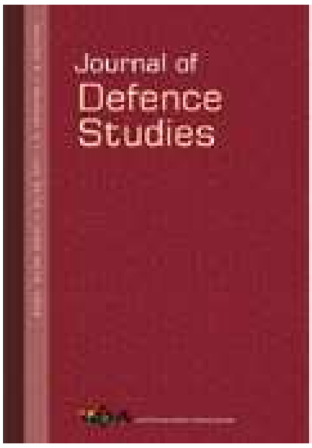

The Evolution of India’s National Security Architecture

P.S. Raghavan

Views expressed are those of the author(s) and do not necessarily reflect the views of the IDSA or of the Government of India.

The Evolution of India's National Security Architecture

P.S. Raghavan[*]

The Kargil War of 1999 focussed the nation's attention on shortcomings in India's national security management system, which was largely inherited from the British in 1947. A comprehensive review resulted in a major overhaul, ensuring tighter coordination between the various security structures, reforming the higher defence organisation, and bringing in a holistic approach, recognising the political, economic, technological, ecological and sociological factors impacting on national security. A set of reviews in 2017-18 resulted in further structural reform, taking cognizance of the global geopolitical flux, a revolution in the nature of military conflict, the transformative role of technology in every aspect of internal and external security, and the challenges arising from India's strategic ambitions. The reformed and new structures emerging from these reviews are still a work in progress. Their functioning as a smooth, well-oiled national security machinery would require a coordinated, all-of-government approach.

In the public discourse in India, the term 'national security' is often conflated with the defence of national borders. This is the sense in which it figured in the campaign rhetoric of the recent general elections. However, the national security establishment—particularly after the nuclear tests of 1998 and the Kargil War in 1999—has developed a more holistic approach to national security and established structures to tackle it in all its aspects. The role and functioning of these structures have not

[*] The author is a former diplomat and now Chairman of the National Security Advisory Board.

ISSN 0976-1004 print
© 2019 Institute for Defence Studies and Analyses
Journal of Defence Studies, Vol. 13, No. 3, July–September 2019, pp. 33–52

attracted adequate attention or analysis, though much of the information about them is in the public domain.

This article analyses the evolution of thinking in the Indian government on national security challenges, the structures created to address them and the effectiveness of their functioning. It identifies continuing and emerging challenges as well as the way forward to further reinforce India's national security architecture.

The Pre-1999 System

The procedures established to deal with national security immediately after independence in 1947 were based on a framework recommended by Lord Ismay (Lord Mountbatten's Chief of Staff) to the government of newly independent India. The main pillar of this system was the Joint Intelligence Committee (JIC) under the Chiefs of Staff Committee (COSC) of the armed forces, which was to provide integrated intelligence assessments on defence-related matters to the COSC and the Union Cabinet. The JIC was progressively strengthened and upgraded over the years, and its mandate widened to include both internal and external threats to national security. However, its limitations as an effective source of integrated national security advice to the leadership were repeatedly exposed.[1]

Political decisions on security issues were taken by the Cabinet or its relevant committee. At the official level, a Committee of Secretaries headed by the Cabinet Secretary considered these issues. These bodies tended to focus on immediate law and order, defence, terrorism and insurgency threats. They had neither the information inputs nor the time to recognise broader trends, or to evaluate medium or long-term policy options. This often prevented a holistic approach towards security, including an assessment of the impact of economic, social or environmental factors on it.[2] There were a few attempts to address this lacuna, with indifferent results. Ad hoc advisory bodies set up, during the tenure of Prime Minister Rajiv Gandhi, for multidisciplinary inputs on security-related issues did not last long.[3] Again, in August 1990, the government set up a National Security Council (NSC) to evolve an integrated approach to national security policymaking. A Strategic Core Group (SCG), headed by the Cabinet Secretary, was to assist it. This NSC met only once, in October 1990, and was not convened thereafter.

The difficult security environment leading up to, and following, the nuclear tests of 1998, once again, provided the impetus to efforts for a holistic approach to India's national security challenges. A task force, headed by then Deputy Chairman of the Planning Commission, K.C. Pant, was requested to recommend an appropriate national security management system, drawing on the experience of other countries. Based on the recommendations of this task force, the government constituted an NSC in April 1999, with the Prime Minister, Home Minister, Defence Minister, External Affairs Minister, Finance Minister, and Deputy Chairman of the Planning Commission as its members.[4]

The resolution announcing the creation of the NSC stated that its purpose was to promote 'integrated thinking and coordinated application of the political, military, diplomatic, scientific and technological resources of the State to protect and promote national security goals and objectives.'[5] It was further specified that the NSC's deliberations would include:

1. the external security environment and threat scenario;
2. threats involving atomic energy, space and high technology;
3. global economic, energy and ecological threats;
4. internal security, counter-insurgency, counter-terrorism and intelligence;
5. patterns of alienation: social, communal and regional;
6. trans-border crimes: smuggling, traffic in arms and narcotics; and
7. intelligence collection, coordination and analysis.

