tree' for any event – which dissects scenarios, shows causal linkages and identifies problems, factors or alternatives. After listing all criteria, the analyst has to, or should assign weightage to likely scenarios and undertake a 'sanity check' of the weightage given. The basic function of analysis – hypothesis testing – involves asking searching questions: who is the source, what is his access (from whom is he claiming to get inputs), what has been his reliability in the past (did it prove correct?) and the overall plausibility of the report.

There are several proven methods of hypothesis testing. These include creating a probability tree, comparing utility of end results, ranking options as well as devil's advocacy or reverse analysis – perceiving a development or outcome not from one's own perspective, but from that of the adversary.

It is very important that this analysis and assessment is undertaken in an independent and unbiased manner, without being affected by the baggage of pre-conceived ideas, conventional wisdom or political compulsions of policy makers, whether these be of the political leadership or the policy making bureaucracy.[62]

[62] Jerome Clauser (2010), "*An introduction to Intelligence Research & Analysis*" Pentagon Press: Washington DC

Training of analysts is therefore very important and these skills and traits, especially of estimative analysis can only be honed after spending long years on the job.

Unfortunately, the pressures of the moment often overwhelm these considerations, especially as more and more analysts are made to feel insecure if they hold on to any threatening inputs pertaining to terrorist actions by non-state actors that may take place. These pressures also lead to intelligence analyses being characterised as suffering from the 'cry-wolf syndrome', if they do not prove to be correct. In sum, the analytical process has to be action oriented and accountability driven.

For these reasons, as the task of an analyst becomes increasingly complex, most modern intelligence agencies in the world are now clearly and completely separating the tasks of intelligence operations and analyses.

Operations

Intelligence operations can be broadly divided into three categories:

i) The 'classical' intelligence collection activity which involves locating and then subverting well placed HUMINT in sensitive areas of the target subject. Such assets, in external intelligence, can provide accurate foreknowledge of that country's security policies, approaches on vital international or bilateral issues impinging on the home country's own national security concerns, data on target country's defence and nuclear potential etc, preferably or ideally with documentary support. Such assets can be difficult to find and still more difficult to sustain. A lot depends on the motivation of such persons – whether it is monetary alone or a combination of monetary and personal or ideological/ emotional/psychological, which may often constitute various strains in the personality of the asset. A lot also depends on the nature of rapport that is struck between such assets and a particular Handling Officer. Often, such assets become problematic when the handler changes. The handling officer has to be continuously aware of and adapt to safety and surveillance environs, while handling such assets. The casualty rate of such assets is high.

ii) The second type of intelligence operation can be described as the 'influence operations'- which involve cultivation of prominent policy formulators in the target country, or society, – to influence, change or continue policies that benefit the home country's larger or long term strategic or national security interests.

Major decisions with regard to this second category of intelligence operations, particularly in the external field, are usually not left to the individual discretion of any one intelligence operative of the agency dealing with such issues. Rather, the main thrust areas of such initiatives or tasks are identified collectively at quite a high level, with even the concerned committee of the cabinet being kept in the loop, if not with regard to the specific nitty-gritty of operational details, then at least in

general terms about the direction of such efforts.

Large sums of money can be involved at this stage and it may sometimes be difficult to quantify results in the short term or have justifiable yardsticks to continuously monitor or review progress in the assigned tasks and in terms of the objectives achieved, or sought to be achieved. This is also the area where major lacuna can occur, requiring mid-term course correction or even a reversal of the operational policy. While initial policy decisions may have been authorised initially at the highest level, qualitative reviews either do not take place at those levels regularly or with sufficient frequency or in the required depth .

iii) Finally, there are 'liaison operations' – which involve relations between intelligence agencies of different countries, facing common security problems or want to share intelligence on issues like terrorism. These too are usually authorised at the highest level of political decision making and are carried out by specifically designated intelligence agencies.

Trans-national intelligence co-operation has three aspects: sharing of intelligence collected independently, making available training facilities to each other and joint operations for collection of intelligence through penetration and for neutralising terrorist organisations identified as common enemies.[63] It would seem that India's success or progress in the last aspect has apparently been rather limited, due partly to political compulsions/parameters and partly, perhaps, due to a conservative or overly cautious operational mindset.

Drift in Operational Work

Operational routine in the above categories tends to get caught up in a 'drift' in most intelligence agencies across the world. This may be because of HUMINT without having a clear, direct or reliable access to the type of information required, both at the at the grass root level, as also at senior levels of intelligence. They may have had access at one time or been proved right on one or two occasions, but since then, they may have fallen out of circulation in the quarters where they enjoyed access and do not presently have the same capacity to cater the required information. Yet they are reluctant to admit this.

Operators in the intelligence community do not often have the honesty to make quick course corrections by either acknowledging their reduced access to the source, and the concomitant reduced value of the output. They find it difficult to discard such assets and tend to pad up flimsy inputs. Their reports then merely serve the purpose of statistically inflating the output. Another reason for this tendency of not discarding sources who are no longer useful is the convention in the intelligence community – that of being able to handle several HUMINT assets and of not wanting to be seen to have closed down a HUMINT operation and dropping of an erstwhile useful source.

The very nature of field operations makes

[63] B. Raman, "Intelligence & Counter Terrorism", *SAAG paper*, April 2004

it necessary that an operative has the same background and in-depth knowledge of the subject as an expert on the analysis desk. He should, in addition know the language of the target area, local customs and social mores and have an understanding of the psychology of the people in target area. Any compromises in this regard make the success of the intelligence collection exercise doubtful. The problem gets compounded due to the inadequate or poor supervision of intelligence collection efforts on the ground by supervisory officers, specifically entrusted with the task of scrutinising the quality of the intelligence production work. Instead of actively guiding and controlling operations, they fail to make a critical assessment of the modalities of intelligence collection or take the tough though unpopular decisions of discarding unproductive assets and curbing wasteful expenditure connected with such operations.

Some very common examples of the abuse of operational practices can be cited here. One is to artfully cloak open source inputs (OSINT) from international publications or local media as source reports based on non-existent HUMINT assets and claim expenses for the reports. Though ease of Internet access has reduced time lags which used to benefit such practices, still, if the officer in the field station is senior and the officer vetting his expenses at the headquarters desk is a junior, chances are that the former may get away with such claims! Some long standing assets who may have done well in the past due to better access at some stage, especially in the information and psy-war operations, continue to send cleverly padded reports that analysts at headquarters would like to receive, or pass on to their political masters, as coming from impeccably reliable and highly paid assets. Over time, this can become a money spinning racket detectable by seasoned analysts at relatively junior levels, who can at best voice their muted suspicions to superiors.

Again, over the years a convention might have developed and persisted – because of inadequate supervision - that a good operator is one who maintains a voluminous data bank of sources and higher source expenditure rather than one who concentrates on good quality and less voluminous reporting. Intelligence experts generally speak of cases where Handling Officers have been found to be not fully committed to improving the quality of output and maintaining an unholy nexus between them, their useless sources, and perhaps even their supervisory or controlling officers. To rid intelligence agencies of this malady, the supervision of production work needs to be taken a lot more seriously and with high ethical standards than is, perhaps, presently the case within most intelligence agencies in India.

Of late another dangerous trend has been underlined in the IB. Because of operational requirements, more or 'better' men are often diverted to 'high-profile' operational tasks to the detriment of the hardcore, basic and unglamorous field intelligence or counter intelligence (CI) work. CI branches get denuded and the quality of CI work suffers.[64]

[64] D. C. Nath, "Thoughts on Intelligence Reform", Paper submitted at IDSA Round Table, Aug 06, 2010

Whether Analyst or Operator

The issue of the overlapping or interchanging of roles of intelligence professionals requires careful deliberation. In the past, intelligence agencies followed a mix of practices wherein the analyst of today could be the operator of tomorrow or vice-versa. Some agencies in India still follow this practice, partly to provide all-round exposure to the intelligence professionals and partly, to alleviate or balance the arduous grind of analysis with the adrenalin rush of operations. The merits of continuing with this practice however are debatable.

Today, the CIA in USA has analysts who perform what is seen as a specialised function. Exposure to the local situation, for which there can be no substitute, is given in diverse ways – either by temporary tours of short duration, or through long term undercover assignments. The British MI-6 or SIS has also reverted to this model now, by establishing the Joint Terrorism Analysis Centre (J-TAC) that has a multi-disciplinary outlook and a manpower deployment profile, wherein analysts have to play a more specialised role, separate from operations. The Butler Committee review (2004) in UK after the Iraq WMD assessment debacle led to the creation of the post of Head of Intelligence Analysis - that has been merged with that of the Chairman, JIC since 2007. The JIC is now supported by a small, specially trained team of analysts. Of particular importance is the alignment of Defence Intelligence Staff (DIS) with the JTAC.[65] In their reports to consumers – Foreign Office, J-TAC or JIC/recently set-up National Security Council, SIS operators send in almost unprocessed inputs, indicating only vaguely from where obtained or commenting in only very general terms about the reliability thereof. Any analysis value or assessment is left to the specialist analysts in these specially designated bodies.

Analysts' vs. Operators

Though the functions of both analysis and operation are equally important, in practice, the analysts tend to get the rough end of the stick while operators get the glitter and perks of the job, which may include 'justifiable' absence from the desk during office hours and large expense accounts which cannot be questioned, or are not generally questioned. As a contrast, apart from the sustained grind, the present day analyst has to cope with the increasingly alarmist nature of source inputs pertaining to terrorism incidents or threats, which require immediate dissemination, with scant time for proper evaluation through established modes of analysis.

High flyers in the intelligence community try to avoid this grind and gravitate towards 'more glamorous' operational desks. This also leads to heartburn among analysts. In the long run though, even among those who project themselves as

[65] British Cabinet Office paper on Improving the Central Intelligence Machinery published in *Journal of Intelligence & National Security;* July 2009

'great operators', it is possible within the intelligence community to separate the chaff from the grain. As stated earlier, it is difficult for the really good operator to completely ignore the tenets of sound analysis or habits of sound analysis such as extensive area/topical reading to assist in his operational work, especially if he is to elicit substantive output from high value assets.

Meaningful intelligence reform in Indian agencies would perforce have to take note of emerging international practices and take a considered or balanced decision on those most suited for Indian conditions.

Source Protection/Welfare of Retired Assets

This brings up the related and important issue of what to do with discarded assets or sources that may have become casualties in hostile territory but may re-surface later, after being incarcerated. This is an area where there is a lot of *adhocism* about how different intelligence organisations in India deal with such assets. This is in sharp contrast with the practice in the West. Both the CIA and SIS/SS have detailed and prescriptive safeguards for dealing with retiring/retired assets or casualties and their families. Indian establishment also needs to devote more attention to this aspect of intelligence reform.

Chapter 6

Technology Upgrade

Intelligence agencies must continuously upgrade their technical capabilities - be it signal intelligence (SIGINT), communications intelligence (COMINT-interception capability), monitoring, cryptology - in both encryption and decryption modes- information sharing mechanisms and creation of databases of security relevant materials which may need to be shared for better coordination with other sister agencies (NATGRID). Personnel in intelligence agencies must also be skilled in these modern technologies.

Delay in Procurement of Modern Equipment

Several lacunae in the procurement and deployment of V-SAT equipment have been detected in the telecommunications sector. Procurement was initially hampered by long procedural delays. It needed to be fast tracked but this has not always been possible due to established government procedures. In-house financial scrutiny has often been more in the nature of a somewhat unhealthy or needless curiosity to learn about the operational utility or applicability of the equipment sought to be purchased, which goes against the 'need to know' principle, especially as some of the operations are of a highly sensitive nature. One way to circumvent this problem would be to follow the 'expression of interest' method, under which companies known to be having the required equipment could be approached to make presentations. This could be in two stages – technical and financial. At the latter stage, a committee could be formed, at an appropriately high level, associating the competent and authorised finance department representative to scrutinise and clear the proposal. Once this 'fast track' approach is adopted there should be no scope for subsequent delays at the processing stage, or at the level of the Internal Financial Advisers. However, there has to be an adequate appreciation of the need for fast tracking of the purchase of technical equipment without sacrificing the norms of financial propriety.

Cryptography

While encryption capabilities were built up, not enough attention was paid to security requirements. Some systems were claimed to be secure enough but when offered for communication use with friendly liaison agencies abroad, were not found to be secure enough or state of the art. The decryption capacity and technical know how of personnel in intelligence agencies are in any case extremely limited. Therefore, there is a need to create in-house

Research & Development facilities in every agency, as also a centralised or dedicated training agency for encryption/decryption work related to intelligence functions.

Manpower & Trainers

Finding appropriate trainers for any such institute is also extremely important. The short term deputation of specialists/ engineers from Ministries/Departments of Telecommunication, Railways (Signals) or Defence (Signals) could be one way to do so. Doubts persist within the intelligence community about the extent to which outsourcing of such tasks to experts – even from reputed institutes of technology etc. - would be worthwhile without them really understanding the concepts and operational contexts of intelligence work. There are successful examples of such specialised or dedicated institutes for intelligence agencies abroad, both in the West and in the erstwhile Soviet bloc countries.

Existing in-house capabilities and quality of manpower are stated to be below par in most of these fields at present. Manpower upgrades are essential. At present, technical field officers are recruited at the level of non-gazetted employees whose pay scales are lower than those of ministerial cadres. As a result, even after considerable investment of time and money on their technical training, they often seek transfer to other general cadres which offer better opportunities for career progression. One solution for this would be to provide fast track promotion avenues to technical staff, so that their careers could advance within a short time span. Such proposals are considered during various cadre reviews in the intelligence agencies, but do not get adequate support from those in authority, perhaps due to the inadequate appreciation of the special constraints under which intelligence agencies have to function. Better qualified recruits can also make a big difference to in house R&D work as well. Direct recruitment of qualified engineers through the UPSC could also be considered, clubbing the additional requirement of 5 or 10 posts at equivalent levels to those of other government departments like Telecom. Personnel taken in through this process could then be given intensive training in intelligence work.

Linguistic capability is another vital qualification for those in technical cadres. They must have more than just a modicum of familiarity with languages/dialects spoken in border and bordering areas – such as Urdu, Bengali, Pashto, Persian, Chinese, Bodo, Assamese, Naga, Manipuri, Kuki, Kashmiri, etc. Training in some of these languages could be imparted just after initial recruitment, but the quality thereof and the expertise acquired by the telecom staff would depend on application as well as learning on the job. Nowadays, standards of capability are being mandatorily linked to career progression for the telecom recruits, but hazards of frequent inter-operability due to any possible shortages of staff remain.

Open Source Information (OSINT)

Any and all information that can be derived from overt collection i.e. published documents, scientific research reports, documents posted on commercial websites – can be useful inputs for desk analysts in intelligence agencies. New information

technologies are today very much part of the information revolution. These may include high resolution satellite imagery, sophisticated search and data-visualisation systems, and multiple language search and translation tools. Also, this vast data bank must be accessed swiftly.

Intelligence agencies in India have only hesitantly started taking steps to enhance their OSINT capabilities. Partly, this is due to mental blocks against the hazards of hacking or intrusion wherein Internet connectivity has been made available too easily. However, a balance is necessary. Today, every area analyst needs timely access to all vernacular publications relevant to the target area as well as any specialised reports or documents which may help in analysing the offensive, defensive or nuclear capabilities of target countries. A case can be made out for centrally provided Internet connectivity but also access to advanced meta search engines like Copernic, Profusion, Lexibot, Ixquick, Dogpile, Metacrawler, Northern Light, Lexis-Nexis etc. Specialised search engines like International Security Network (ISN), Limited Area Search Engine (LASE), FAS & CIAO (Columbia International Affairs Online)-for nuclear research, could also be considered. Analysts will have to be trained in the proper use of search engines- they must familiarise themselves with techniques like needle in the haystack, treasure hunt, fishing or trawling, save and run as well.

