THE PANKAJ KUMAR JHA
CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

SEPTEMBER 2026

India's National Security Guard: Structural Reforms and the Path to Reform

Arsh Mandlaus

Edited by: Indraayan Das

About the Author

Arsh Mandlaus is an undergraduate student at the Jindal School of International Affairs and is a Research Intern at the Pankaj Kumar Jha Centre for Security Studies, JSIA.

About the Pankaj Kumar Jha Centre for Security Studies

The Pankaj Kumar Jha Centre for Security Studies (PKJCSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof. Dr. Pankaj K. Jha. Researchers at PKJCSS explore both regional and thematic topics in the broader field of international security studies to write issue briefs, policy briefs, defence white papers, and dialogue session reports on contemporary issues. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Pankaj Kumar Jha Centre for Security Studies attempts to unfold. Please refer to www.pkjcss.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


https://www.instagram.com/pkjcss_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

IB260901

Abstract

The paper evaluates the role of the National Security Guard (NSG) in India's counter terrorism policy. Specific focus will be paid to the evaluation of gaps existing systematically in the employment of NSG and offering policy options aimed at overcoming such gaps. The central question asked throughout this paper is: What is the level of effect created by deficiencies in either structure or operations in the role played by NSG, and what can be done to overcome them? It is suggested that although the NSG remains an elite force, there are some gaps remaining in the utilization of the NSG.

Introduction

Terrorism has been one of the major internal security threats faced by India throughout several decades due to both cross-border and internal factors. Among various agencies in charge of counter-terrorism activities in India is the NSG, the country's elite rapid-deployment counter-terrorism force[1]. Established under the National Security Guard Act of 1986 following the 1984 Operation Blue Star and the assassination of Prime Minister Indira Gandhi, the NSG was meant to serve as India's counter-terrorism response team in case of hostage rescue, aircraft hijackings, neutralisation of nuclear or chemical threats and other emergency situations[2].

Over its almost three-decade-long history, the force has seen participation in several significant events that exposed its capabilities and limitations. In particular, the 2008 Mumbai terrorist attacks – a coordinated and prolonged assault lasting for more than 60 hours – highlighted serious issues with respect to the NSG activation times and the structure of the overall counter-terrorism response mechanism in India. This event became the trigger for further discussion on the NSG's preparedness for handling current threats in India and its ability to effectively cope with these challenges[3].

This paper seeks to engage in a discussion of these issues through systematic analysis and provide concrete recommendations for improving NSG performance. As such, recommendations formulated in this paper will directly follow from the conclusions derived from the above analysis

[1] Gill, P. (2004). Securing the state: India's internal security apparatus. Journal of Strategic Studies, 27(3), 441–461.
[2] National Security Guard Act, 1986, No. 47, Acts of Parliament, 1986 (India).
[3] 3 Puri, L. (2010). Decoding 26/11: The why, who and how. Amaryllis.

The NSG in India's Counter-Terrorism Architecture

Institutional Origins and Mandate

The NSG was established based on the British SAS and German GSG-9 models as an elite federal force used to respond to extreme emergency situations at the request of a state or central authorities, when conventional policing forces cannot handle the threat adequately. According to the NSG Act of 1986, the force consists of two groups – the Special Action Group (SAG) made up of members of the Indian Army and the Special Ranger Group (SRG) recruited from the ranks of Central Armed Police Forces. The mission of SAG is focused on active counter-terrorism activities, while SRG personnel are charged with VIP protection and securing vital installations[4].

Though officially the force is subject to the control of the Ministry of Home Affairs, it can be deployed to any part of the country. Practically speaking, however, the NSG is neither the first nor immediate responder in a counter-terrorism scenario and can be used only in case of emergency when the local authorities and police forces have exhausted their possibilities[5].

Operational History and the 26/11 Watershed

In addition to being involved in the famous siege of the Golden Temple during the 1988 Operation Black Thunder, the NSG participated in several operations over the years. However, each of those operations indicated certain flaws in the force's readiness to respond quickly to emergency situations. The 2008 Mumbai attacks turned into another case in point[6].

It should be noted that the force did arrive at all three primary attack sites of the terrorists – the Taj Mahal Palace Hotel, Oberoi Trident, and Nariman House. However, the commandos arrived several hours after the attack started, because of which many civilians died. This happened because at the time the NSG was located at the base in Manesar, Haryana. The time required for travelling from the base to Palam Airport, taking off in a specially arranged charter flight and arriving in

[4] National Security Guard. (2023). Overview and mandate. Ministry of Home Affairs, Government of India.
[5] Sahni, A. (2002). South Asia Intelligence Review: India. South Asia Terrorism Portal.
[6] Srivastava, A. (2009). The Mumbai terror attacks and India's internal security. South Asian Survey, 16(1), 35–53.