The post of a National Security Adviser (NSA) was also notified. Brajesh Mishra, the then Principal Secretary to the Prime Minister, was to hold additional charge of this post. The SCG of the 1990 notification was renamed Strategic Policy Group (SPG), with an expanded composition. The notification confirmed the status of the National Security Advisory Board (NSAB), which had already been constituted in December 1998, as an advisory body of eminent persons outside the government to render advice on national security issues referred to it by the NSC.

A National Security Council Secretariat (NSCS) was set up to assist the NSC, NSAB and SPG. One of its tasks was to prepare papers for the consideration of the NSC and SPG. It also inherited the intelligence integration role of the JIC, which merged into the NSCS. It was stipulated that all ministries/departments shall consult NSCS on matters having a bearing on national security.

Post-Kargil Developments

The Kargil conflict in May 1999 had a profound impact on the approach towards national security, because it focused national attention on its multiple dimensions. As the war unfolded on TV screens across the country, there were public discussions on intelligence voids, coordination gaps, technological shortcomings and structural issues that could have been better handled before and during the crisis. This led to an in-depth internal government review, which resulted in decisions by the Cabinet in July 1999 on the role and functions of the various elements of the newly created system, and measures to equip it with the required multidisciplinary expertise.

The government constituted the Kargil Review Committee (KRC), headed by a strategic analyst, K. Subrahmanyam, to review the events leading up to the Kargil War and to recommend measures to safeguard against such armed intrusions. The KRC Report (December 1999) recommended, inter alia: a thorough review of the national security system in its entirety; more effective tasking, evaluation and coordination of intelligence agencies; strengthening of their technical capacities; improved border management structures and procedures; and better civil–military liaison mechanisms.[6]

The government then constituted a Group of Ministers (GoM) in April 2000 to review the national security system in its entirety, focusing on external and internal threats, and to formulate specific proposals for implementation. The GoM was headed by the Home Minister and included the ministers of Defence, External Affairs and Finance. The NSA was a special invitee. The GoM set up four task forces—on intelligence, internal security, border management and defence—with membership drawn from acknowledged experts in these fields.

In February 2001, the GoM submitted its recommendations, drawing from the reports of the four task forces, as well as the KRC's recommendations. In May 2001, the Cabinet Committee on Security (CCS) approved all the recommendations, except the one on the institution of the Chief of Defence Staff (CDS), which the CCS felt needed consultation with 'various political parties'.[7] This body of decisions is the foundation of the current national security management system. It was the first comprehensive review of the county's security mechanisms in their entirety and the first (and only one) to be made public, after excision of sensitive information (mainly relating to intelligence).[8] Over the years, these structures and mechanisms have been reinforced and new ones added, in response to emerging challenges.

The National Security Council System

The KRC recommended that: the intelligence agencies should be tasked as per the requirements of security agencies; there should be close coordination between them to plug intelligence voids; and they should be equipped with modern technological tools, even while avoiding unnecessary duplication of expensive, sophisticated technical equipment. Such equipment could be centrally procured and used as a common resource by all concerned agencies. These recommendations were incorporated in the GoM Report and resulted in the establishment of an Intelligence Coordination Group (ICG), a Technology Coordination Group (TCG) and the National Technical Facilities Organisation (which, in 2004, was renamed the National Technical Research Organisation [NTRO]).

The ICG's role was to provide 'systematic intelligence oversight', take decisions on the allocation of resources to the intelligence agencies, task them and evaluate their output, on the basis of the feedback from the users of the intelligence. The TCG was to oversee the technical intelligence (TECHINT) capabilities of the intelligence agencies and coordinate their acquisition of 'new, costly, major strategic facilities/ equipment', to maximise their technical capabilities, while avoiding unnecessary duplication in the procurement of expensive assets.

The idea of an apex TECHINT organisation emanated from the KRC Report, drawing inspiration from the United States (US) National Security Agency, and was endorsed by the GoM. This apex organisation was to set up and operate all major, new TECHINT facilities, keeping in view the need to integrate multiple emerging technologies. However, as Satish Chandra has described in detail, the translation of the concept into implementation faced multiple organisational and budgetary challenges. After a detailed study by a task force, headed by the then Principal Scientific Adviser to the Government of India, Dr A.P.J. Abdul Kalam, NTRO was eventually established in 2004.[9]

The need to break down the silos between intelligence agencies was emphasised by both the KRC and the GoM. Real-time dissemination of relevant intelligence to law enforcement agencies was to be the responsibility of the Multi-Agency Centre (MAC), set up by the government in 2001, with Subsidiary Multi-Agency Centres (SMACs) across the country.