NATGRID

Actionable intelligence should be accessible to all law enforcement agencies. Building up a national database of intelligence that allows all agencies to receive crucial real-time intelligence has become an urgent requirement. Some groundwork in this regard has already been completed. Once the system becomes functional, data-mining will become an important tool to establish correlations between information available from immigration authorities, transport bodies, police stations, intelligence agencies, banks, mobile telephone operators etc. The capability of intelligence analysts would thus be enhanced, with better prediction potential.

CYBER WARFARE

The not so uncommon hacking of some of India's sensitive websites should bring the country abreast with the Cyber warfare capabilities of its opponents, particularly the Chinese. The threat has the potential to multiply manifold if we add to this the efforts by terrorist and criminal groups to acquire the capability to hack into various websites to ferret out information, or to plant misinformation. Existing offensive and defensive capabilities of various agencies need to be enhanced, by keeping abreast with the latest technological developments in the connected fields.

Chapter 7

Establishing India's Military Intelligence Needs and Strategy

The use of intelligence by militaries across the world is as old as warfare. No military commander will knowingly or unknowingly risk an operation by leading his rank and file against an enemy, and into a terrain of which he has little or no knowledge. In any conflict situation, it is essential for the military commanders to continuously collect, collate and evaluate all relevant information concerning the enemy and the terrain, as also the military capability and the intent of an adversary to deal with any a hostile military action. This applies not only to times of conventional war or conflict, but also peace-time to deal with myriad sub-conventional and non-traditional military threats that a country faces.

India's security concerns are accentuated both by external and internal factors. The external security threats emanate from China and Pakistan, while the internal security threats involve challenges arising from cross-border terrorism, non-state and trans-national actors, illegal migration, drug trafficking and organized crime. These threats are ever mutating and blurring – particularly the collusive China-Pakistan military nexus and the growing Naxal challenge in the Indian hinterland. This demands adoption of superior intelligence collection, collation and dissemination - both in the military and non-military domain.

The importance and relevance of military intelligence in the Indian context has to be examined at five levels. First, the problem of military intelligence is to be analysed in strategic and tactical terms. Second, the sources of military intelligence have to be identified. Then India's military intelligence needs and strategy in their wider context have to be established. The fourth point concerns the limitations and hurdles in achieving this strategy. And the last point is to consider some of the remedial measures to improve the management of military intelligence.

The Problem of Military Intelligence

Over the decades since India attained independence, there has been a continual pressure and change in the intelligence requirements of the Indian Armed Forces. The general trend has been the broadening of military intelligence needs in terms of geographical space for military commanders-both at the strategic and tactical level. This has primarily resulted from the increase in the range and the power of destruction of weapons, and

secondly from the increase in military mobility. In addition to this extension of the geographical and technological area of interest, there has been a widening of the range of military engagements in which the army might have legitimate intelligence interests. Clearly, and apart from the basic intelligence required about the enemy's whereabouts, intentions, strengths, weapons, state of training and morale, the requirements are gradually extending the military intelligence needs to include, political, economic, manpower, research and development, industrial, communications and other matters relating to the potential adversary. This extension of the range and breadth of the country's military intelligence needs today even impinges upon or overlaps into the domain of foreign policy. In other words, there is likely to be increased dependence on strategic intelligence in the future.

Establishing Military Intelligence Needs

Military intelligence needs are only likely to grow rather than diminish in the future. Not only will they have to cover the extended range of future weapon systems and equipment but will also have to cover the possibility of local conflicts, conventional war, as well as terrorism and other subversive threats. According to Services' experts, particularly from the Army, at the tactical level, military commanders in the field will still need their own eyes and ears, and perhaps to a greater extent than at present. Thus to prevent duplication and simplify the inter-communication of intelligence between the armed forces because of overlapping of the intelligence interests; the collation and dissemination of strategic intelligence could increasingly be carried out by a joint services organisation.

In this connection, three important aspects of the issue are as follows:

Sources:

In peace time, the problems of military intelligence collection are very different from those during war, but in both cases there is likely to be greater reliance on technical (TECHINT) rather than human intelligence (HUMINT). This trend is obvious and will undoubtedly continue in times to come. However the information sought will become progressively more difficult to obtain, as methods of electronic and spectral camouflage and deception evolve to keep pace with the new ways of gathering military intelligence. TECHINT is inherently more reliable, the intelligence provided is more current and measurable, and there are no problems of communication. It does without the dependence on human resources and to commit them to situations that can be dangerous. With advancements in the field of electronics, more sophisticated means of eavesdropping on the plans of potentially hostile countries will follow rapidly. This will entail keeping ahead in the field of military specific technical intelligence methods and devices. Fewer systems will be in active mode, and those active will be so for even briefer periods of time, thus making interception and deception more difficult.

This is not to say that HUMINT will lose all its relevance in the future. Even in the case of the hunting down of Osama bin-Laden by US commandos, the very substantial technical inputs could not have ensured the success of the mission, without

key and crucial inputs provided by traditional human sources. The temptation to totally replace HUMINT resources with TECHINT will have to be resisted since there are still situations where human agents can be invaluable. For instance, in sub-conventional threats such as rural insurgencies and Naxalism, quality penetration by human intelligence can be crucial. HUMINT will continue to be a cost effective means of gathering military intelligence, specifically where technology cannot penetrate or simply cannot decode the complexity of the intelligence problem. There will continue to be a place for human agents in the overall context where selectivity and judgment are required.

Peacetime needs:

In peacetime, it is probable that the future will see further increases in the quantity and quality of military intelligence from technical sources due improvement in sensor based collection devices; computer based analytical tools and electronic dissemination. The security of computer systems will, however, be the weak link. This will be true for the adversary as well. Emissions in the electromagnetic spectrum, open broadcast policy, and as sound waves, vibrations and radiations sensed or monitored in the active and passive mode today are important sources of technological intelligence.

At yet another level, the peace time military intelligence gathering will have to increasingly rely on open source information or intelligence (OSINT). This includes vast OSINT resources in the form of international, national and regional press, electronic media, defence periodicals, literature from the original equipment manufacturers, government publications and Internet resources. The open skies policy adopted by several countries with regard to their continental and maritime mapping initiatives provides mind boggling imagery related data and intelligence (IMINT).

War time needs:

In war time or situations of localised military conflict, HUMINT will remain important, especially for operating behind the enemy lines, identification of enemy units, troop movement and equipment, and obtaining documents of operational relevance. Most intelligence during localised conflicts will come through captured documents, interrogation reports, maps etc. In addition, there will be a wide range of all weather military sensors and surveillance equipment that will open up on the battlefield on outbreak of hostilities. This will enhance the peacetime HUMINT and TECHINT capabilities on the battlefield. In other words, there will obviously be a requirement for both strategic and tactical intelligence in times of war, regardless of the type and duration. Collation and dissemination of strategic intelligence has increasingly become a tri-service affair, whose output will percolate down to the tactical level through computer based secure communications and information management systems.

At yet another level, initial and replacement costs of the technical means of collection can be high. Information and communications systems are required for analysis and dissemination. All these systems require highly skilled manpower to design them, to man them, and to maintain them. Security of these systems

adds to the technical and operating costs. Some of these devices are extremely vulnerable to direct or indirect attacks. Even if a fully effective strategic defence were to prove feasible, the eternal security dilemma of attack and defence will ensure that means of countering, deceiving or destroying will necessitate the development and deployment of counter measures.

The future of counter-intelligence is very closely tied to the technical developments in the field of intelligence collection, collation and dissemination. Developments in technology will play a great role in the acquisition of counter-intelligence information through passive electronic, or optronic devices and active audio surveillance devices.

Evolving Military Intelligence Strategy

India occupies a predominant geo-strategic position in South Asia. Some analysts argue that, while India's location makes eminent geographic sense, its natural boundaries are vulnerable and prone to conflict. The country shares land borders with six countries. Against this backdrop, India's critical security challenges and threats that drive military intelligence needs can be discussed at five broad levels:

Border Security:

The long and porous land borders present a significant security challenge. The multiple security agencies deployed along India's extensive land borders compound the security issue. Issues of uneven operational control and organisational efficacy over time have led to gaps in intelligence gathering and dissemination. Experience shows that gaps in border security have exacerbated insurgencies and have created additional problems like illegal migration, entry of political asylum seekers and the movement of terrorist groups. Similarly, sporadic Chinese incursions continue despite the many confidence-building measures undertaken. In the west, infiltration by Pakistan-abetted terrorist groups and border violations continues. Surveillance across and along the borders by utilising HUMINT and TECHINT therefore becomes important.

Internal Security:

In recent times, the menace of left wing extremism has been characterised as the single biggest internal challenge faced by India. At yet another level, the scourge of Pakistan sponsored militancy in Kashmir, which though substantially reduced, is still a cause for concern. Maintaining large counter insurgency forces will require appropriate military intelligence structures to generate local information wherever and whenever military forces are employed. Here Indian armed forces have to make the painful choice between the conventional and sub-conventional military intelligence needs because of its future internal security commitments.

External Security:

While an all out war with China and Pakistan is somewhat unlikely, given its political costs and dangers, the obsolescence of the concept of a limited war is not assured. So how India manages its military intelligence needs to successfully implement a fast paced

limited war will be important. It will require, besides new technologies, doctrines and concepts of operation, enormous amounts of investment in military intelligence. Another aspect affecting military intelligence planning will pertain to the acquisition of nuclear capabilities in the neighbourhood. It is imperative to have a clear appreciation of the Chinese and Pakistani nuclear doctrines and their arsenals in order to fashion a sound military strategy and capability.

The disruptive potential of technologies such as nanotechnology, biotechnology, and information technology, if used by our adversaries with malicious intent is also a matter of concern. Clearly, the possession and impact of such technologies by trans-national and non-state actors could also seriously hamper national security. Effective military security against such external threats will demand heavy investments and building up both HUMINT and TECHINT resources.

Maritime Security:

The Indian Ocean Region is critical to the country's security in terms of trade, energy needs, protection of island territories and exploitation of the EEZ. This strategically significant oceanic region characterised by narrow navigational channels to its east and west can be easily interdicted or disrupted. The littoral spread too, is critical for the smooth flow of oil, raw materials and trade for several countries. The need to evolve comprehensive security and intelligence gathering measures for protection of India's exclusive zone, island territories, deep sea mining zones and littorals will assume greater importance in the future. In this regard, the military intelligence units of the navy and air force, especially their TECHINT resources, can be expected to play an important role. How these responsibilities are to be fulfilled by the Coast Guard and the Indian Navy, and what should be the mechanism for coordination or division of responsibilities between them needs to be clearly spelt out.

Regional Security:

If India aspires to become a power of some consequence, it has to become a net provider of regional security in the sub-continental context, and even beyond. This might involve a developed capacity to deal with natural disasters, threats to or overthrow of friendly, legitimate governments, civil strife, illegal migration, organised crime, trans-national terrorism, and occupation of island territories, blockade of sea routes or channels, and countering the illegal exploitation of the exclusive economic zone. Once the military intelligence needs for the foreseeable future are identified, there will also be a need to formulate a broad approach to collect, collate and communicate these strategic and tactical intelligence needs down to the appropriate levels of military command with clarity.

The process of collection, collation and dissemination of intelligence to meet the military's operational needs brings to fore the question of the shape and structure of civilian and military intelligence agencies, their capacity to perform in a rapidly altering geo-strategic environment and the gaps and deficiencies in inter-agency coordination. Currently there seems to be an apparent and serious dissatisfaction within the military directorates about the

availability, quality and timeliness of the intelligence inputs received from the premier civilian intelligence agencies of the country. Their ability to provide military grade or specific strategic and tactical intelligence of significance is rather limited, and this in turn, drives the much-reported friction between the "collector" and "consumer" of intelligence. Though some remedial measures have been taken in recent years, there still remains a considerable disconnect between the civilian and military intelligence agencies Besides, there also remain several structural and systemic deficiencies within the military intelligence directorates and units of the three services. These primarily pertain to the quality and competence of the military intelligence staff and the incentives to perform.

DIA - An inadequate mandate?

The military intelligence needs of three services in the emerging context can be stratified at three levels namely: the broad security or operating scenarios for the military in the foreseeable future; the intelligence tools required to meet the intelligence challenge and the efficacious intelligence production. The following tabulation attempts to contextualise the broad strategy for fulfilling the military intelligence needs of the future:

Strategising Military Intelligence Needs

Military Scenario (s)	Central Agencies	DIA	MI	Remarks
Border	POLINT TECHINT OSINT	TECHINT HUMINT IMINT	HUMINT TACINT*	* refers to the technical resources organic to each military service.
Internal	POLINT TECHINT OSINT	TECHINT IMINT	HUMINT TACINT*	POLINT and HUMINT will be the principal drivers.
External	POLINT TECHINT OSINT	TECHINT HUMINT IMINT OSINT	HUMINT TACINT*	POLINT, TECHINT and IMINT will be the principal drivers.
Maritime	POLINT OSINT	TECHINT IMINT OSINT	TECHINT IMINT HUMINT	HUMINT shall play a limited role.
Regional interventions	POLINT TECHINT OSINT	TECHINT IMINT OSINT	-	POLINT and IMINT will be the principal drivers.

The above analysis highlights two important issues. First, the focus of military intelligence collection and collation, due to the nature of military engagements in the future, will have to gradually shift from the service specific military intelligence directorates to the Defence Intelligence Agency (DIA). There is some evidence that such a shift is already taking place but greater organisational clarity is required regarding the division of work between these agencies. Secondly, the increased involvement of the three military services in benign but non-traditional and trans-continental roles will require that specific aspects of external military and strategic intelligence resources be either accessible or directly placed under the charge of the DIA and the military intelligence directorates. For instance, military interventions overseas in the form of peacekeeping missions, disaster relief etc would demand more than the routine technical or tactical intelligence. In this context, the collection and collation of localised POLINT might become equally important for the armed forces in the designated area of operations.

Limitations and Hurdles

Rigidity has been the hallmark of India's intelligence agencies – both civilian and military. This is the absolute antithesis of the desired core competence of "imagination" and "unconventional-ism" in the field of intelligence. In India, the evolution of the intelligence agencies has suffered particularly because of the lack of cross-cultural talent or cross-pollination among civilian intelligence agencies. This is partly reflected also within the military intelligence community. The inadequacy of field footprints and technological know-how and capacity has been the bane of the intelligence community. Most importantly, the external intelligence system is focussed more on political content, and less on military intelligence aspects. On the other hand, the military intelligence functions are confined to the services but have little authority to operate beyond tactical horizons. This lack of coordination contributed to three gravest intelligence failures in independent India: the 1962 war with China, the ill-conceived intervention in Sri Lanka, and the limited Pakistani incursion in the Kargil sector. There is yet another important inter-organisational problem - that of mutual distrust between the civilian and military intelligence agencies. The civilian intelligence agencies seldom take the military intelligence agencies seriously. Consequently, there is no forum for military intelligence to present its assessments to the highest authority except when crises are imminent. By which time, the damage may have already been done. Though there have been significant attempts to address this problem post the 26/11 Mumbai terror attacks, the intelligence flow is predominantly one way. The military makes an intelligence demand, and the intelligence agencies often supply it without duly confirming its relevance and validity in the given operational context. Although the civilian agencies purport to supply strategic intelligence, the inputs delivered seldom fit the bill or are merely operational in nature. Therefore, many military experts feel that the military too needs to invest in strategic intelligence gathering, collation and analysis so as to arrive at a correct estimation of enemy's intent and capacity. There, however, is no attempt to explain

how this military intelligence structure would avoid the pitfalls bedevilling its civilian counterpart. Or, why military intelligence is equally at sea in providing hard and actionable inputs in disturbed areas, such as J&K and the Northeast, etc.