Mumbai was estimated at nine hours. Thus, it became obvious that the centralised basing system hinders fast NSG mobilisation in response to terrorist threats[7].

Structural and Operational Gaps

Centralised Basing and the Deployment Gap

The most significant structural limitation of the NSG lies in its concentrated presence in a small territory. Even though the Indian government has allocated four regional bases for the force to ensure fast mobilisation of its members in case of emergency (in Mumbai, Chennai, Hyderabad, and Kolkata), there have been certain issues regarding staffing levels and equipping of these bases. In several instances, regional bases remained nothing more than nominal units that could not make decisions independently and lacked necessary sub-units and specialisation[8].

Consequently, the response area of NSG remained considerably smaller than anticipated. Therefore, vast territories of India including the northeastern regions, Kashmir and the Red Corridor areas lack NSG's coverage and fast response[9].

Federal Coordination Failures

India's federal system poses an obstacle to fast response to emergency counter-terrorism incidents. According to the Seventh Schedule of the Constitution, public order and policing are among state matters and therefore, the use of NSG forces can take place only in accordance with request by the corresponding state authorities or based on central directives[10].

Often, this causes delays in mobilisation of NSG forces due to the reluctance of state police forces to acknowledge the gravity of the threat. Moreover, the lack of activation protocols and joint command structures between the force and regional authorities creates additional delays. There is also an institutional problem in terms of state authorities seeing the NSG deployment as an admission of their inability to deal with the threat. Thus, even if a situation becomes critical and requires involvement of the NSG, state governments still tend to rely on the existing manpower

[7] Ramachandran, S. (2011). India's counter-terrorism architecture: Gaps and challenges. The RUSI Journal, 156(2), 58–65.
[8] Ministry of Home Affairs. (2020). Annual report 2019–2020. Government of India.
[9] Raghavan, V. R. (2001). Internal security and the Indian Army. Strategic Analysis, 25(5–6), 675–690.
[10] Tankel, S. (2011). Storming the world stage: The story of Lashkar-e-Taiba. Hurst.

and resources. This issue needs further work to build stronger collaboration between state and central authorities and establish more trustful relationships[11].

Intelligence-Operations Disconnect

Successful counter-terrorism operations are always based on proper intelligence data. At the same time, the NSG is not an intelligence agency, but a rapid response force designed to tackle terrorism at later stages of the process. Currently, there is no established mechanism for exchange of tactical information between the Intelligence Bureau, the Research and Analysis Wing, the National Investigation Agency and state intelligence departments with the operational units like the NSG. Furthermore, the NSG lacks a unit dealing with the constant monitoring of potential terrorist targets within its operational area of responsibility and the collection of relevant information[12].

Asymmetric and Emerging Threat Environments

Today, the environment in which NSG operates has become significantly more complicated. Apart from conventional hostage and hijacking activities, terrorists can attempt cyber-terrorism, attacks via unmanned aerial vehicles, solo terrorists inspired by internet propaganda, or even use radiological or chemical agents against densely populated urban territories. Doctrinal adaptation to such threats is far behind the curve and NSG training programmes and equipping cycles are out of sync with the pace of non-state actor innovation[13].

Personnel Rotation and Institutional Knowledge

NSG uses personnel from the Indian Army (SAG) and Central Armed Police Forces (SRG) through three-year deputations. Although this helps in securing a steady influx of professionals, it leaves a gap in institutional knowledge. Some of the roles performed by NSG members are hostage negotiations, urban warfare, CBRN response, and explosives handling, all of which require a great deal of specialization. If personnel change before having mastered all skills required for those tasks, the force will repeatedly find itself with underdeveloped specialists[14]

[11] Bhattacharyya, R. (2012). Federal crisis response: India's inter-agency coordination failures. Studies in Conflict & Terrorism, 35(10), 730–747.
[12] Intelligence Bureau. (2017). Coordination frameworks for counter-terrorism in federal polities. Government of India.
[13] Ahuja, N. (2020). Cyber terrorism and India's preparedness: Emerging threats and institutional responses. Journal of Defence Studies, 14(2), 45–66.
[14] Pant, H. V. (2009). Indian national security: Annual review 2008–09. KW Publishers.