According to the most recent available public information, a total of 429 SMAC nodes and 251 district police offices are connected to the MAC–SMAC network, which covers all the states of the country. A National Memory Bank (NMB), linked to this network, functions as a central databank for information related to counter-terrorism.[10]

The decision to establish a National Intelligence Grid (NATGRID) followed the 2008 Mumbai terrorist attacks.[11] The purpose of NATGRID was to connect diverse databases, covering telecommunications, Internet usage, property transactions, financial transfers, immigration records, air and rail passenger information and tax returns, to create a strong analytic base for generating early warning of terrorist activities or organised crime. This combined data would then be made available to central intelligence, investigative and tax authorities. While this initiative is invaluable for criminal investigators, it faces a number of challenges, including big data analytical techniques, inter-regional flows, privacy concerns and departmental obstructions. Issues of structural, procedural and technology safeguards, as well as of oversight mechanisms, remain to be resolved.

The KRC and GoM stressed the importance of effective integration of relevant economic intelligence into the analyses of intelligence agencies. For this, they recommended broadening the mandates of the Economic Intelligence Council (EIC) and the Central Economic Intelligence Bureau (CEIB), as well as setting up a Financial Intelligence Unit (FIU) to monitor currency flows linked to organised crime or terrorism. The EIC is now an apex body, which brings together all economic agencies, including customs, tax, narcotic control and revenue intelligence, with the 'traditional' intelligence agencies and the NSCS, under the chairmanship of the Finance Minister. An FIU was set up in 2004 to monitor major cash transfers, cross-border financial movements, suspicious property transactions and international financial flows with possible terror linkages. The FIU represents India in the Financial Action Task Force (FATF), which drives international cooperation against money laundering, terrorist financing and other threats to the international financial system.

The GoM also recommended fundamental reforms to the system of higher defence management, including: the appointment of a CDS; development of a holistic long-term defence perspective plan, based on rigorous inter- and intra-service prioritisation; creation of a tri-service Defence Intelligence Agency (DIA); and a progressive delegation of decision-making powers to service headquarters, which would become an 'Integrated Headquarters' of the Ministry of Defence (MoD), rather than 'Attached Offices'.[12] A number of reforms were implemented, improving operational and administrative efficiencies. However, the postponement of the decision on a CDS diluted the force of many other proposed reforms, including more effective 'jointness', participation of the forces in the defence planning and strategy process, and dovetailing the inter-service and intra-service resource allocations with the National Security Strategy. The establishment of a National Defence University too is not progressing at the intended pace.

Following India's emergence as a nuclear weapons power after its nuclear tests of 1998, a Strategic Forces Command (SFC) was set up. In January 2003, the CCS approved the appointment of a Commander-in-Chief (C-in-C) of the SFC and authorised the first articulation of India's nuclear doctrine. It confirmed the existence of a Nuclear Command Authority (NCA), comprising a Political Council, chaired by the Prime Minister, and an Executive Council, chaired by the NSA, to provide inputs for decision making and execute the directives of the Political Council, which is the sole body that can authorise the use of nuclear weapons.[13] The CDS was to exercise administrative control over the strategic forces. In the absence of a CDS, the Chairman, COSC exercises this role.

The Cabinet Secretariat Resolution of 16 April 1999 said that the SPG, chaired by the Cabinet Secretary, would be the 'principal mechanism for inter-ministerial coordination and integration of relevant inputs in the formulation of national security policies.'[14] The SPG membership included the service chiefs, Governor of the Reserve Bank of India, Secretaries of the ministries of Home, Defence, External Affairs, Finance, Space and Atomic Energy, heads of intelligence agencies, and the Secretary NSCS (who was also the Deputy NSA). It was stated that the Cabinet Secretary or the NSA could call meetings of the SPG.

National Security Advisor

The Cabinet Secretariat Resolution of 16 April 1999 stated that the NSC 'shall have a National Security Advisor, who shall function as the channel for servicing the NSC.'[15] It did not expand on the NSA's role. The ambiguity was reinforced by the description of the SPG as the 'principal mechanism' for inputs into national security policy formulation and, further, by locating the NSCS in the Cabinet Secretariat. The fact that the first NSA, Brajesh Mishra, was also the Principal Secretary to the Prime Minister enabled this ambiguity to be papered over. However, subsequent government decisions, including the CCS's acceptance of the GoM Report, clarified the NSA's pivotal role in national security policy formulation and implementation. In March 2002, the NSCS was formally designated a 'special unit' under the direct charge of the NSA in the Prime Minister's Office. Later, in accordance with the GoM recommendations, as approved by the CCS, it was also clarified that the NSA would chair the ICG and TCG. The NTRO would function under his supervision.

The posts of Principal Secretary to the Prime Minister and the NSA were separated in 2004, but the NSA continued to be a part of the Prime Minister's Office. Underlining the importance of these areas for national security, the NSA was to assist the Prime Minister on foreign policy, defence, atomic energy and space issues (besides internal and external security). In June 2003, India and China appointed Special Representatives to address the boundary problem from a political perspective and to directly report to their leaders. Prime Minister Atal Bihari Vajpayee appointed his NSA as India's Special Representative and since then, the NSA has been India's Special Representative.