While the shortcomings discussed above pertain to both civilian and military intelligence agencies, the following section specifically examines the limitations and hurdles that hamper the military's intelligence needs and strategy at the three levels of structure; capability and coordination.

- **Structure:** The establishment of the DIA under HQ Integrated Defence Staff set the pace for integration of military intelligence needs of the three services. While the DIA is gradually emerging as the nodal intelligence coordination agency among the military services, the primacy of service specific military intelligence directorates still holds. With the SIGINT, HUMINT (Defence Attaches only) and IMINT resources now placed under the DIA, the collection, collation and dissemination of these aspects of military intelligence has been partly centralised. A major part of HUMINT and counter-intelligence resources on the other hand remain with the military intelligence directorates of the three services.

There might be a case to allocate a larger role and resource to the DIA in the context of CYBERINT and HUMINT related operations. Today, cyber based capabilities in the neighbourhood have discernable military components. Therefore, this aspect might need the specific indulgence of the military vis-à-vis civilian intelligence agencies, given the domain expertise of the former. In the foreseeable future, pursuit of out of area contingency tasks by the military might require the placing of select HUMINT resources at the disposal of the DIA to acquire strategic intelligence.

- **Capacity:** In terms of capacity, the DIA and the military intelligence directorates suffer from several qualitative and quantitative deficiencies. The recruitment, training, and calibre of the intelligence staff, ranging from officer down to the non-commissioned levels requires a serious re-think in terms of their technical qualifications. A military intelligence operative today needs to have a fine balance of qualities that span geographical, political, economic, cultural, sociological, and technical knowledge to perform the assigned strategic and tactical intelligence tasks.

Language skills, area and technical expertise will be an important qualification for military intelligence staff in the future. The knowledge of advanced information and communication systems will be equally important to handle military intelligence related collection, collation and dissemination tasks. Data mining in the open source Internet domains (OSINT) will be an added requirement for military intelligence practitioners and analysts in the future.

- **Coordination:** There are several gaps and deficiencies in inter-agency coordination that need to be addressed. These are essentially at two levels - inter-service and inter-agency. Among the services, the three military intelligence directorates of the Army, Navy and Air Force still act as the

principal field or tactical intelligence collection agencies (barring SIGINT and IMINT- handled by DIA). Furthermore, these military intelligence directorates differ in size, role and structure, and are extremely stove-piped – even when it comes to sharing information between themselves. Though the establishment of DIA has facilitated the exchange of information among the three services, the problem of inter-service coordination still persists. A more critical problem is that of the inter-agency coordination -between the DIA, IB and R&AW. Turf issues invariably crop up and have a tendency to turn prickly. As of now the basic differences essentially stem from two issues: recognising or accepting the Army's role and resources in collecting and generating strategic intelligence; and the precise status of the DIA and the three MI Directorates in the hierarchy of other national intelligence agencies. Till these issues are resolved, the inter-agency coordination dilemmas will persist. Militaries of today are far different from those of yester years in terms of their fighting capabilities, organisational capacity and strategic reach. For instance, an aircraft carrier tasked to undertake a relief mission in response to a catastrophic natural disaster several hundred miles away cannot be expected to operate without dedicated strategic intelligence resources. Similarly, an army's field formations deployed on peace keeping mission or in conflict stabilisation operations far away cannot be expected to perform effectively if it is not suitably equipped with strategic intelligence resources.

It is apparent that the military today seeks an enhancement in its capability to generate strategic (only requisite) and tactical intelligence required to meet the myriad security challenges and threats of the future. Given the intelligence mandate, resources and capacities at its disposal, the Indian Armed Forces feel constrained in terms of military planning and future development. Specifically, they seek a share in external military intelligence (strategic) resources, both in terms of HUMINT and TECHINT.

While HUMINT needs can be separately explicated, the importance of military specific IMINT and CYBERINT resources (as subsets of TECHINT) have a greater relevance for tactical intelligence. Imagery and cyber technologies greatly influence military planning and execution on a modern day battlefield, and hence the operational necessity of launching defence satellites.

It might be prudent to draw a lesson from the United States in this regard, where the three technical agencies namely the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA) are the important technical intelligence gathering components under the Department of Defence. The Intelligence Reforms and Terrorism Prevention Act promulgated post 9/11 in 2004 was consciously retained by the DoD despite several reservations expressed by the office of the Director of Central Intelligence (now DNI) and other intelligence organisations.

Remedial Measures

Remedial measures can be taken with regard to role, structure, capacity, culture and accountability.

- **Role:** Security itself is seen in an all encompassing national construct with political, social, cultural, economic and territorial dimensions; intelligence gathering too needs to be seen as a construct of "national security intelligence" rather than as two distinct domains of "strategic" and "tactical" intelligence. The role and charter of civilian and military intelligence agencies must undergo a corresponding change. National security intelligence is eventually to be seen as the accumulation of complementing information (i.e. emanating from various sources), process (i.e. intelligence cycle), missions or tasks (collection and collation, or analysis and dissemination, and/or counter-intelligence) and organizations (comprising R&AW, IB, NTRO, DIA, MI etc). The context of military intelligence needs and strategy will have to be defined in the context of "national security intelligence", no more or no less.
- **Structure**: The structural imbalance between intelligence agencies is at present rather acute. Given the role of the armed forces in guaranteeing security against internal and external security threats, the significance attached to military intelligence in the national context is rather low. Civilian intelligence agencies, over time, may have managed to monopolise the business of intelligence gathering, collation and dissemination, so much so that they have tended to become both the "producers" and "policy makers" of intelligence. Over-reliance for intelligence needs even at the tactical level on civilian intelligence agencies compounds the problem. Consequently the ability of the armed forces to formulate military strategy and generate options in times of crises is constrained. Military intelligence therefore needs to be vested with requisite capability and authority to generate military grade strategic and tactical intelligence.
- **Capacity:** security intelligence needs are simply too vast to be met by any single agency. However, new technologies and practices have made this task easier. Today a wide range of intelligence gathering tools ranging from HUMINT, to OSINT, to several forms of TECHINT such as SIGINT, COMINT, ELINT, MASINT and IMINT are available. The sheer volume of TECHINT compared to HUMINT poses a problem. The ability, or inability, of the intelligence agencies to process these large volumes of information raises the question of capacity and competence. Clearly this is lacking because of uneven division of intelligence work, particularly the inadequacies in the handling of external military intelligence by the civilian intelligence agencies. Besides, what was deemed as strategic intelligence a few years ago is relevant today for planning intelligence at the tactical level as well. This implies that a substantial amount of strategic intelligence related resources and processes can be transferred to the military. A capacity related issue that

assumes significant importance in the military context is the allocation of advanced IMINT and CYBERINT technologies. The sooner this need is addressed the better. However, a related issue that will have to be resolved concerns the inter-relation between the NTRO and the MI's various wings and the overlaps and redundancies.

- **Institutional culture/ recruitment, deputation policies**: The need for close coordination among intelligence agencies cannot be stressed enough. The oft repeated "need to know" dictum of intelligence perhaps now needs to give way to the "need to share" principle. This alone can foster better cooperation. Collectively attending training courses of professional interest could pave the way for institutional bonding and camaraderie.

Defence services need to take due care while selecting and posting candidates on deputation to civilian intelligence agencies. This aspect has significantly suffered in recent years and needs to be righted by the personnel directorates of the three services. The civilian intelligence agencies too on their part must be willing to accept military intelligence personnel with proper equivalence of rank and seniority. In the old days, deputation and the posting of officers from the defence forces to intelligence agencies used to be much simpler and an easy flow of traffic was maintained. Most of the officers so selected were from the military intelligence stream and had field exposure, experience in trans-border intelligence collection work, at least relating to tactical intelligence. Over time, however, due partly to long or specialised tenures for the officers so deputed - at the request of the intelligence services - it was felt that these officers were being lost to the parent defence organisation, both in terms of the parent arm professional expertise and intelligence specialisation. If there was a regular turnover of officers from the services to the intelligence agencies, this problem could have been obviated. However, the requirement or aspiration for foreign assignments under intelligence organisational cover, to which the deputed defence officer could justifiably aspire, with concomitant financial benefits, interfered with his career advancement in the parent service.

Defence officers even now voice the view – that the deputed personnel should get adequate opportunities for assignments abroad. They have been given such opportunities within the external intelligence organisation, though not in a consistent manner. For instance, some times the defence officers have been deputed to a domestic trans-border field stint in the intelligence set up, which they have been reluctant to take on, for family constraints and also the comparative lack of creature comforts and the anonymity that such postings entail.

The policy of the regular inflow and outflow of defence officers in intelligence agencies deserves a close and urgent re-look, especially if strategic intelligence needs have to be met by the external intelligence organisation. The problem of equivalence of rank needs to be tackled head on. Military experts feel that if an Army Colonel or Brigadier, or officers from the Navy and the Air Force of similar seniority is reluctant, or deem it a humiliation to join the intelligence set up

as Under Secretary/Deputy Secretaries/ Directors, where even promotee field officers directly recruited from the Grade 'B' intelligence cadre are serving as Directors, then there is a justifiable case to ensure a flexibility in the ranking and the perquisites offered to the particular deputationist. This argument shuts the eye to the fact that the criterion for career progression in the armed forces and the civilian intelligence agencies are different and equating oranges with apples is not going to solve the problem. It is also argued that perhaps a fixed initial tenure of four years could be agreed upon for defence service officers going on deputation to a civilian intelligence agency, within which time frame a very deserving or especially proficient officer could even be given a foreign assignment. Obviously, this argument also does not go into, or considers the nitty-gritty of the process through which a person could be getting selected for a foreign assignment and considers such assignments to be one of the 'advantages' of service and an integral part of the service conditions of services officers' deputation to a civilian intelligence agency.

Perhaps, a better alternative could be the reversion of a defence service officer to his parent service as per prior commitment, with the proviso that an officer with intelligence expertise could return to the organisation at a later date, after picking up his rank and performing the required professional stint within his service. However, this could seem like the 'Permanent Secondment' policy for police officers to central intelligence services, which is creating more problems than offering solutions, by way of inter-se seniority, promotions etc, vis-à-vis their 'son-of-the-soil' colleagues.

Surely, imaginative policies could be framed to ameliorate promotion bottlenecks and overcome rigid structures and mindsets.

DNI – A POLITICAL APPOINTEE?

A sizeable section of young and middle level serving officers in the defence forces have begun to believe that the answer may lie in simply empowering the DIA to deploy suitable resources for analysing foreign military developments - particularly in China and Pakistan. They believe external, strategic military intelligence has to be brought under the charter of the DIA. Concomitantly, some of them even espouse a rather radical view that civilian and military intelligence agencies need to be placed under a Director of National Intelligence (DNI), who would be fully aware of security matters, have first hand and in depth knowledge of security issues and an articulate political person rather than an intelligence professional to avoid the 'stove-piping' of intelligence inputs to decision makers at the highest level. However, such a viewpoint may be somewhat radical or even flawed. Just because intelligence agencies may not be performing their job well enough – as regards military or external strategic intelligence – is not a sufficient reason to so empower the DIA, or create an entire intelligence collection edifice under the services headquarters, which may then be in danger of becoming a colossal behemoth without adequate expertise. Let us take the example of Pakistan. Has the creation of the mammoth Inter Services Intelligence (ISI) by emasculating civilian intelligence

agencies ensured that Pakistan has effective intelligence to deal with its internal security problems? Has it managed to penetrate and influence the Tehriq-e-Taliban Pakistan (TTP) till date? The ISI used its powers and reach to create various jihadi networks as an extension of its military policies and doctrines of fomenting trouble in Afghanistan and India. The jihadi networks willingly cooperated with it at that point of time, making the ISI gloat over its successes. However, when the goals shifted, ISI is all at sea in dealing with either these groups or their plans. Whatever reform is undertaken in this regard would have to be carefully thought out after a careful weighing of all options.

Chapter 8

External Intelligence – Relations with Ministry of External Affairs

When modern states were in their infancy, their foreign policies were often an amalgam of diplomacy, espionage and covert action. Only gradually did the boundaries and distinctions between the two emerge, but the links between them remained crucial.

The 1815 Treaty of Vienna codified some guidelines in this regard; terming any interference in the internal affairs of another country to be unwarranted, and condemning espionage. In 1876, Etienne de Condillac in his *Dictionnaire des Synonymes* defined an Ambassador as, " a man sent to a court, first to represent his country with pomp and splendour, then to deal with problems should they arise, and third, to give an account of what he observes…" Other rules and customs were codified at the 1961 Vienna Convention on Diplomatic Relations.[66] It is acknowledged that a diplomat's job includes "ascertaining by all lawful means conditions and developments within the receiving state, and reporting thereon to the government of the sending state".

After the 1815 Vienna Treaty proscription, intelligence services had to become more professional and the differences between intelligence and diplomacy in terms of norms, objectives, means and methods gradually crystallised.[67] Intelligence services realised they had to obtain information, but in their own particular way. Intelligence had to focus on what was either inaccessible or accessible only with difficulty to the diplomat. This could extend to the hidden face of powers and people, concealed intentions and the anticipation of threats before they materialised. Intelligence thus has to cover the full gamut of security issues in the modern world- terrorism, proliferation, trafficking, trans-national crime etc.

One of the fundamental distinctions -now commonly accepted- is that although both deal with international affairs, they do not

---

[66] Pascal Teixeira, Director of Strategy, DGSE, France, "*Diplomacy & Intelligence*: *Mondes*", Journal of the French Foreign Office, Winter 2010; pp122

[67] John D. Stempel, "Intelligence, Covert Action and Ethics: Oxymoron or Necessity", ISA Conference, March, 2008

have access to the same type of information. They acquire information through different means. This difference in operating methods often leads to irritation and raises suspicions about each other's activities. Diplomats often do not take kindly to covert activities, fearing that these may adversely damage their countries' relations with important allies or enemies. Intelligence officers on the other hand believe that diplomats are sometimes too diffident or nervous about taking steps that could benefit a nation's security and vital national interests.

The 1961 Vienna Convention highlights that diplomacy is a matter of representation, negotiation and development of bilateral relations. These are not intelligence tasks. However, in order to negotiate successfully, diplomats may need to anticipate the strategies and intentions of the other parties, and intelligence may help them to do this better. Intelligence serves not only diplomacy but also the military and national policy makers in the context of internal security

"Intelligence diplomacy" also exists in the form of liaison between intelligence services of friendly, or sometimes, even not so friendly countries. These relations are part of a wider set of bilateral relations which usually the foreign ministries of both the liaising countries are aware of and may themselves have initiated or sanctioned.[68]

Cooperation between the Foreign Service and external intelligence, which is vital and essential, can be examined from a four point perspective:

i) Information: the role of intelligence in understanding and anticipating problems;

ii) Action: intelligence in support of diplomatic activity;

iii) Protection: intelligence that ensures the security of diplomats and citizens;

iv) Influence: intelligence in public, bilateral and multi-lateral diplomacy;[69]

An intelligence service's areas of interest and activity naturally overlap the geographical and thematic territory covered by the Foreign Service. In order not to tread on each other's toes and maximize complementarities, some measures may be needed to be taken. First, at a strategic level, both must identify the areas where intelligence is required. Most countries nowadays specify or codify these tasks at a fairly high level - in the national intelligence council or in a core committee consisting of the National Security Adviser, Foreign Secretary and other co-opted special dignitaries/officials. Some states formulate their national intelligence plan annually.