Recommendations

The recommendations provided below have been crafted with specific gaps in mind. This means that not only are these recommendations more focused, but some of them present innovations to be introduced for the first time.

Genuine Operationalisation of Regional Hubs

To make regional hubs work effectively, each must comprise a full-fledged, ready-to-go combat team made of one combat-ready SAG squadron of around 50 members, helicopters, explosives removal teams, hostage negotiators, as well as separate logistic capacity. The Cabinet Secretariat must conduct yearly surprise readiness reviews to ensure that all hubs are always fully prepared to work without specialized support from the Manesar base. Finally, future hub locations should be chosen based on the results of an analysis of past attack patterns, infrastructure risks, and other factors, and not simply based on convenience[15].

Automatic Activation Protocols and Joint Command Frameworks

Automatic NSG activation procedure should be established either through special legislation or executive orders. Certain scenarios, such as coordinated multiple site attacks, a hostage situation involving over fifty people, or strikes against nuclear/chemical facilities, should automatically lead to NSG activation. After this point, appropriate formal approvals may be sought. At the same time, joint commands with state authorities should be worked out in a binding agreement with a clearly defined hierarchy, communication lines, and responsibilities. Finally, permanent NSG liaison offices could be established at the police headquarters of the most threatened states to ensure smoother cooperation[16].

Establishment of a Dedicated NSG Threat Intelligence Cell

A Threat Intelligence Cell (TIC) should be established as a permanent department in the NSG, composed of analysts permanently recruited from the Intelligence Bureau, RAW, and NIA. The primary mission of TIC would be to continuously monitor threats, identify vulnerabilities, assess terrorist activity, and develop actionable operational plans based on this information. Unlike

[15] United Kingdom Home Office. (2010). Contest: The United Kingdom's strategy for countering terrorism. Her Majesty's Stationery Office.
[16] Ministry of Home Affairs. (2009). Report of the high level enquiry committee on the Mumbai attacks. Government of India.

existing arrangements on intelligence sharing among federal agencies, this approach would enable the development of actionable intelligence, tailored to NSG's operational use. This is due to general national intelligence, even in the form of a brief, does not always translate into concrete and location-based intelligence required for deployment[17].

Doctrinal Reform for Emerging Threats

NSG doctrine revision should be carried out every five years through an extensive process supervised by the National Security Council Secretariat. This revision process should involve signals intelligence agencies providing input on cyber threats, as well as DRDO input regarding counter-drone tactics and chemical defence. In addition, input on advanced threats from countries with experience in countering them should also be obtained. One of the most important steps toward that goal is the establishment of the Advanced Threats Unit within NSG, which would focus on analysing new threats and developing operational strategies in response to them. This unit should be allowed to operate independently from deployment activities to provide the required freedom of action[18].

Structural Reform of the Personnel Rotation Model

Currently, the three-year rotation system requires modification, especially for specialists. Whereas the existing rotation model can be maintained for general operation personnel, specialists in areas of explosives handling, hostage negotiations, CBRN response, as well as specialists in dealing with cyber threats should have longer term of service – ideally seven years. Also, various forms of incentives could be used to reward such specialists, making them want to stay in the position for as long as possible. In addition, NSG should implement a formal Knowledge Management System that would accumulate lessons learned from both actual operations and trainings[19].

[17] National Security Council Secretariat. (2021). India's national counter-terrorism policy framework. Government of India.
[18] Counter Terrorism and Counter Radicalisation Division. (2022). National counter-terrorism strategy review. Ministry of Home Affairs, Government of India.
[19] Singh, M. (2009). Counter-terrorism in India: A review of structures and strategy. Institute for Defence Studies and Analyses.

Conclusion

The NSG still plays an important part in India's counter-terrorism efforts and enjoys considerable success due to its high levels of personnel professionalism. Nevertheless, the organization faces certain issues, such as slow deployment, inefficient coordination, lack of intelligence, and insufficient personnel continuity. In addition, there is a problem of constantly emerging threats and advances in technology and decentralized terrorist activity, requiring a shift from reactive to proactive responses. The reforms recommended above, especially regarding Threat Intelligence Cell and Advanced Threats Unit, are designed to facilitate such transition. At the same time, the proposed reformations would strengthen the organization, rather than change it dramatically[20].

[20] 20 Sahgal, A., & Anand, V. (2003). Terrorism and low intensity conflict in South Asian region. Institute for Defence Studies and Analyses.