In the early 2000s, India was among the relatively few countries with the institution of an NSA. Today, every major country has one, though the designation may not be the same. Typically, the NSA (or equivalent) is appointed directly by the executive head of government, is someone who enjoys his/her confidence, has immediate access and coordinates national security-related actions of the government. Therefore, the quickest and most effective means to reach a foreign head of government during times of crises is through the NSA. It is now a well-established channel for urgent communications between heads of state or governments of strategic partner countries. Periodical dialogues of our NSA, his deputies and secretariat with their counterparts in major countries are also regular features.

National Security Council Secretariat

As mentioned earlier, the NSCS was set up for 'servicing' the NSC, NSAB and SPG, and tasked with the preparation of papers for the NSC and the SPG. It also inherited the intelligence-related functions of the JIC. This involved the extraction of strategic intelligence from multiple intelligence and open-source inputs, so as to provide decision makers with policy options to meet security threats and challenges. It also involved tasking intelligence agencies and reviewing their output, in consultation with the consumers. This was done in the ICG.

Over the years, NSCS's role and functions have evolved, based on the recommendations of the GoM and responding to new developments. Its role in establishing the national cybersecurity architecture and coordinating the cybersecurity-related policies of the government has been particularly important. Presently, a National Cybersecurity Coordinator (NCSC) in the NSCS, with a comprehensive charter of responsibilities, coordinates this activity.[16]

The NSCS also represents India in the Shanghai Cooperation Organisation's (SCO) Regional Anti-Terrorist Structure (RATS). It is the secretariat for multilateral NSA-level dialogues, including in BRICS (Brazil–Russia–India–China–South Africa); Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC), which includes India, Nepal, Bhutan, Bangladesh, Myanmar, Thailand and Sri Lanka; Russia–India–China dialogue on Afghanistan; and the India–Maldives–Sri Lanka Maritime Trilateral. It coordinates bilateral NSA and Deputy NSA-level dialogue with over 20 countries.

In addition to 'traditional' areas, the NSCS has been engaged with issues in space security, environmental security, geospatial sciences, maritime security, blue economy, strategic minerals, rare earths, pandemics and technology security, involving coordination of actions by various departments and agencies and drafting of national policy papers.

The NSCS has been periodically expanded to equip it for its enlarged responsibilities. In 2001, the GoM had emphasised the importance of enhancing its analytical capabilities, through creation of a strong cadre of analysts, attracting the best expertise from within and outside the government and encouraging mobility between departments and agencies of the national security establishment. Neither the expansion nor the induction of specialised personnel was carried out to the extent recommended by the GoM.

After a change of government in New Delhi in 2004, some changes were made in the organisation of work within the NSCS, including: the revival of the JIC as a separate division; creation of a project division to monitor the nuclear doctrines and postures of other countries; a policy division to prepare policy option papers (and to service the NSAB and SPG); and a defence division to focus on the modernisation of the defence forces and the credibility of India's nuclear deterrence.[17]

In 2011, about a decade after the fundamental restructuring of the national security apparatus, the government appointed a task force, headed by the then Chairman of the NSAB, Naresh Chandra, to review the system and suggest course corrections as may be required. The report of the task force, submitted in 2012, was not made public, but some media reports[18] indicated that the recommendations included: the appointment of a Permanent Chairman of COSC (instead of a CDS, on which the members of the task force could not reach a consensus); some suggestions for better integration of the service headquarters and the MoD (unfinished business of the GoM recommendations); improvement of intelligence coordination; and a coherent strategy to source and obtain secure access to critical raw materials for the civilian and defence industries. There is no evidence of any significant government action on the recommendations of the task force.[19]

Review and Restructuring, 2017–18

The GoM had recommended in 2001 that, in view of the rapidly changing security environment, another comprehensive review of the national security management should be undertaken after five years. The changes made in 2005–06 were limited in scope. The review in 2011–12 did not result in any significant changes, before a change of government in 2014. In 2017, however, the NSAB initiated an exercise, in collaboration with NSCS, to review the system and to recommend responses to the transformation of India's strategic environment over the past two decades. This exercise, along with other parallel reviews within governmental bodies, resulted in decisions for a restructuring of existing mechanisms and creation of some new ones.