Within this framework, the demands of diplomats and others have to be matched with supply from intelligence services.

[68] Teixeira, Op cit.

[69] Teixeira, op cit.

These needs have to be identified, updated or modified through the constant or ongoing mechanism of dialogue. These needs could range from the macro to the micro: the security situation in a conflict zone; the threat of terrorism in general or in any particular country or part of it; identifying the decision making channels or centres within the country; the actors involved in destabilising activities; as also issues like the personality traits of important foreign dignitaries; their integrity profiles, foibles or weaknesses, which could be exploited; intentions of a protagonist at any given moment in time and factors which could influence or change these attitudes etc. Diplomats can and should call for data from intelligence units on historical aspects i.e. to find old or forgotten connections between actors and events. Intelligence services have the advantage of long memories. Feedback from diplomats on the inputs being supplied by the intelligence service is crucial and must be given freely and in a constructive rather than in an overly critical manner.

Intelligence is essential but its purpose must be to inform action. It has a broader range of applications in the context of modern day threats. For instance, intelligence could open up channels of communication with non-state actors, with whom it might be difficult for diplomats to associate officially. At any time, it may be useful for foreign policy decision makers not only to know what is really going on in a semi-clandestine politico-military movement, but also to be able to communicate with the movement discreetly, if necessary. Of course, the parameters of who should be doing what, have to be very clearly laid down by the nation's top policy makers so that no conflicts occur at the local level and lines of communication do not get crossed. The intelligence service operatives in the field must know how far they can or should pursue this type of contact and the element of risk it entails- both for the service and the country's diplomats. In some cases, secret communication channels can successfully lay the groundwork for diplomacy, once the conditions are right for diplomats to take over.

In the related sphere of nuclear proliferation, the intelligence community's nuanced understanding of the different actors in the host nation's proliferation programme and operating methods could prove useful, not only for formulating policy on sanctions etc., but also to reduce or prevent illicit activities. Recently, Iran's covert nuclear facility at Qom was detected by an intelligence operative. Diplomats then alerted their national policy makers and partner countries. Information was shared both through diplomatic and intelligence channels.

In the fight against terrorism, a comprehensive diplomatic strategy should include a security dialogue with the affected countries. The capacity of the diplomatic establishment to design and implement such strategies would depend on their analysis of crucial intelligence inputs relating to the attitudes of local actors, terrorist groups, the fringe elements in the community with pro-terrorist sympathies and the likely response of the political and security authorities of the host country.

During important negotiations with the host country, diplomats need to get timely information about the intentions and the

attitude and/or flexibility of the negotiating parties and here too intelligence must provide the inputs that the diplomat cannot legally obtain for himself. Sometimes, this interaction may raise issues of responsibility- whereas diplomats must constantly explain or justify themselves, intelligence operatives are not obliged to do so even when mistakes are made, as they do not carry the burden of decision making. It is not their duty to build up political support for any policy that is being determined. In fact, good intelligence should highlight the costs and dangers implicit in such policy.[70]

Intelligence can continue to contribute only if diplomats absorb or understand the pitfalls and limitations of operations. Otherwise, intelligence operatives may tend to remain silent, in order to protect their sources and operating methods. Secondly, in many cases, time is of the essence. Intelligence delayed may become intelligence wasted. The long term focus of national policy objectives or interests may have to give way to the short term necessities of crisis management.

Diplomatic services remain exposed to espionage by host country's agencies. Some of these threats are not new but terrorism against diplomatic agents has emerged as a new feature. Here too, intelligence services play a vital role – to prevent and to provide assessments of such threats, or those that are likely to develop in the country of assignment. Intelligence can raise timely alarms about imminent threats to premises and personnel of diplomatic legations. Intelligence officials can, and do play a part, in tackling crisis situations.

Influence control has become a fundamental aspect of diplomacy. Intelligence services can be called upon to detect disinformation and manipulation in the host country's media. At a more conventional level, they do participate in bilateral influence diplomacy, which may partially be conducted through liaison channels.

Despite these philosophical or theoretical foundations postulating constructive cooperation and inter-dependence between diplomats and intelligence officers in a legation abroad, what should be a symbiotic relationship degenerates into estrangement and several practical issues make the relationship abrasive, leading to erosion of trust.

Despite their efforts to adapt and change, most foreign intelligence agencies continue to follow the World War II model. They were meant for supplementing their foreign offices, and were to adopt a similar culture and outlook, for undertaking intrusive and at times coercive diplomacy. They succeeded to a greater or lesser extent, depending on how well the operational, protocol or other related constraints could be managed. They operated largely out of the safe sanctuary of their embassies, using the conventional tools of intelligence such as cut outs, drop boxes (DLBs) and 'cover' meetings. Liaison contacts and TECHINT also

---

[70] Robert Jervis (2010), "Why Intelligence & Policymakers clash, *Political Science Quarterly*, summer, Vol. 125(2), pp. 187-196

helped. All this may have changed with the onset of terrorism and globalisation, whereby the origins of security or strategic threats have moved away from the domain of normal diplomatic life.[71]

The Cover Job

The first point of potential conflict lies in what sort of cover job is assigned to the intelligence official in a mission. It is only fair and reasonable for the intelligence official deployed to a mission to expect to be given facilities commensurate with his rank and position in the mission. Sometimes this is not done or equivalence issues are deliberately ignored. This can lead to bad blood. Proper conditions have to be provided to maintain the cover of the intelligence official, particularly in hostile conditions and this should clearly be the responsibility of the Head of the Mission (HoM).

Diplomatic cover limits access to real targets. A heavy load of cover work could also be a constraint. Long time cultivation of assets, especially high value assets, can be hindered because they sometimes resent being 'handed over'. For gathering economic intelligence, it may be essential to access likely sources in financial centres, multinational corporate offices and technology centres apart from the government which diplomatic cover may not always be able to facilitate.

Visa Work

It has been customary to assign consular duties such as visa/passport work to the intelligence official to enable him to come in contact with the largest cross-section of diasporas, as also potentially suspect visa aspirants. Yet, where the pressure of visa applicants is heavy, there is scope for misuse of these powers.

Sometimes, misunderstandings occur because most HoMs want to retain some discretion in the grant of visas. It is the duty of the intelligence officer handling visa work to point out the proscriptions in the visa manual that forbid such authorisations. A balance needs to be struck between discretionary powers and rules. In fact, with the advent of terror related threats, it may be wiser to stick to the letter of the restrictive provisions and patiently wait out the procedural delays and let the safeguards of the verification process take their course. The practice now being followed in US missions abroad needs to be studied and may be, emulated. For example, the Homeland Security unit in the mission has absolute primacy in the processing of visas and the discretion of the HoM is reduced to a minimum.

Integrity

The personal integrity of all intelligence staff assigned to visa duties is very important and the head of station has to lead by example. Otherwise, mission diplomats are very easily convinced, by junior mission staff, about the nefarious intentions of the intelligence official in question. When allegations of this nature surface, instead of summarily making changes in the cover job; HoMs should

[71] V. Balachandran, '*Note of Non-Official Cover'* – recorded 12.01.2011 for IDSA Task Force

give the officer in charge of the visa division a chance to correct the lacuna or the perception of wrong doing.

Other Cover

The information and education desks in missions also make for useful cover assignments, especially in countries from where students come to India. When the intelligence complement in any mission is large, it may be possible to spread them across all such wings of the mission.

Dissatisfaction arising from cover jobs not being efficiently performed is often a reason for friction between the regular diplomat and the intelligence official. The excuse given by intelligence officials is that the heavy workload of a cover job leaves little time for real intelligence work, which may require very different type of legwork. However, it has also been seen, that in the long run, an intelligence officer is more successful where he first earns the respect of his peers in the diplomatic mission by virtue of the efficient discharge of cover duties. Here again, a balance needs to be struck. A proper appreciation of the onerous nature of the intelligence officer's real work and making due allowances instead of insisting on too literal a discharge of routine cover duties can reduce mutual distrust, which is often an inherent part of intra-service hostility.

Independence in Conduct & Manner of Reporting

Sometimes HoMs and other senior diplomats take umbrage over the comparative independence and access to separate channels of reporting enjoyed by the intelligence officer. Such reservations can be offset by clarifying that the authority of diplomats will not be undermined. Intelligence officers in legations abroad have very clear instructions to share all crucial matters relating to national interest and the security of the missions and its personnel fully and promptly with the HoM. The only reservation is against disclosure of the assets or intelligence sources from whom inputs are obtained and details of the methodology of operations. Most Heads of Mission are considerate enough not to press for such disclosures, especially if there are no issues regarding the intelligence officer's probity and conduct in cover duties.

Nevertheless, misunderstandings do occur and sometimes erupt into major scandals, with consequences deleterious to both – the diplomats as well as the intelligence services.

Liaison Related Misunderstandings

Heads of Mission are sometimes suspicious about the substantive aspects of intelligence sharing or about the comings and goings of mission officers. They are very much within their rights to expect to be kept generally informed about the drift of the liaison relationship and the day-to-day movements of mission officials or deployments within the host country made at the direction of the HQ. But such problems can be resolved with a little tact on the part of the intelligence officer on the spot. Again, experience shows that if the initial relationship has been harmonious, usually through respect earned by good cover performance, not much difficulty is faced in this regard.

Playing Intelligence Agencies Against Each Other

Sometimes problems can occur because of the scope to play officers of different intelligence agencies deployed in the mission, against one another. Because of the threat from terrorism and need to deploy specialised personnel for mission security and protection duties, such officers are posted together. Though their duties and approaches are different, their professional training is similar and in larger legations, or in places where there is a large diaspora, Heads of Mission find it convenient to use these intelligence officers for mission related tasks. This can be because of better personal chemistry or psychological pre-disposition.

Officers from some agencies sometimes harbour grandiose ideas about their own superiority or their expanded scope of duties. They may be insecure or report the external intelligence official for making unwarranted contacts with foreigners, who may be potential targets. They can play up these traits if supported by mission diplomats. In such cases the external intelligence service official can overcome such obstacles by displaying resoluteness of character, unimpeachable integrity and a dogged dedication to the tasks at hand. He should refrain from falling into the trap of one-upmanship or petty squabbling

Perceived cowardice during crisis situations in difficult/hostile stations can queer the pitch for intelligence officers in the eyes of the HoM or the deputy chief of legation. Sometimes the intelligence officer can be directed to take on ticklish responsibilities, which may needlessly blow his cover, and he deliberately avoids taking on such tasks. This can be a difficult situation. It may be better to take on the task and later explain the reluctance to do so to the HoM.

Misunderstandings also occur due to a perception that the HoM has to shoulder the blame if anything goes wrong in covert operations, authorised or seen to be authorised by the political executive back home. This justifies the demand, especially in neighbouring countries, that the Ambassadors must be kept broadly in the intelligence loop at the mission level and has some sort of say in what goes on in various operations, even if he is kept in the dark about the exact details of source running.

Institutional Safeguards

A mechanism that usually works well is that a HoM on a visit to homeland headquarters or a HoM designate calls on the chiefs of intelligence services. During such meetings, problems that are either endemic or location/person specific can be discussed and sorted out in a spirit of camaraderie.

In hostile stations, a supportive HoM can be extremely useful in tackling sensitive operational initiatives though contrary views exist within the intelligence community, especially among senior level supervisory intelligence officers, who have served only in cushy locations abroad, about the extent to which the operational methodology can be shared. Nowadays, hard and fast rules can be laid down in this regard as intrusive practices have developed even at headquarters, where joint high level scrutiny has become the norm rather than the exception, before granting approval for any influence operation abroad. The recent practice has

been to associate the HoM in such decisions. The implementation is left to the intelligence official on the spot but the HoM remains broadly aware of the progress in such operations. This system usually works well enough.

Other mechanisms are also possible. The Foreign Secretary and head of external intelligence should meet periodically to develop or discuss joint plans of action for the quarter, half-year or year. Instructions could go out to missions regarding certain crucial or sensitive projects, where the HoM should clearly be the overall mission supervisor, so that there is some order and discipline. This could even be done selectively.

Cooperation at the cutting edge of area desk level, between Joint Secretaries, is essential. Foreign Service officers do not always have an understanding of the intelligence officers' role in a mission and may not take them seriously or even treat them as undeserving interlopers. This could change for the better if there is a mechanism for greater interaction or exposure by posting Foreign Service officers in intelligence organisations for limited tenures in the domestic circuit. In the past, there used to be a system of posting a fairly senior Foreign Service officer - of Joint or Additional Secretary level- in the external intelligence agency. This system has almost fallen into disuse, partly on account of reluctance of Foreign Service officers to take up this post on alleged grounds of career planning or due to the indifferent quality of exposure given to them in the intelligence agency, especially in terms of sensitive operational work. Such problems could easily be sorted out if there is proper synergy between the two organisations in general and the respective heads of service in particular. External intelligence service officers could also benefit from postings in the foreign ministry.

In the perception of some Foreign Service officers, a reform worth considering is to place the external intelligence organisation under the External Affairs Ministry instead of the Cabinet Secretariat, as this might lead to better coordination similar to that prevailing between the Intelligence Bureau and the Ministry of Home Affairs. However, career intelligence officers may have reservations about the efficacy of such a change.

Case for Non-institutional Cover (NOC)

In the long term, intelligence agencies need to consider the option of deploying their personnel for non-diplomatic assignments abroad. This may be possible in countries where the Indian diaspora are getting employment opportunities in the services, high-tech or trade related sectors. Such officers themselves can become agents. If successfully placed, they can be deemed more reliable than paid sources. Such non official cover (NOC) employees may need to be recruited through a separate process, without exposing them to other regular staff. They could even be placed under cover with business houses.[72]

[72] V. Balachandran, restricted circulation note recorded Aug, 2005, made available on request for IDSA report

Some of the well-known CIA NOCs have been Air America and its successor Aero Contractors Ltd. In India, efforts were made to experiment with non-NOC- by the setting up of a travel agency or a security agency for operations overseas but these proposals did not get off the ground due to last minute bureaucratic obstacles.

Professional training as also language facility would be essential to succeed in such endeavours. This must be undertaken in real earnest and institutional mechanisms to seek out such openings for appropriately qualified intelligence personnel must be created in consultation with federations / chambers of industry and commerce.

Chapter 9

INTELLIGENCE CO-ORDINATION

Consequent upon the establishment of the National Security Council (NSC) and its substructures in April 1999 in India, reforms were undertaken from May 2001 onwards in pursuance of the Group of Ministers (GOM) report on **"Reforming the National Security System"**

ROLE OF CCS

Prior to 1999, and indeed right down to this day, apex level political decisions on security issues are taken in the Cabinet Committee on Security (CCS). The CCS, which continues alongside the NSC system, is chaired by the Prime Minister and currently includes as regular members the Ministers for Defence, Home, Finance, and External Affairs. Other Ministers are invited to CCS meetings on a need basis. During the NDA government, the Deputy Chairman of the Planning Commission attended all CCS meetings as a special invitee.

CORE GROUP

At the bureaucratic level, security issues have traditionally been, and continue to be addressed by the Committee of Secretaries (also called the Core Group). This is presided over by the Cabinet Secretary and has the Home, Finance, Defence and Foreign Secretaries as its members. Other Secretaries, the Chiefs of Staff, and heads of intelligence agencies are invited to these meetings on a need basis.

Discussions in the CCS as well as the Core Group have tended to centre on security matters of immediate concern. There is neither the time nor the inclination in these bodies to debate, analyze and develop medium and long-term policy options and strategies. Moreover, neither of these bodies is geared to view security holistically. Their field of vision is restricted essentially to insurgencies and law and order, terrorism, foreign policy, defence etc. The security aspects of issues like good governance, health, water management, environment, technology or even the economy are rarely debated in these bodies. Indeed, many issues with security implications are discussed in other committees of the Cabinet such as the Cabinet Committee on Political Affairs (CCPA) or the Cabinet Committee on Economic Affairs (CCEA) and as a result their security dimensions often escape attention.

CoSC

Issues of inter service coordination, both before and after 1999, have fallen within the domain of the Chiefs of Staff Committee (CoSC). The Chairman of this Committee is the senior most of the three

serving Chiefs of Staff, with seniority being counted from the date of appointment as Chief of Staff. The incumbent also continues to remain the head of his Service.

The Chairman's efficacy in bringing about coordination and offering single point military advice to the government is limited by the fact that he cannot impose his will on his other two colleagues. Moreover, most of his time is devoted to the running of his own Service. It was with a view to overcoming this lacuna, as well as creating greater joint-ness in the Armed Forces and administering the strategic forces that the GOM report recommended the creation of a Chief of Defence Staff (CDS) who would act as the head of the Chiefs of Staff Committee. His objectivity and independence were sought to be ensured by providing that after completion of his tenure he would not return to his Service. Unfortunately, a decision on this recommendation was deferred and therefore the Chiefs of Staff Committee continues to be headed, as in the past, by one of the Chiefs of Staff in rotation and not by a CDS.

Intelligence

While acquisition of intelligence on developments abroad has been the responsibility of the R&AW, both before and after 1999, intelligence pertaining to domestic developments has been, and continues to be, the responsibility of the Intelligence Bureau (IB). In addition, each of the three services has its own intelligence wing for collection of defence related intelligence. The various intelligence agencies like R&AW, IB, etc have always furnished their inputs and assessments directly to the user agencies/departments as well as to the Joint Intelligence Committee (JIC), and, after 1999, to the National Security Council Secretariat (NSCS).

JIC / NSCS

Prior to 1999, the JIC was the apex intelligence coordinating organization.[73] Lacking any primary intelligence collection capability, it was to be provided with all relevant inputs by the intelligence agencies as well as the Ministry of External Affairs and the Ministry of Home Affairs. In addition, it could call for any input from any department of the government. On the basis of these inputs, and discussions with all concerned as well as open source material, the JIC and later, the NSCS issued a Monthly Intelligence Review and Strategic Analysis as well as special papers on important topics.

Its charter of duties as detailed in the KRC report and as laid down in 1985 mandated the JIC to:

> (a).assemble, evaluate and present intelligence from different sources pertaining to internal and external developments as may have a bearing on National Security; (b) prepare reports on its own initiative or as required by the Policy Planning Group on National Security or by the Cabinet Committee on National Security;

[73] Kargil Review Committee Report

(c) prepare special reports which would help in policy formulation in the Ministry of Home Affairs (MHA)/Ministry of Defence (MOD)/ Ministry of External Affairs (MEA).

Systemic Deficiencies

The glaring deficiency in the actual functioning of this intelligence system was the lack of any effective direction or control over the various intelligence agencies and an absence of any meaningful coordination of their activities. They tended to work in watertight compartments. There was no institutionalised system for coordinated action or for information sharing. Neither was there any apparent and concerted sharing of information amongst each other. There was also no systematic tasking of the agencies or any focused evaluation of their performance.

Upgradation of TECHINT was undertaken in a somewhat haphazard fashion and there was little coordination in the acquisition of TECHINT assets.

The JIC, as an evaluator and coordinator of intelligence, was marginalised. Its product rarely received the attention it deserved. It had no political support and was not nurtured to play its required role. Accordingly, it had no clout within the system. It is no surprise, therefore, that the intelligence collection agencies tended to bypass the JIC in their keenness to be seen as being the first to provide important information at the highest level. Such bypassing not only resulted in an information overload but also in submission of unprocessed and inadequately assessed intelligence to decision makers.

Dissatisfaction with the prevailing security system, which lacked the mechanism for viewing security holistically and of paying focused attention to the entire range of security related issues on a continuous basis, led the government from the 80's onwards to experiment with new structures to overcome this lacuna. Thus, as cited by Mr K Subrahmanyam in "Shedding Shibboleths", an inter disciplinary group was set up under Prime Minister Rajiv Gandhi, interalia comprising two key ministers from the Cabinet, Shri Arun Singh, the Cabinet Secretary, Chairman CoSC, the two intelligence chiefs, the Chief Economic Advisor, Chairman Atomic Energy Commission, Director IDSA and Chairman of the JIC. It served as an informal discussion group for brainstorming on a variety of security related issues. It lasted only a year. A multidisciplinary policy planning committee was also set up under G. Parthasarthy. It too was wound up after seven or eight meetings.

National Security Council

Subsequently in August 1990, the VP Singh Government announced the establishment of a National Security Council (NSC) along with supporting structures. This exercise was as short lived and the 1990 model of the NSC never took off. The next government set up a task force under K.C. Pant in April 1998 to work out the constitution, role and functions of a new NSC.

The prevailing NSC system, influenced in part by the system set up in 1990 and in part by the Pant Committee report, was put in place by the Cabinet Secretariat

Resolution of April 16, 1999, with the objective of ensuring a more pro active, coordinated and holistic approach to security management. Underlining that national security needed to be viewed "not only in military terms, but also in terms of internal security, economic security, technological strength and foreign policy" the Resolution stated that the Government recognised that national security management required "integrated thinking and co-ordinated application of the political, military, diplomatic, scientific and technological resources of the State to protect and promote national security goals and objectives."

The NSC system was not meant to supplant the existing apex institutional mechanisms, like the CCS or the Committee of Secretaries, but to provide support to them and to cover the gaps left unaddressed by them. These gaps arose from the fact that the existing mechanisms were essentially geared only to handling crisis situations in areas traditionally associated with security and were unable to bring to bear coordinated action across the entire spectrum of national life designed to promote national security. It was clearly recognised that efficient management of national security entails not merely the effective handling of crisis situations but, perhaps, even more importantly their pre-emption. While the former demands coordinated action by several different departments, agencies and authorities, the latter requires the undertaking of threat assessments - short, medium and long term, identification of contingencies likely to impact the country, and formulation of alternative strategies to counter such contingencies. The NSC system comprises the National Security Advisory Board (NSAB), the Strategic Policy Group (SPG), the National Security Advisor (NSA) and the National Security Council Secretariat (NSCS).

The NSC, as constituted in 1999, was chaired by the Prime Minister and its members included the Home Minister, the Defence Minister, the External Affairs Minister, the Finance Minister and the Deputy Chairman of the Planning Commission. (Under the UPA Government the NSC was reconstituted and omitted the Deputy Chairman of the Planning Commission. This brought the NSC's membership in line with that of its 1990 predecessor, but diluted somewhat the holistic flavour that the earlier composition of the NSC reflected.

The Cabinet Secretariat Resolution, while clearly limiting the NSC to an advisory role gave it an extensive remit in order to enable it to address security holistically. Accordingly, it specifically called upon the NSC to deal with the following broad areas of interest:

(a) external security environment and threat scenario;

(b) security threats involving atomic energy, space and high technology;

(c) trends in the world economy and security threats in the areas of energy, foreign trade, food, finance, and ecology;

(d) internal security, including counter insurgency, counter-terrorism and counter intelligence;

(e) patterns of alienation emerging in the country, especially those with a social, communal or regional dimension;

(f) security threats posed by trans-

border crimes such as smuggling and traffic in arms, drugs and narcotics; and

(g) co-ordination in intelligence collection and tasking of intelligence agencies so as to ensure that intelligence is focused on areas of concern for the nation.

It may be mentioned that, contrary to what has been made out by some experts, the NSC's remit is not limited to only medium or long term issues as was the case with its 1990 predecessor, it is free to address all security related issues, along the entire time spectrum, including those of immediate import.

National Security Advisory Board (NSAB)

The NSAB which was approved by Government in December 1998, comprises a Convenor and other persons of eminence outside government "with expertise in the fields of foreign affairs, external security, defence and armed forces, strategic analysis, economics, science and technology, internal security, and related areas."[74] The size of the NSAB, inclusive of the Convenor, is limited to a maximum of 30. While the first NSAB had as many as 27 members, subsequent NSAB's have been much smaller, ranging from 15-20 members, in the interests of cohesion and efficacy. The NSAB's role as stipulated by the Cabinet Secretariat Resolution is to advise the NSC on issues relating to national security referred to it by the Council. The NSAB's utility lies in the fact that its establishment enables government to tap expertise from outside the existing official set up.

The NSAB has been amongst the more active substructures of the NSC system. NSAB members for the first four Boards were appointed for a one-year term, which was normally extended by another year. On advice from the late NSA, J.N. Dixit, NSAB members for the fifth Board under the UPA government were nominated for a full two year term *ab initio*. The NSA invariably attends the first and last plenary of the NSAB. At the first plenary he sets the agenda for the NSAB. This is sometimes increased or modified by him, during the course of the year, depending upon the requirements of government. The NSAB meets in plenary at least once, and often twice, each month. However, its sub-groups meet much oftener in order to develop papers on subjects allocated to them by the Board.

The NSCS quite deliberately has been given no role in the development of NSAB studies, apart from providing purely secretarial assistance, with a view to ensuring - as stated earlier - that the NSAB's views are independent and in no way coloured by government thinking. An effort was, however, made by the then NSA to encourage the preparation of joint studies by the NSCS and the NSAB. This effort did not succeed, primarily due to opposition from the NSAB members who realised that this would impact on their mandate of placing their views before the government, untainted by NSCS advice.

[74] Cabinet Secretariat Resolution of April 16, 1999

All major NSAB papers produced by the sub-groups are cleared in a plenary and are sent to the NSA through the NSCS. It is free to interact with Ministries, the Services, any agencies, or indeed anyone within the system. The NSAB has proved itself to be a useful conduit for passing on advice to the government from outside the system. Every Board each year provides the government with several studies, some on request and some self initiated. Their main value lies not in the details or facts furnished, which cannot and are not expected to be comprehensive, but in their line of approach. The output of the first two Boards of which K. Subrahmanyam was convenor has yet to be matched. It produced two seminal high quality papers: one on India's nuclear doctrine and another entitled "Strategic Defence Review". Much of what was contained in the former became a part of India's official nuclear doctrine and the latter served as a template for subsequent National Security Reviews that were extensively absorbed within the government.

Strategic Planning Group

The SPG is required to assist the NSC by acting, as stated in the Cabinet Secretariat Resolution, as the "principal mechanism for inter-ministerial coordination and integration of relevant inputs in the formulation of national security policies". The SPG is chaired by the Cabinet Secretary and comprises the three Service Chiefs, the Secretaries to Government comprising the Core Group, Governor of the Reserve Bank of India, Secretary, Department of Defence Production and Supplies, Scientific Advisor to the Raksha Mantri, Secretaries of Departments of Revenue, Atomic Energy and Space, Director, Intelligence Bureau, Secretary, R&AW and Secretary, NSCS (ex–officio Deputy to the NSA). As and when necessary, representatives of other Ministries/Departments can be invited to SPG meetings which may be convened by either the Cabinet Secretary or the NSA.

The SPG is a critical component of the NSC system. By convention its meetings are to be convened by the Cabinet Secretary on the first Wednesday of each month in order to discuss NSCS monthly intelligence reports and strategic analyses as well as security related papers prepared by the NSCS or other organisations/ agencies/ ministries. These meetings usually lead to meaningful action oriented decisions. Though theoretically the NSA is authorised to call SPG meetings, in practice this has never happened and the SPG has remained very much a creature of the Cabinet Secretary. The frequency of its meetings has therefore tended to depend on the Cabinet Secretary's interest in security related issues. Accordingly, while in some years the SPG has met on 7 or 8 occasions, in others the frequency of its meetings has been much lower. In these circumstances it would be evident that the SPG has not been as effective as it could be.

National Security Council Secretariat (NSCS)

The NSCS was set up for servicing the NSC, the NSAB, and the SPG. In order to enable the NSCS to effectively support the NSC and the SPG it was specifically mandated by the Cabinet Secretariat Resolution of April 16, 1999 to "prepare or cause to be prepared papers for consideration" of each of these bodies. It

needs to be noted that the Resolution imposed no similar obligation on the NSCS in respect of the NSAB. The reason for this was that the Government wanted the views of the NSAB to be independent and uninfluenced and untainted in any manner, by the thinking within the system.

In addition to its role as a secretariat for the NSC system, the NSCS also inherited all the intelligence related functions of the JIC. Indeed, it was created out of the existing JIC, which had to be revamped in order to meet the enlarged responsibilities of the NSCS. There was sound logic in vesting so important an intelligence role in the NSCS as the NSC itself was specifically mandated to address the coordination of intelligence collection and the tasking of the agencies.

The importance attached by government to the NSCS may be gauged from the fact that the Resolution establishing the NSC system required all ministries/departments to "consult" it "on matters having a bearing on national security". Moreover, while initially the NSCS was "located" in the Cabinet Secretariat, from March 2002 it became a special unit under the direct charge of the NSA in the Prime Minister's office.

In the area of intelligence the NSCS, like the JIC, is not a collecting agency but is totally dependent on intelligence inputs from various agencies like R&AW, I.B. DIA, etc. Its task is to evaluate these inputs, by weighing them against each other and against inputs received from ministries/ departments, as well as from open sources to develop a more authentic and complete picture. Apart from presenting these evaluations to the Government regularly each month, as was done by the JIC, the NSCS does this oftener on a need basis.

The NSCS evolved mechanisms that were designed to encourage the intelligence community to work together in a more cooperative and cohesive mode. One of the most significant achievements of the NSCS was to put in place a system for the annual tasking and evaluation of the agencies. Hitherto, there was little interface between the consumers and producers of intelligence. As a result, while the consumers did not know what they should seek from the agencies on an annual basis, the latter furnished whatever they could get to the consumers, irrespective of the actual requirements. In the absence of any conscious tasking by the consumers there could not be any realistic evaluation of the performance of the agencies. This was further fine tuned in the Intelligence Coordination Group (ICG). This system was designed to ensure the greater accountability of the agencies and a more focused collection of intelligence in accordance with the requirements of the consumers through the reallocation of resources. Subsequently, the change of guard in the NSCS saw this mechanism being discontinued. It needed to be tried for a longer period and its resumption is strongly recommended if the NSCS is to continue playing a constructive role in providing long term strategic analyses.

Security Reform

Based on the recommendations of the GOM report on "Reforming the National Security System" that was accepted, more or less in toto, by the CCS in May 2001, the role of the NSA and the NSCS saw a further enhancement. Over and above

what was originally envisaged, the NSA and the NSCS came to acquire oversight functions over the newly created National Technical Research Organisation (NTRO), and mechanisms like the Intelligence Coordination Group (ICG), Technical Coordination Group (TCG), and National Intelligence Board (NIB).