The flux in great power relations has created new uncertainties in India's strategic environment. The global commons in oceans, and in space, are being increasingly contested. Technology has transformed the character of war, terrorism, crime and internal security challenges. In military conflict, conventional and nuclear forces are reinforced by actions in the cyber, space and information domains. Patterns of terrorism are changing, with innovative use of social media and new technologies. Cybercrime, sub-national movements, demographic disruptions, water conflicts, agrarian distress and various social issues pose new domestic challenges. Energy security, ecological balance and secure access to critical raw materials need to be factored into a national security strategy. With the advent of 5G, technology will be even more intimately intertwined with politics, economics, defence and security. It is imperative that our national security structures are suitably upgraded to effectively tackle these challenges. This includes their staffing, skill sets and systemic capacity to develop strategies and harmonise approaches across ministries, agencies and non-state actors.

The NSCS is consequently being expanded, to induct domain experts from within and outside government. Its work is now organised in four verticals, three headed by Deputy NSAs and the fourth, the military vertical, headed by a Military Adviser of the same rank. The strategic affairs vertical will deal with strategic and security interests in the neighbourhood and in key geographies. The technology and intelligence vertical will work on infusion of the latest technologies for intelligence, civil and military applications, and coordinate efforts to plug technology gaps. The internal affairs vertical will focus on next-generation threats, in addition to the ongoing issues in Jammu and Kashmir, the North-East, counter-terrorism and counter-insurgency. The Military Adviser will provide a military perspective to security policymaking; his vertical will also focus on military developments in the neighbourhood and defence requirements in India's strategic environment. These are broad indicative descriptions; there will be a number of cross-cutting issues, requiring coordination between various verticals. In addition, the plan is to induct professionals who can work on economic, sociological, ecological and legal aspects of national security policy.

An anomaly created in 1999 has been corrected in 2018, with the reconstitution of the SPG, with NSA as its Chairman.[20] There is an obvious logic in this. The development of the NSA's role and functions has clearly established his position as the principal security adviser to the NSC. It is, therefore, appropriate that he should chair the SPG, which is 'the principal mechanism for…integration of relevant inputs in the formulation of national security policies.'[21] For the rest, the new SPG has retained the composition of its predecessor, except for the addition to it of the Vice Chairman of Niti Aayog. In 1999, the Deputy Chairman of the Planning Commission was a member of the NSC; later on, the Vice Chairman of the successor organisation, Niti Aayog, was not. His inclusion in the SPG, in 2018, indicates a recognition of the importance of a developmental perspective in national security strategy.

As mentioned earlier, reforms in higher defence management remained incomplete. Among the issues that had not been satisfactorily addressed were: the rational allocation of resources between the three services; alignment of defence capability with strategic objectives; and dovetailing procurement procedures with defence manufacturing and export goals. The GoM Report had envisaged a pivotal role for the CDS, heading the Headquarters of Integrated Defence Staff (HQ IDS), in dealing with these problems. In the absence of a decision on the CDS, or an alternative mechanism in its place, the government decided to create a consultative structure to generate recommendations on these issues.

A Defence Planning Committee (DPC) was notified by the MoD in April 2018. It was chaired by the NSA and included the three service chiefs, the defence, foreign and expenditure secretaries and the Chief of IDS. It was reportedly tasked with drafting a national security strategy, drawing up strategies for promoting defence manufacturing and exports and recommending initiatives in defence diplomacy.[22] Four sub-committees were to be constituted on policy and strategy, capability development, defence diplomacy and defence manufacturing ecosystem.[23] The DPC will submit recommendations on these issues to the Defence Minister, for further consideration and approvals by the CCS.

It was announced in October 2018 that a Defence Space Agency (DSA) would be constituted, as a platform for integration and optimal use of space resources. In June 2019, the CCS approved the contours of the DSA, which would include representatives of the armed forces, the Indian Space Research Organisation (ISRO), and the Defence Research and Development Organisation (DRDO), and would be tasked with developing a range of platforms to protect Indian assets in space. It was clarified by the government that India continues to oppose weaponisation of space and supports international cooperation for the safety and security of space-based assets. However, the country cannot remain oblivious to emerging realities, including the recent creation of a US Space Command and similar initiatives by other major powers. The successful anti-satellite missile test in March 2019 was intended to demonstrate the capacity to meet threats to India's growing space-based assets. There are reports of plans to set up a defence space research organisation for developing further counter-space capability.[24]

In response to the recent explosion in offensive and defensive cyber technologies, the government has also announced the establishment of a Defence Cyber Agency, to develop measures and strategies to defend India's military assets, including critical infrastructure, against cyber threats.

The functioning of the NSAB has also been reviewed to see how it could be made more responsive to the needs of the national security establishment. While reconstituting the Board in January 2019, a diversity of domain expertise has been introduced, including (among others) foreign and strategic affairs (including neighbourhood experience), intelligence, internal security, international commerce, finance and emerging technologies. The NSAB can co-opt other domain experts for specific studies. As per its original mandate, the NSAB considers subjects referred to it by the NSC or by government departments or agencies. The idea is that its members can draw on their experience and expertise to give serious consideration to important issues, without being hampered by the day-to-day preoccupations that take up an inordinate proportion of the time of those in government. In addition, the NSAB aims to develop into a bridge between the national security establishment and think tanks/ research institutions working on national security and strategic affairs, so as to enhance communication and understanding of national security policies and perspectives. Looking ahead, it could also act as a receptacle of public views on national security-related issues, which it could funnel back to the national security establishment.