National Technical Research Organisation (NTRO)

The idea of setting up an apex TECHINT organisation like the NTRO emanated from the KRC Report which recommended that the possibility of establishing such a body patterned on the US National Security Agency should be examined, as it was "neither healthy nor prudent" to endow any one agency alone with "multifarious capabilities" for both HUMINT and TECHINT capabilities. The GOM duly examined this idea and endorsing it, proposed the creation of the National Technical Facilities Organisation (NTFO), subsequently renamed as the National Technical Research Organisation (NTRO), as the apex TECHINT organisation which would:

1. Plan, design, set up and operate any major new strategic and expensive TECHINT facilities as approved by the TCG keeping in view the rapid convergence now taking place among hitherto different technologies.
2. Examine and process plans of the intelligence agencies for the acquisition of all new facilities/ equipment costing more than Rs 3 crores, for consideration by TCG
3. Plan and establish modern, secure digital networks connecting the intelligence agencies in Delhi as well as (where required) outside Delhi.
4. Create, support and maintain a common database of requisite information as approved by the TCG so that intelligence can be rapidly disseminated among all concerned agencies to authorised guidelines and protocols.
5. Explore and establish facilities required for monitoring missile launches, or preparations therefore, in any country of interest.
6. Develop capabilities for defensive and offensive cyber operations.
7. Carry out such other projects or programmes as the TCG may direct.[75]

The creation of such an apex TECHINT organisation was one amongst the approximately 340 recommendations contained in the GOM report approved by the CCS in May 2001. It proved difficult to implement as the modalities for executing the task with optimal efficiency and economy remained unaddressed. Specifically, the GOM report had not looked into the fact that if the NTRO's capabilities were to be built up from scratch, it would not only be prohibitively expensive, but also very time consuming. Its early and cost effective setting up quite obviously required a judicious transfer of

[75] Press release issued after CCS meeting,, May 11,2001

capabilities from existing structures like the Aviation Research Centre (ARC) to it. Neither the Task Force on Intelligence (set up by the GOM to help it in its work), nor the GOM itself apparently foresaw this problem. Accordingly, they failed to specify what assets were to be transferred to the NTRO and from which organisation. It fell to the lot of the NSA and the NSCS to resolve this thorny problem, which was essentially a battle for turf. After much cogitation, involving a feasibility study on the matter undertaken by the then Principal Scientific Advisor, Dr Kalam, and innumerable interagency discussions, the NTRO was finally established as late as April 2004, though its Chairman had been appointed in March 2003. The NTRO's charter as ultimately determined was largely along the lines recommended in the Group of Minister's report and agreement was also reached on the manner and time frame in which assets would accrue to it from various other entities. The NTRO, like the NSCS, is directly answerable to the NSA.

Technical Coordination Group (TCG)

The **Technical Coordination Group (TCG)** was constituted in June 2003 soon after the appointment of the Chairman of NTRO. Its main function is to coordinate and regulate plans for acquisition of all new, costly, major strategic facilities/ equipment by the intelligence agencies, exercise oversight over intelligence agencies and examine issues relating to the allocation of funds for this purpose.[76] It is also required to ensure that in the procurement of expensive assets, there is no avoidable duplication or redundancy. It is headed by the NSA and the Chairman NTRO serves as its Member Secretary. Other members include the Principal Scientific Advisor to Government of India, the Cabinet Secretary, the Chairman, Chiefs of Staff Committee, Secretaries of the Department of Space and Atomic Energy, Scientific Advisor to Raksha Mantri, Deputy to the NSA, Secretary (R) Cabinet Secretariat, DIB, and DG Defence Intelligence Agency (DIA)[77]

Intelligence Coordination Group (ICG)

The Intelligence Coordination Group (ICG) became operational in June 2001. It is presided over by the NSA and includes the Cabinet Secretary and Secretary NSCS, as Member Secretary, other Secretaries, Secretary (R), DIB, DG DIA, the head of NTRO, and Chairman CoSC. Service Chiefs can be called for meetings as and when required. Its main purpose is to provide systematic intelligence oversight at the apex level to address the following issues:

- Allocation of resources to the intelligence agencies
- Consideration of annual reviews on the quality of inputs
- Approve the annual tasking of intelligence collection

[76] Press release after CCS meeting, May 11,2001

[77] NSCS Resolution of June16,2003

- Oversee the functions of intelligence agencies
- Examine national estimates and forecasts.[78]

National Intelligence Board (NIB)

The NIB was constituted in August 2002 for national level policy formulation on information warfare and information security as well as for the creation of the required institutions and structures for implementation of the policies developed. The NIB was also mandated to task and monitor the institutions and structures created by it. Chaired by the NSA, the NIB is serviced by the NSCS. The Cabinet Secretary, service chiefs, Secretaries who comprise the Core Group, Secretaries belonging to the Ministries/Departments of Information Technology & Telecom, Information & Broadcasting, Dept of Space, Chairman Atomic Energy Commission, Scientific Advisor to Raksha Mantri, DIB, Secretary (R), Chairman NTRO, DG DIA are members and Secretary NSCS/Deputy to the NSA is Member Secretary.[79]

Apart from the foregoing elements of security reform which impinged directly on the NSC system there were two other elements which also impacted it but not in so direct a manner. The first pertained to the Armed Forces and the second to the issue of economic intelligence.

As regards the Armed Forces, a number of measures were implemented designed to promote greater "jointness". In the area of intelligence, a Defence Intelligence Agency (DIA) was created to ensure a better integration of intelligence collected by the three service directorates and to serve as the principal military intelligence agency. While the creation of a Chief of Defence Staff was stymied, a Chief of Integrated Defence Staff was appointed in lieu of a Vice Chief of Defence Staff in order to promote 'jointness' over a variety of issues like doctrine, training, the planning process, both long term and short term, etc.

As regards economic intelligence the GOM while stressing that the intelligence agencies should upgrade their capabilities in this area also called for the broadening of the mandates of the Economic Intelligence Council (EIC) and the Central Economic Intelligence Bureau (CEIB) as well as for the setting up of a Financial Intelligence Unit to keep a track of suspicious financial transactions.

Structures to manage nuclear deterrent

The GOM report had recommended the creation of a Strategic Forces Command (SFC) to manage India's strategic forces. It had also recommended the creation of a CDS who would, apart from his other functions, also exercise administrative control over these strategic forces as distinct from operational military control which would vest in the highest political authority. In effect, the Commander in Chief, SFC, would function under the

[78] Press release after CCS meeting, May 11,2001;

[79] NSCS Resolution, Aug 29,2002

control of the CDS who would be the channel for communication between the Government and him. While the Commander in Chief, SFC, was appointed in early 2003, a CDS has not been appointed till date. This, incidentally, was the only major GOM recommendation not accepted by the CCS in May 2001. In the absence of the CDS all his functions, including those pertaining to the nuclear deterrent, are undertaken by the Chairman Chiefs of Staff Committee who currently also doubles as a Service Chief.

Subsequent to the GOM report, the CCS in January 2003 reaffirmed that the SFC would manage and administer all our strategic forces and that nuclear retaliatory attacks could only be authorised by the civilian political leadership. Such authorisation would be through the Nuclear Command Authority (NCA) comprising a Political Council and an Executive Council. The Political Council is chaired by the Prime Minister. It is the sole body which can authorise the use of nuclear weapons. The Executive Council is chaired by the NSA. It provides inputs for decision making to the NCA and executes the directives given to it by the Political Council.[80]

National Security Adviser (NSA)

The Cabinet Secretariat Resolution for setting up the NSC system somewhat cryptically stated that there would be a National Security Advisor (NSA) who would "function as the channel for servicing the National Security Council".

The NSAs have had a critical role in the selection of each NSAB and in giving it the requisite guidance. Each NSA has set the agenda for the NSAB and engaged with it from time to time. The NSA has traditionally been the sole recipient of all the NSAB's output.

The NSA, has, under the NSC system and with the creation of the ICG, NTRO and the TCG, emerged as a powerful coordinator of intelligence. Apart from being the recipient of all critical intelligence inputs from the agencies, he also gets regular evaluations and assessments from the NSCS of the intelligence inputs transmitted to it by the agencies which include not only the R&AW, the IB and the intelligence wings of the military and paramilitary forces etc, but also the newly created DIA as per the recommendations of the Group of Ministers.

In more recent times, the NSA has also been playing a vital role also as the principal diplomatic adviser to the Prime Minister, be it in the negotiations relating to the civil nuclear deal with the United States, or any bilateral Track –I or Track – II initiatives undertaken to resolve thorny stalemates.

The importance of the role of the NSA in making our nuclear deterrent operational and ensuring its credibility cannot be underestimated. As Chairman of the Executive Council he is the main conduit

[80] Press release after CCS meeting, Jan 4,2003

for the inputs passed on to the Political Council for decision making and for the execution of its orders.

It would be evident from the foregoing that, contrary to what has been made out by the critics, the NSC system actually works and along with introducing some reforms in the security sector, has added value to our security/intelligence structures like the CCS with which it has coexisted. However, this is not to suggest that the NSC system is performing perfectly and that there is no scope for improvement. Indeed, a view has been expressed that the NSA's overall responsibilities are so vast that they leave him with little time to devote to the intricacies of intelligence coordination. There may seem to be a need to clearly define the NSA's responsibilities and functions relating to intelligence through statutory provisions so that there is no vacuum at the apex of the intelligence structure.

While in purely structural terms the system *per se* cannot be faulted, its actual performance has remained less than optimal because its meetings are held rather infrequently. The SPG headed by the Cabinet Secretary has met less frequently than warranted. Inter-agency turf battles have also taken their toll in slowing down or even completely blocking reforms. Implementation of the GOM recommendations has been much slower than it should have been. Perhaps, what really demonstrates the general absence of security consciousness afflicting both the political class and the bureaucracy is the fact that the NSC has rarely met.

The infrequency of NSC and SPG meetings, designed to be in the nature of freewheeling brainstorming sessions, has hampered the evolution of a culture of looking at security holistically. The management of soft security issues like water, health, energy, etc has suffered as these are rarely viewed from the prism of national security. Regrettably, the political and bureaucratic leadership continues to remain wedded to a damage control mode rather than a more systematic and well-structured long term policy evolution mode as reflected by the fact that the meetings of the CCS and Committee of Secretaries are held far more frequently than the NSC or SPG meetings.

Progress in addressing economic security issues also leaves much to be desired. While, as recommended, intelligence agencies, like R&AW and IB, were asked to upgrade their ECOINT collection capabilities and the mandates of the Economic Intelligence Council (EIC) and the Central Economic Intelligence Bureau (CEIB) have been revised and a Financial Intelligence Unit has been set up, the EIC and CEIB have regrettably remained largely inactive.

Another major deficiency in the manner in which the NSC system has been functioning is that the NSCS is not kept fully in the loop on all security related issues as mandated. Advice on security related issues is sought from the NSCS on an ad hoc basis rather than as a matter of routine. If the NSC system is to work with optimal efficacy the NSCS must be kept fully in the picture on all security related issues including "soft" security issues and it should be consulted regularly In addition, its products should be given the benefit of due consideration at the highest level. If these lacunae are addressed the NSC system will function much more

effectively and enable the Government to better handle our internal and external security concerns. [81]

Implementation of recommended reforms raises problems of coordination, which is not always fully thought through. The Kargil Review Committee (KRC) flagged this lack of coordination while noting in particular, that a June 1998 report of the IB disseminated at the highest level was not copied to either the R&AW or the JIC. It pointed out several instances where the military did not share relevant information with other concerned agencies that could corroborate the inputs. For instance, 'bits and pieces' of information regarding the ORBAT changes of Pakistani Battalions opposite Kargil was available but the central message emanating from these inputs could not be read correctly.

The G.C. Saxena Task Force after Kargil had recommended a two tier arrangement to tone up coordination -the NSA & then Principal Secretary to PM presiding over all intelligence agencies-IB, R&AW, etc and a separate Committee on Technical Intelligence.

Several measures for reform that are being currently undertaken, include the proposal to establishment of a National Counter-Terrorism Centre (NCTC) and some others that are still in the proposal stage, such as a new Maritime Intelligence and Coastal Security Centre, or a centre for Nuclear and Missile Intelligence. Although much needed but they do have the potential to intensify turf battles among existing agencies with overlapping spheres of responsibilities. Some such problems have already been experienced between the newly set up NTRO and the ARC, over the ownership, use and sharing of expensive, valuable technical facilities and assets.

By 2003-2004, a Multi Agency Centre (MAC) and a Joint Task Force on Intelligence attached to the Intelligence Bureau had also been set-up, mainly to effectively coordinate inputs related to terrorism obtained from different field agencies on a day-to-day basis. Subsidiary MACs (S-MACs) were also established at the state level, assigning their responsibilities to different lead agencies (BSF, CRP or SSB) with the main task of synergizing the special or intelligence branches of the state police organisations and bringing about operational convergence between them and central agencies .

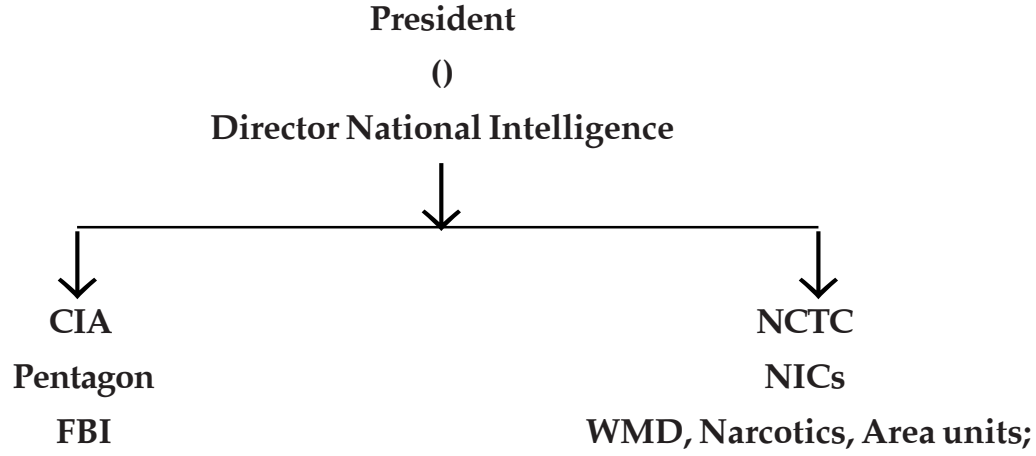
After the Mumbai attack in November 2008, question marks arose once again about the effectiveness of these coordination mechanisms. The NSCS and the JIC have had to undergo a role redefinition. The latter has been directed to focus more on the immediate or short-term intelligence inputs, that too on terrorism centric data, while the NSCS has reverted to more in-depth, policy oriented prognoses relating to intelligence and national security priorities. These changing roles are still in the process of evolution.