Continuing Challenges

The expansion in the size and capacity of the national security structures is necessarily a gradual process. It is still a work in progress. The expanded NSCS and the new structures—DPC, the cyber and space agencies, the reconstituted SPG—all need to establish methodologies of functioning that mesh into the larger national security strategy. The staffing of these structures, with the required domain expertise over the wide canvas of their activities, would be a major exercise. The intention is to tap such expertise from within and outside government. This means a departure from normal government selection procedures and remuneration packages, to attract the best talent in various disciplines. This effort may also be made more difficult by a pervasive shortage of manpower trained in national security matters. Arvind Gupta has noted the acute need to train professionals in areas like counter-terrorism, cybersecurity, net assessments and geospatial intelligence, so that they can function effectively within various national security structures.[25]

As these structures come to terms with their responsibilities, they will confront the systemic issues that have plagued national security management over the decades. Coordination of activities is often hampered by 'turf' concerns, which result in imperfect real-time information sharing and resistance to coordination supervision. This problem is not unique to India; it haunts professionals in the national security establishments of even developed countries. Each country finds workable solutions within its framework of governance; India has to do the same. The MAC–SMAC networks need to be strengthened and expanded in geographical and domain reach. Projects like NATGRID underline the potential of technology as a powerful tool in tackling crime and countering terrorism. But they have to overcome political frictions between the central and state governments, provide credible assurances against misuse of personal information, ensure integrity of data and satisfy the courts about protection of individual freedoms, including privacy.[26]

Despite all the efforts undertaken since 2001, the reform of various aspects of the higher defence organisation remains incomplete. Many in the armed forces feel strongly that the reforms stopped well short of ensuring meaningful involvement of the services in defence planning and strategy formulation. According to this view, the reforms did not address the chronic issues in civil–military relations, including the dynamics of interactions between the service headquarters and the MoD.[27]

There are continued divisions within the defence establishment and the strategic community on the subject of the CDS. The GoM Report identifies four main roles of a CDS: (i) provide single-point military advice to the government; (ii) exercise administrative control and management of the strategic forces; (iii) oversee intra-service and inter-service acquisition and allocation priorities; and (iv) promote 'jointness' in the armed forces. While describing the role of the CDS as the 'Principal Military Adviser of the Defence Minister', the report emphasises that the role of the Defence Secretary as the 'Principal Defence Adviser' to the Defence Minister should not be diluted.[28] Arun Prakash and others have argued that in the existing system, the government receives only military advice that has been filtered by the bureaucracy; the Chairman, COSC does not have the time to attend to the management of the strategic forces; he is unable to rise above service loyalty to formulate objective resource allocation options; and (flowing from the above) the achievement of 'jointness' has been limited.[29]

The DPC could make a serious contribution towards promoting synergy in tri-service strategies, including intra-service and inter-service prioritisations. Its additional task of evolving strategies for indigenisation of defence capability provides a welcome focus on an area of significant vulnerability in national security. India, today, has the dubious distinction of being among the world's largest arms importers. The Narendra Modi government has clearly enunciated the goal of indigenous defence manufacturing, to reduce the vulnerabilities caused by overwhelming external dependence. However, the 'Make in India' initiative has made only modest progress in the defence sector. A number of systemic changes are required to create an ecosystem more conducive to indigenous research, development and manufacture. This means moving out of the straitjacket of current procurement procedures, creating an investment-friendly regime and a level playing field for the private sector vis-à-vis the public sector. The DPC could generate practical recommendations for development of this ecosystem, since it includes representatives from the ministries that would make the required policy decisions for its implementation. The DPC can do a Strategic Defence Review, flowing from a National Security Strategy, to be defined in consultation with all relevant stakeholders. This would form the basis for the Operational Directives of the Defence Minister, a joint military doctrine formulation by the IDS, and long-term perspective operational and acquisition plans.

Going beyond this, the government has to engage in resolving the other pending issues in civil–military relations, including closer involvement of the military in national strategic and defence planning. The DPC may take up some of the urgent issues that would normally have been handled by a CDS, but this does not diminish the rationale for a CDS. The DPC is not a long-term solution to long-standing issues in higher defence management. It is a band-aid, not a cure.

The rationale for a CDS has been discussed threadbare in the defence establishment and the strategic community. Opposition from within the armed forces and from some official quarters has ensured that successive governments have not appointed a CDS. The GoM has outlined the methodology of functioning of a CDS and has suggested consultative procedures to reconcile the interests and allay the concerns of the various constituencies that would be affected by this appointment. It would be desirable for the government to bite the bullet and take this decision. In most countries, the appointment of a CDS has been a top-down decision.

The national security implications of the overwhelming impact of technology on society have been noted. As technology transforms societal behaviour and actions, the sources of technologies have become the focus of national security concerns. Fast-paced developments in the rollout of 5G technology and the US warnings to its partners against Chinese 5G technologies have created dilemmas for a number of countries. Our national strategy for deployment of 5G technologies would have to consider political, economic, technology and security implications. Besides the dominance of Chinese smartphones in the Indian market, Chinese equipment is widely deployed in India's telecommunications and other infrastructure industries. There may, therefore, be time and cost implications of developing 5G systems without building on existing Chinese equipment. At the same time, a US-China technology cold war, which appears to be in the making, would increase US pressure on India to boycott Chinese products. The facts and myths about the security implications of various competing products need to be carefully sifted. Getting Indian patents accepted for 5G standards and encouraging India-based companies to design and manufacture 5G equipment in India are desirable objectives, which may have to be rescued from vested interests in India and abroad. These challenges require addressing by an all-of-government approach, with the participation of all relevant stakeholders and directions from the political leadership. The expanded and strengthened NSCS would have an important role in this endeavour.

The extraordinary churn in international politics over the past decade has impacted on India's strategic and security interests. Our relations with the US, Russia and China have been complicated by the course of the bilateral relations among them. The US–Russia standoff has reached a level of acrimony comparable to that during the Cold War. This has resulted in American pressure on India to dilute its relations with Russia, particularly in the defence sector. The interest of US business in the huge Indian arms market has reinforced this pressure. India has been gradually diversifying its defence acquisitions since 2000, moving away from a near-total dependence on Russia, but any abrupt disengagement would cause major defence vulnerability, involve huge expenditure and damage the current strategic partnership with Russia. Moreover, India-Russia relations are important not only for defence cooperation, but also (among other reasons) because of Russia's geographical location adjacent to India's extended neighbourhood, and India's desire to retain strategic autonomy from the great powers to avoid being caught in the crossfire between them.

The development of India's relations with China since 2000 has resulted in strong trade and investment links, alongside strategic challenges stemming from China's activities in India's near and extended neighbourhoods. India's strategic partnership with the US has gained in vibrancy since 2000. Besides mutual interest in trade, investment, defence and technology ties, the US sees a strong India in Asia as an important partner, particularly in the context of a resurgent China. The ongoing US–China trade war and the looming 5G war may present India with both opportunities and difficult choices. Managing these three bilateral relationships in accordance with India's strategic interests needs a nuanced political and economic approach, which may involve compromise in some areas to secure desired outcomes in others. In many ways, a similar cross-sectoral approach is required in relations with India's neighbours in South Asia and its wider neighbourhood in West, South-East and East Asia—each of these are also areas of involvement of the three great powers.

Modern-day national security management thus needs an appreciation of the complexity, multidisciplinary nature and international reach of the challenges, and a coordinated approach to tackling them. The recent reform of the national security structures demonstrates recognition of this reality and the determination to address it effectively. The implementation is still a work in progress. It is important to disseminate a broader understanding of the country's national security perspectives to think tanks and the general public, so that the country's national security strategy has a broader public support base.

Notes

1. S.D. Pradhan, 'National Security System—Evolution', in Satish Kumar (ed.), *India's National Security: Annual Review 2010*, New Delhi: Pentagon Press, 2010, pp. 435–49. The chapter describes in detail how the JIC mechanism worked in the early years of its existence.
2. Satish Chandra, 'National Security System and Reform', in Satish Kumar (ed.), *India's National Security: Annual Review 2005*, New Delhi: Pentagon Press, 2005, p. 202.
3. K. Subrahmanyam, *Shedding Shibboleths: India's Evolving Strategic Outlook*, Delhi: Wordsmiths, 2005, pp. 22–23.
4. Cabinet Secretariat Resolution No. 281/29/6/98/TS, dated 16 April 1999, *The Gazette of India*, 19 April 1999, available at https://archive.org/details/in.gazette.e.1999.383, accessed on 22 May 2019.
5. Ibid.
6. *From Surprise to Reckoning: The Kargil Review Committee Report*, New Delhi: Sage, 2000.