---

[81] Satish Chandra, former Deputy NSA: Article on the National Security set up: *AGNI: Forum for Strategic Studies journal,* Vol X, No IV, Oct-Dec '07**;** also see Satish Chandra: Article on National Security Coordination in journal: Indian National Security Review,2005;

Coordination problems in USA

The question as to who should take on the mantle of responsibility at the apex level for intelligence co-ordination could be open to controversy, as has happened over the appointments of successive DNI in the USA. As envisaged by the Kean Commission recommendations, the hierarchy chart of intelligence outfits would look something like this:



Before the appointment of the DNI, the CIA Director was also designated Director, Central Intelligence (DCI). Three multi-disciplinary centres – the Counter Terrorism Centre (CTC), the Counter Proliferation Centre (CPC) and Counter Intelligence Centre (CIC) reported to DCI. The CIC leadership rotated between the Directors of the CIA and the FBI. Several quick changes of leadership occurred within the CIA in this period – Porter Goss to Michael Hayden and later Leon Panetta.[82] Though notionally the DNI is superior to the CIA Director, who should report to him, in practice this did not happen immediately.[83] CIA lawyers raised questions of legislative language to stress its independence and pointed out that nowhere was it clearly specified that the DNI was the CIA Director's boss. In five years, there have been three DNIs, each with a different approach to the job. High profile appointments of Negroponte and Dennis Blair were rather short lived, though reasons for their short tenures have not been made public so far.[84] Though intelligence spending has doubled in the last few years, many intelligence professionals in USA 'looked at the reform brouhaha with detached bemusement,

[82] B.Raman :CIA & the war on Terrorism –*Saag Paper* no70,June 2006

[83] B.Raman -9/11 Report – Old Wine in new Bottle – Five Part analysis: Saag.Org -July-Aug, 2004 ;

[84] *Economist*.com ,May 27,2010: *Seeking a new spy-in-chief* ;& ISN ,ETH Zurich: *DNI: Help Wanted again*: May 26,2010;

believing that reform would result in no meaningful change'.[85]

In India too, post Mumbai 26/11, the question whether India should or should not have an intelligence Czar has been much debated.

Role of HM

After P. Chidambaram became Home Minister, the Ministry's marginalisation in matters relating to intelligence co-ordination has been decisively reversed and steps have been taken to strengthen its role in internal security management. The Home Minister currently holds a daily meeting of Intelligence chiefs where all intelligence inputs relating especially to terrorism threats are examined in detail and follow up action points and co-ordination bottlenecks between central and state agencies are sorted out. This has brought about some toning up of the performance, alertness and coordination between agencies, both at the centre and in the states.

The Home Minister's statement in the December 2009 meet of Directors General of Police[86] indicated that more soul searching was in process, even as steps were being formulated to set up a new NCTC, which could be modelled on the US Homeland Security Department set up as per the recommendations of the Kean Commission report of 2004.

In May, 2010 the *Times of India* reported that the PMO was contemplating the setting up an Intelligence and Security Co-ordination Committee, consisting of the NSA, the Cabinet Secretary and the Home Secretary. These steps have the potential to dilute the co-ordination role and responsibilities of the NSA. The PMO is trying to find an alternative mechanism by making the NSA share this responsibility with the Cabinet Secretary and the Home Secretary. [87]

Other security analysts and professionals have opined differently. A suggestion which was discussed in some depth at the IDSA Round Tables on the subject was that there should be a National Intelligence Coordinator (NIC), directly under the PM and the NSA, on the pattern of the US DNI. He could report directly to the Home Minister on matters relating to internal security and to the External Affairs Minister on issues impinging on foreign policy matters. The JIC would be under the DNI or NIC and not the Home Ministry. The proposed NCTC can still report directly to the Home Minister. The DNI/NIC and NSA would continue to be the vital organs in the functioning of the national security apparatus.[88]

---

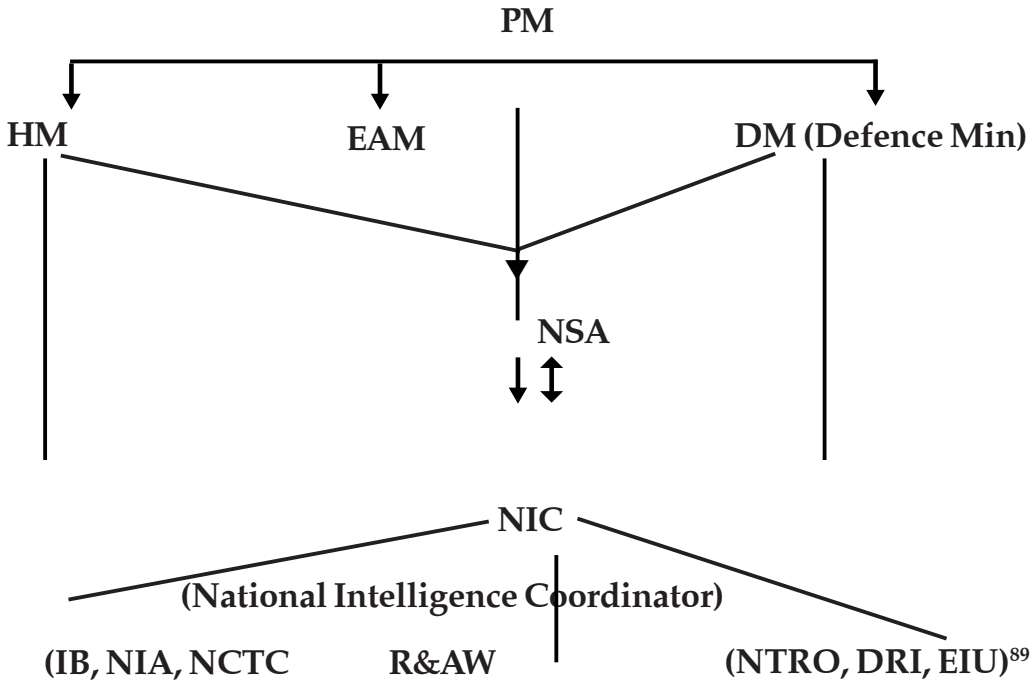
[85] Patrick Neary, Principal Dy. Dir, ODNI: Intelligence Reform,2001-2009:Requiescat in Pace ? :*Studies in Intelligence*, Vol 54,No1 : Quarterly Intelligence Journal ,April 2010;

[86] 22 nd Intelligence Bureau Endowment lecture, New Delhi, 23.12.09;

[87] B.Raman: *No More Co-ordination Czar ?:* Saag.Org paper No.3832 ,28.05.10;

[88] K. Subrahmanyam: views shared at IDSA Round Table,Aug2010;

The flow chart for the intelligence apparatus would then look something like this:



The logic behind this coordination mechanism would be to leave enough scope for a specialised role. The NIC and the NSA would be complementary assisting structures for the Prime Minister, Home Minister and a Minister for Intelligence. The NIC could be at a level lower than the NSA and the primary responsibility of giving advice on strategic matters, or long term foreign policy would still remain with the NSA. The NIC would assist on specific security policy related initiatives. Similarly, he could provide coordinated inputs to the Home Minister on internal security matters, if needed. On defence related issues, NIC could assist the NSA or advise the Defence Minister directly if required, without disturbing the hierarchy of the Service Chiefs, DIA and Chief of Defence Staff, if and when appointed.

Another view voiced in this context by eminent retired intelligence exponents, who have dealt with security issues, is to consider having a separate Minister for National Security, who could be entrusted with all national security related responsibilities and be answerable to the

[89] A. K. Verma, former Secretary, R (Cabinet Secretariat): IDSA Round Table, Aug 2010;

Prime Minister and the Parliament for the same. Routine functions of the Home Ministry could be separated from this role. The NIC could then emerge as the main intelligence professional to assist such a Minister while the NSA could focus more exclusively on his diplomatic tasks while assisting the PM.[90] In such an eventuality, the nomenclature of the NSA may have to be changed.

This proposal to have a separate coordinating mechanism on the lines of a NIC would, of course, have the disadvantage of eroding the powers and access of the DIB and Secretary, R&AW to some extent, as their direct access to the Prime Minister will tend to get restricted in this arrangement (the 'dwarpal' concept). This is already happening to an extent ever since the office of the NSA came into being -though all NSAs strenuously refute the idea that they prevent the access of the chiefs of agencies to the PM. But, it may reduce the burden on the Home Minister for day to day coordination, even if it pertains specifically to terrorism related follow up coordination only.

[90] Brajesh Mishra, former Principal Secretary to PM & NSA : at IDSA Round Table, 19.2.11;

Chapter 10

Oversight & Accountability

Modern day theorists on intelligence reform identify the following principal concerns relating to oversight:

1) Legality, 2) effectiveness, 3) efficiency, 4) budgeting & accounting, 5) conformity with human rights and 6) policy & administration;[91]

These could be divided into two main areas – efficacy and propriety. Efficacy has several dimensions – one of which is to see the extent to which an intelligence service is able to meet expectations of its consumers- the military headquarters or the Ministries for External Affairs or Home. The other concern, of propriety, is to ensure that ethical and legal standards are maintained and adhered to by intelligence agencies. This relates to achieving a balance between commitment to civil liberties/human rights and tolerance for their inevitable infraction in the national security interest.

The Geneva Centre for the Democratic Control of Armed Forces [DCAF), the Human Rights Centre of Durham University, UK and the Norwegian Parliamentary Intelligence Oversight Committee undertook a joint exercise to draft legal standards for accountability of intelligence services in liberal democracies. They followed the definition of 'good governance' prescribed by the World Bank.[92] They created a methodology according to which legal standards need to cater to four levels of oversight: internal control at the level of the agency; executive control; parliamentary oversight and oversight by independent bodies.[93]

Different Oversight Structures across the World

The need for establishing oversight mechanisms vis-à-vis intelligence agencies has been felt and dealt with in different parts of the world. The United States set up two Congressional committees in 1976 and 1977- the Church and Pike committees, which documented systematic abuse both in the United States

---

[91] Wolfgang Krieger: *Oversight of Intelligence: A comparative approach : National Intelligence Systems, Current Research & Future Prospects*: Treverton & Agrell : Cambridge University Press,2009;

[92] The World Bank: '*Governance : The World Bank Experience'*

[93] Born & Leigh, *Making Intelligence Accountable: Legal standards and Best Practice for Oversight of Intelligence Agencies*, pg 23…

and abroad by US intelligence agencies. These became a model for the strengthening of oversight that has been replicated in many countries since.[94] Following the US, Australia[95] and Canada[96] also legislated for intelligence oversight in 1979 and 1984. Reforms spread to Europe over the next two decades. Countries like Argentina, South Korea and South Africa have also established systems of accountability.

The United States

A set of 16 agencies constitute the United States intelligence establishment. Led by the DNI, these include units under the United States Departments of Defence, Justice, State, Homeland Security, Energy and Treasury.[97]

Though there is overlapping both in foreign and domestic areas, oversight of intelligence, particularly in the foreign realm is concentrated to a large degree in the House and Senate Select Committees on Intelligence. It, however, is not centralised there. Each panel has exclusive legislative authority over only the CIA and the DNI. A number of other committees share oversight. These include the appropriations, armed services, foreign affairs/foreign relations, and judiciary committees that have representation on their chamber's intelligence committee. Additional panels with oversight or legislative jurisdiction over parts of US intelligence include those dealing with: civil liberties, cyber security, government-controlled information and access to it, government organisation and reorganisation, homeland security, military affairs, or individual agencies that collect intelligence themselves or rely on other entities for it.[98] Further, there are informal agreements between members and staff in the Congress and officials and staff in the executive branches.[99] This organisational structure of the US intelligence community has been criticised for being a bit of a morass and it still continues to be extremely fragmented.

The DCI, who is the CIA chief himself, is seen as being weak, lacking as he does, the final budgetary and personnel authority over the agencies, (with the exception of the CIA) that are supposed to be his responsibility. In addition, the management of satellite imagery remains in a muddle, with tangled lines of authority and responsibility between the NSA, the National Reconnaissance Office and the new National Geo-Spatial Agency. Other structures have arisen in the

---

94 U.S. Senate (1976), Final Report, Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee)

95 Australian Security Intelligence Organisation Act 1979

96 Canadian Security Intelligence Service Act 1984

97 An Overview of the United States Intelligence Community for the 111th Congress, 2009

98 Frederick M. Kaiser, Congressional Oversight of Intelligence: Current Structure and Alternatives, CRS Report for Congress, available at www.crs.gov.

99 Ibid.

aftermath of 9/11, such as the Department of Homeland Security and the Terrorist Threat Integration Centre, where there is even more fragmentation and ambiguity over mission and authority definition.[100]It can even be argued that the lesson to be learnt from the United States is the danger of too much oversight. Accountability has been spread over too many committees, with oversight becoming too complicated.[101] The Department of Homeland Security for instance, has to answer to a total of 44 Congressional committees.

The United Kingdom

The Security Service (SS), which is UK's domestic intelligence agency is responsible for security threats that include terrorism, counter-intelligence, weapons of mass destruction, and organised crimes. Falling under the Home Ministry, and equivalent to India's IB, the SS, along with the Secret Intelligence Service (SIS) which is the external intelligence agency, and the Government Communications Headquarters (GCHQ), responsible for communication interception and code breaking, is one of the three tiered coordinated intelligence structure in UK.

Initially, it was the Maxwell-Fyfe directive of 1952 that was the sole officially published document detailing the work of the intelligence agencies and from where they drew their power.[102] This charter could be changed without reference to Parliament, and established no formal legal limits and controls. The operation of the intelligence services of the UK in such a legislative void was eventually challenged at the European Court of Human Rights in the case of *Harman and Hewitt v. UK*[103], where the lack of a specific statutory basis for the MI5, was held to be fatal to the claim that its actions were "in accordance with the law" for the purpose of complaints of surveillance and file-keeping, contrary to Article 8 of the convention on the right to privacy. While the ECHR permits restrictions of certain rights such as that of privacy in the interests of national security, the necessary precondition is that the restriction must be authorised by law: clearly the administrative charter fell foul of this requirement. It was following this ruling that the UK enacted a statutory charter for the SS in 1989[104], and later in 1994, for the SIS and GCHQ[105].

Further, the Interception of Communications Act 1985 allowed communications (telephone, fax, telex and post) to be intercepted when authorised by a warrant signed by a Secretary of State. It was replaced by the Regulation of

---

[100] Born, Johnson and Leigh; "*Who's Watching the Spies: Establishing Intelligence Service Accountability*, p. 58

[101] Ibid, at p. 65.

[102] Maxwell-Fyfe Directive,1952

[103] (1992) 14 E.H.R.R. 657

[104] Security Service Act 1989

[105] Intelligence Services Act 1994

Investigatory Powers Act 2000, which was designed to ensure that the UK legislation was compatible with the ECHR and the Human Rights Act 1998.[106]

Agency heads are required by the Security Service and Intelligence Services Acts to report annually to the Prime Minister and the relevant Secretaries of the government. The Foreign Secretary is responsible for the activities of the SIS and GCHQ as he signs their warrants and authorisations. Similarly, the Home Secretary is responsible for the activities of the SS and signs their warrants.

Oversight is further undertaken by the Parliament through the Intelligence and Security Committee which examines the administration, policy and expenditure of the agencies. In this the MPs are assisted by Commissioners, who review the exercise of powers by a Secretary of State and report to the Prime Minister annually. Commissioners hold, or have held, high judicial offices. In addition, tribunals appointed by the Queen and presided over by a person who either holds or has held high judicial office are tasked to investigate individual complaints into actions of the agencies.