7. The CCS decisions were summarised in a press release, Press Information Bureau (PIB), 23 May 2001, available at http://pibarchive.nic.in/archive/releases98/lyr2001/rmay2001/23052001/r2305200110.html, accessed on 24 May 2019.
8. *Reforming the National Security System: Recommendations of the Group of Ministers,* February 2001. The text, as tabled in the Parliament, is available at https://www.vifindia.org/sites/default/files/GoM%20Report%20on%20National%20Security.pdf, accessed on 24 May 2019.
9. Chandra, 'National Security System and Reform', n. 2, pp. 210–11. The chapter gives a detailed account of the operationalisation of the CCS decisions on the roles and functions of the new structures. As India's first Deputy NSA, Satish Chandra played a pivotal role in shaping these structures.
10. Arvind Gupta, *How India Manages its National Security*, New Delhi: Penguin Random House India, 2018, pp. 216–17.
11. A series of coordinated attacks at different locations in the city, claiming at least 174 lives and wounding over 300, as per multiple agency reports of the time. These have been documented in Shanthie Mariet D'Souza, 'Mumbai terrorist attacks of 2008', *Encyclopaedia Brittanica*, available at https://www.britannica.com/event/Mumbai-terrorist-attacks-of-2008, accessed on 20 July 2019.
12. Press release, PIB, n. 7.
13. 'Cabinet Committee on Security Reviews Progress in Operationalising India's Nuclear Doctrine', Press release, Prime Minister's Office, 4 January 2003, available at http://pibarchive.nic.in/newsite/archivepage.aspx, accessed on 30 May 2019.
14. Cabinet Secretariat Resolution No. 281/29/6/98/TS, dated 16 April 1999, n. 4.
15. Ibid.
16. NSCS Notification No. A-19011/01/2015-Ad. of 30 August 2016, *The Gazette of India,* 24 September 2016, pp. 867–68, available at https://www.greengazette.in/documents/government-gazette-39-2016-i2-w_20160930-120-00039.pdf, accessed on 30 May 2019.
17. See Pradhan, 'National Security System—Evolution', n. 1, pp. 444–45, for fuller details of the reorganisation.
18. For one such report, see Nitin Gokhale, 'Naresh Chandra Task Force's Report on National Security: An Appraisal', Vivekananda International Foundation, 16 July 2012, available at https://www.vifindia.org/article/2012/july/16/naresh-chandra-task-force-s-report-on-national-security-an-appraisal, accessed on 30 May 2019.

19. Gupta, *How India Manages its National Security*, n. 10, p. 362.
20. NSCS Notification No. C-182/207/CCS/2016-NSCS(NGO), dated 11 September 2018, *The Gazette of India*, 8 October 2018, available at http://egazette.nic.in/WriteReadData/2018/190593.pdf, accessed on 30 May 2019.
21. As per the Cabinet Secretariat Resolution No. 281/29/6/98/TS, dated 16 April 1999, n. 4.
22. 'Doval Chairs First Meet of Defence Panel', *The Hindu*, 4 May 2018, available at https://www.thehindu.com/todays-paper/tp-national/doval-chairs-first-meet-of-defence-panel/article23765476.ece, accessed on 30 May 2019.
23. Shishir Gupta, 'India to Create Super-committee for Defence Planning', *Hindustan Times*, 19 April 2018, available at https://www.hindustantimes.com/india-news/india-to-create-super-committee-for-defence-planning/story-PQSPeTpZ8Xm2QKjINXzxnK.html, accessed on 30 May 2019.
24. 'Government Finalises Broad Contours of Defence Space Agency', *The Economic Times*, 11 June 2019, available at https://economictimes.indiatimes.com/news/defence/government-finalises-broad-contours-of-defence-space-agency/articleshow/69745921.cms, accessed on 15 June 2019.
25. Gupta, *How India Manages its National Security*, n. 10, p. 360.
26. The judgement of the Supreme Court in *Justice Puttaswamy (Retd.) and Anr.* vs *Union of India and Ors.*, lays down principles for data collection, so that it is in accordance with an individual's right to privacy. Though the judgement was in the specific context of the Aadhar Act, these principles would be applicable to data collected for uses, such as for NATGRID. The text of the judgement is available at https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf, accessed on 30 May 2019.
27. See, for example, Arun Prakash, 'India's Higher Defence Organisation: Implications for National Security and Jointness', *Journal of Defence Studies*, Vol. 1, No. 1, August 2007, pp. 13–31.
28. *Reforming the National Security System: Recommendations of the Group of Ministers*, n. 8, p. 101.
29. See Prakash, 'India's Higher Defence Organisation', n. 27 and Arun Prakash, 'Defence Reforms: Contemporary Debates and Issues', in B.D. Jayal, V.P. Malik, Anit Mukherjee and Arun Prakash, *A Call for Change: Higher Defence Management in India,* IDSA Monograph Series No. 6, July 2012, pp. 18–36. Having served in the task force on defence in 2001 and the Naresh Chandra task force in 2011–12, besides having been Chairman, COSC, Admiral Arun Prakash (Retd.) has a unique insider's view of the

issues in higher defence management. Similar concerns have also been expressed by another former Chairman, COSC, General V.P. Malik (Retd.), 'Higher Management of Defence and Defence Reforms: Towards Better Management Techniques', in B.D. Jayal, V.P. Malik, Anit Mukherjee and Arun Prakash, *A Call for Change: Higher Defence Management in India,* IDSA Monograph Series No. 6, July 2012, pp. 37–51.