Australia

The Australian Security Intelligence Organisation (ASIO) works closely with the Australian Protective Service, both agencies falling under the attorney general. It is influenced by British philosophy, and does not have independent arrest powers. The government's counter-terrorism approach is based on prevention, preparedness, response, and recovery. Improving intelligence capacity, increasing the effectiveness of information sharing, seeking better detection capabilities, and improving law enforcement are the overarching themes under prevention and preparedness.[107]

There is a greater separation between executive and legislative oversight roles than prevailing in UK. The parliamentary joint committee can initiate investigations or respond to requests from the attorney general. Executive oversight is stronger: there is a separate Intelligence Officer independently appointed and located in the PM's office.

Financial Accountability and Oversight in India - Budgeting & Audit of accounts-in-house, external and Parliamentary

A Directorate of Accounts (DACS) was set up in 1963 to serve the ARC and the SSB. In 1968 the R&AW and in 1984-85 the SPG were also brought under its ambit. The SSB has, however, now been taken out of its jurisdiction.

The DACS, which is headed by a Joint Secretary level officer from the Indian Audits and Accounts Service, was declared

[106] Intelligence Oversight, published by the Intelligence and Security Committee, UK

[107] James Burch, A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic intelligence Agencies and their implications for Homeland Security, *Homeland Security Affairs*, Vol. III, No. 2, June 2007.

as an organised accounts cadre for these services in 1990. Recruitment to posts in DACS is through open recruitment under the Staff Services Selection Commission.

Presently, the DACS receives allocations from two or three different budgetary sources. These allocations are lump sum grants, camouflaging details in interest of national security, but the budget proposals are drawn up following the same general procedure as in all other government departments, wherein the Financial Adviser calls for expenditure proposals from the organisation concerned and these are then finalised in consultation with the Secretary Finance (Expenditure).

The monitoring of accounts, with detailed head-wise break up is done on a monthly basis by the DACS. The expenditure is also reviewed by examination of enhancement or reduction proposals at revised estimates stage. This procedure is generally similar to that followed in other government departments - the only difference being that these details are not made public or are not accessible to legislators. Separate running ledger accounts of expenses are maintained in a nationalised bank and closely supervised by the DACS.

Audit powers are derived from the Comptroller & Auditor General of India's (CAG) and function under the Duties, Powers & Conditions of Service Act, 1971. In the first two years, audit was undertaken by the Auditor General Central Revenues (AGCR), but in 1964, the then Director, IB, B. N. Mullick proposed to the PMO to entrust the auditing function to the DACS for greater secrecy. This suggestion was accepted. Since then, the DACS conducts the audit and sends its reports, till recently termed as Inspection Reports, of different outfits under the DGS and R&AW on an annual basis. These reports are not published. The audit covers all normal expenditures relating to the establishment, services, procurement of equipment but not the Secret Service Funds (SSF) complement.

From 2008-2009 onwards, an additional annual audit report is sent by DACS to the secretary (R&AW). These reports cover the activities of the R&AW, ARC, SFF and the Procurement Division of the Cabinet Secretariat (SR Wing) and constitute the normal transaction oriented scrutiny of expenditures incurred. However, this annual audit report does not go beyond the secretary (R&AW), to a higher authority in the government. This is, perhaps a historical oversight. In 1968, there was an executive order that the audit reports should go to the Cabinet Secretary and not to the CAG but at present they are not being sent to either. There should be a 'higher, distanced authority', who should be satisfied about the veracity of the expenditures incurred. In fact, a strong case can be made out to change the nomenclature of the DACS to that of the Principal Director (Audit) for the Cabinet Secretariat.

A standing audit committee could be set up with the Secretary (R&AW), the Financial Adviser and DACS as members, to look into any specific aspects or to oversee that audit objections are being met, as is done in other government departments. Another suggestion is to undertake special audits, periodically at least, of procurement oriented projects or schemes, to review expenditure patterns and oversee if the objectives of the scheme have been achieved.

The newly set up NTRO, whose budgetary allocation comes from the PMO, is presently being serviced by an in-house accounts directorate. It is understood that there is a proposal under active consideration of the Government to have a full-fledged Additional Secretary level financial /audit official to look after NTRO work.

The IB has not been subjected to rigorous accounting and auditing scrutiny by the CAG. The Financial Adviser in the Home Ministry does oversee its budget allocations, but only the Home Secretary can give a certificate that the expenditure has been appropriate. There could be a strong case to strengthen audit mechanisms that have been avoided so far on the grounds of maintaining secrecy. This opens up the possibility that even former Home Secretaries could have entertained reservations about the IB's reluctance to submit these expenditures to scrutiny.

Secret Service Funds (SSF)

Contrary to popular perception, SSF do not form the entire budgetary allocation made from the respective budgets to the intelligence agencies but only a smaller portion thereof, which however, remains outside the purview of any audit - so far. Only a bland annual certificate of full use has to be given by the head of the organisation.

Ironically enough, the SSF portion has been steadily increasing and its unutilised component never gets surrendered, whereas other funds lapse if the project for which they are sanctioned remains unimplemented.

This understandably encourages a suggestion of misuse and emphasises the need for change and some better form of regulation without compromising secrecy. Here too, it is extremely important that the certification of appropriateness of SSF expenditure by the head of the concerned intelligence agency, with broad expenditure patterns and heads enumerated should go to a higher, distanced authority, who could be the NSA or a Minister for National Security.

Several disreputable financial practices have thrived under the garb of operational secrecy, including purchase of capital equipment like cars in violation of standard prescribed norms of the Government, or the indiscriminate hiring of Safe-Houses, which more often than not are properties belonging almost exclusively to in-house employees at different levels of seniority. In earlier times, these practices were perhaps tempered by higher standards of personal probity, but today not all of these hire or purchase powers are exercised with total judiciousness or even been warranted by strict operational needs.

Another recent practice has been to routinely engage retired employees, even in non-specialised categories and keep them employed indefinitely on hefty salaries paid from the SSF, totally by-passing the laid down government rules and regulations.

Intelligence Ombudsman/ Inspector General

Drawing upon the practices in other countries, it is essential that in India too every intelligence agency has an internal corrective mechanism to detect report and correct irregular or illegal actions. This can

be done through the institution of an Intelligence Ombudsman or Inspector General, who can be a senior retired or even sufficiently senior serving professional inured from all other pressures. He can also look into employee grievances relating to postings, promotions, etc.

Executive Oversight

Executive control should also be exercised over the agency concerned at a senior or supervisory level in the concerned line. These channels exist even today but a case can be made out for greater professionalism in the exercise of this executive control function. As of now, the manifold responsibilities vesting in both the Home Secretary and the Cabinet Secretary make it impossible for them to exercise an effective oversight on the day to day running of intelligence agencies. Heavy dependence on the head of the agency alone can impact objectivity, fairness and morale. The practice followed in some countries like the United Kingdom where in there is a separate division for looking after all establishment and financial matters pertaining to the SIS in the Cabinet Office. This arrangement could be considered for India also. This unit is headed by a very senior serving or retired intelligence official who is fully familiar with the working of the agency in question. In India, there is a Special Relations (SR) wing in the Cabinet Secretariat to process administrative and financial matters, especially those relating to the procurement of high tech equipment, but in practice, this office has functioned merely as a post office without any clout. Ideally, the executive would also exercise control over covert action and undertake a concomitant though broad scrutiny of operational funds, without compromising the secrecy of source operations.[108] At present, the NSA has been able to perform such a controlling function to a limited extent, subject to his personality and personal proclivities.

Oversight & Privacy

A major concern with regard to oversight is that of privacy**.** A recent expose of illegal phone tapping by the NTRO[109] highlighted the need to review the telephone tapping powers enjoyed by intelligence agencies in India and the safeguards for the privacy of individuals under law.

Section 5 of the Indian Telegraph Act, which specifies the powers of the government to take control over licensed telegraph operations and to order interception of messages. The provisions of the section are as follows:

(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is

[108] British Cabinet Office Paper, "Improving the Central Intelligence Machinery, July, 2009

[109] Saikat Datta, "Bootleg Tapes: The Rulers Who Listen", *Outlook*, May 2010.

necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On the occurrence of any public emergency, or in the interest of the public safety, the central government or a state government or any officer specially authorised in this behalf by the central government or a state government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the central government or a state government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section. [110]

The Supreme Court judgment in the case of *PUCL v. Union of India* issued a set of guidelines regarding telephone tapping, which are as follows[111] :

1. An order for telephone tapping in terms of Section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee concerned with in one week of the passing of the order-.
2. The order shall require the person to whom it is addressed to intercept in the course of their transmission by means a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the order.
3. The matters to be taken into account in considering whether an order is necessary under Section list of the Act shall include whether the information, which is considered necessary to acquire could reasonably be acquired by other means.

[110] The Indian Telegraph Act, No. 13 of 1885.

[111] People's Union for Civil Liberties v. Union of India and Ors. (18 December 1996)

4. The interception required under Section 5(2) of the Act shall be the interception of such communications as are sent to or from one or more addresses specified in the order belong an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises described in the order.

5. The order under Section 5(9) of the Act shall, unless renewed, cease to have effect at the end of the period of two months from the date of issue. The authority which issued the order may, at any time before the end of two month period renew the order if it by the State Government. (a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act. Where there is or has been an order whether there has been any contravention of the provisions of Section 5(2) of the Act. (b) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material. (c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.

6. The authority which issues the order shall maintain the following records:

(a) the intercepted communications ;

(b) the extent to which the material is disclosed;

(c) the number of persons and their identity to whom any of the material is disclosed;

(d) the extent to which the material is copied and

(e) the number of copies made of any of the material.

7. The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act.

8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.

9. There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, (Telecommunications), at the level of the central government. The Review Committee at the State level shall consist of the Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed under 5(2) of the Act, it shall record the finding to that effect.

It is clear from a reading of the above that only specific phone numbers may be intercepted. These are to be identified by the intelligence authority prior to the interception, with accompanying

justification. The written authorisation of the Home Secretary must be obtained before the interception can begin.

While it is true that the government has to resort to phone-tapping for some degree of intelligence gathering, it is also true that the prevalent safeguards have not been very effective. In actual implementation or practice of day to day snooping, practical problems of discretion may crop up. If the specific phone number is not available, then how can its interception be authorised? If the target is a VIP, why will the Home Secretary give a written authorisation?

The NTRO uses its equipment to search for that one possible number having a bearing on national security from among thousands of others which may not be that relevant. In course of a random search, it may intercept a thousand calls and all of them illegally. The equipment may be deployed every day in some part of the country or the other. The prior authorisation of the Home Secretary cannot be guaranteed. One way could be to safeguard a few VIPs, including senior intelligence officials, by creating a set of mobile numbers that cannot be tapped. The scanning machine could be programmed to shut down on detecting this number. However, how many numbers can be secured and protected in the long-run or how could such self-restraint be ensured? Appropriate checks and balances have to be carefully drawn up in this regard.

Parliamentary Oversight

Parliamentary oversight has been a very sensitive, almost taboo subject amongst the intelligence fraternity in India. Speaking on the occasion of the fourth R.N. Kao memorial lecture in January, 2010 Vice President, M. Hamid Ansari categorically flagged the issue as to 'why a democratic system like ours should not have' some form of parliamentary accountability. Dwelling at length on the possibility and scope of misuse of intelligence agencies, and the widespread perception in media about instances of intelligence lapses or failures in related issues like co-ordination, he said it was essential for India to adopt the accountability practices prevailing in democracies worldwide. Ansari identified three models of intelligence oversight:

(a) **Comprehensive**- to include both policy and operations, as in the USA and Germany;

(b) **Limited** to matters of policy and finance, as in the UK;

(c) **Focused on human rights** and rule of law, as in Norway;

Ansari himself favoured an oversight body that would be given some access to operational details, so as to ensure effective supervision and improve the efficiency of intelligence agencies[112] .

There is likely to be considerable furore, debate and opposition to the proposed scrutiny of intelligence agencies in the name of oversight. The composition of a

[112] Address of Vice President M. Hamid Ansari at 4th Kao Memorial Lecture, Jan 19, 2010: "Intelligence for the World of Tomorrow"

compact but effective legislative body in an increasingly fractured legislature, dependent on small regional parties may itself pose problems. One suggestion given by senior retired professionals conversant with the issue was that there could be a Minister for National Security and Intelligence, who could also double up as the NSA to the Prime Minister and who would be responsible to the Parliament. This would ensure that there were no security leaks.[113]

Another suggestion is for the PM to set up a small Ministerial Committee with the power to oversee the functioning of intelligence agencies, and the proper use of secret service funds.[114] A more conservative view is that an oversight committee set up by the Parliament, headed by the Vice President and comprising the Speaker of the Lok Sabha, the Prime Minister, the Minister for National Security/Home Minister/NSA, the Leader of the Opposition in the two Houses of the Parliament, should monitor the performance of intelligence organisations[115]. While all policy, administrative and financial matters pertaining to the intelligence agencies may come under the purview of this Committee, specific operational matters may remain outside its ambit.[116]

[113] Brajesh Mishra, IDSA Round Table, Aug 2010;

[114] V. Balachandran, Paper on Intelligence reforms: IDSA Task Force deliberations;

[115] A Private Member's Bill on providing a legal framework for intelligence agencies, moved by Shri Manish Tiwari, MP, in Lok Sabha.

[116] A. K. Verma, IDSA Roundtable, Aug 6, 2010 ;

Conclusion

Several efforts have been made in the past to bring about reforms in the intelligence sector. Our contention in this report is that these efforts have been piecemeal and ad hoc. New organisations were created but no thought was given to prevent overlaps of jurisdiction or turf wars on the creation or sharing of expensive new technical assets or know-how.

Given the immense new security challenges confronting India as it emerges as a global power, we believe that a paradigm shift is needed to modernise intelligence work in a holistic manner, which may require radical changes in the existing intelligence culture.

We are mindful of reservations within the intelligence community, especially among police officers in the profession, that excessive harping on accountability could damage operational efficiency and jeopardise secrecy. Yet, it has been felt, on balance, that there can be no getting away from introducing some sort of external supervision and control, including legislative oversight to improve efficiency and to build in self-correcting mechanisms.

The current moral crises across a range of institutions have given rise to this justifiable clamour for institutional reform and political accountability. We believe that to tackle the widely perceived incompetence and malfunctioning of intelligence agencies- it will be necessary to implement a wide ranging set of reforms to improve and empower intelligence agencies.

Even the smallest of reforms can become hostage to divisions, rancour or the monumental short-sightedness prevailing within the intelligence community. This must be avoided. A balanced approach towards systemic and institutional changes is required. Any changes within institutions should be invested with an ethical purpose and it must be ensured that if new institutions are set up, they should not reproduce the pathologies of the existing ones! Any such effort is for the long haul. We hope this exercise can contribute in some small measure to promote a debate on the issue.

It is argued by some that the total expenditure on intelligence agencies in India may be a just a few thousand crores of rupees, which is nothing compared to various multi-billion scams in the country. Therefore, even if there is some misuse/ improper use of funds by intelligence agencies, the nation should take it in its stride and not rake-up unnecessary controversies. It may be mentioned that here the issue is not just money and resources, it is the security implications of the imperfect functioning of the intelligence agencies for the country in terms of security, pride and stability. The Indian intelligence community has for too long fallen short of these expectations and now is the time to remedy the lacunae.

Lastly, any intelligence reforms must also address the internal man-management structures and policies of the intelligence agencies and provide for an effective and satisfactory grievance redressal mechanism. An intelligence agency with a dissatisfied and aggrieved work force can neither safeguard its own security nor that of the nation's.

TASK FORCE MEMBERS

R Banerji
P K Upadhyay
Harinder Singh

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

9 789382 169031