

RUNNING THE EXERCISE: Conducting an Apex-level National Security Exercise



Gp Capt Akash Godbole
Senior Fellow, CAPSS

22 October, 2026

Keywords: National Security Exercise, Wargaming, Crisis Management, Strategic Policy Group, National Crisis Management Committee, Non-Government Elements, Resilience, India

Introduction

The first part of this argument, '[Before The Next Crisis](#),' argued for a biennial national security exercise. It set out why India needs such an exercise, what it would gain, and why it needs nothing more than a directive from the *Raksha Mantri* (RM) to begin. This paper proposes how to conduct it.

In brief, the proposal centres on one unannounced, plausible conflict scenario drawn from the National Security Council Secretariat (NSCS) threat assessment. It is played at three levels: service, ministerial and apex. Non-government elements, such as industry, academia, and field experts, participate from the outset. This being a security exercise, the Chiefs of Staff Committee (COSC) is proposed to lead the design and conduct. The NSCS convenes, and the National Institution for Transforming India (NITI) Aayog brings participants from beyond government. A Red cell acts as the adversary, with full freedom to win. A response cell stands in for the apex leadership and refers the decisions that matter to the principals. The exercise tests resilience as much as coordination. The follow-up is part of the exercise, with fixed timelines for making good the shortfalls.

Lessons from Abroad

Several nations have exercised their entire government and national resources, not just their armed forces. India need not copy any of their frameworks. However, a few lessons are worth emulating. The United States (US) [Nifty Nugget exercise of 1978](#) exposed deep mobilisation gaps, but its value lasted only as long as it was repeated. [Proud Prophet](#), in 1983, showed that a strategy fails when it ignores the adversary's perception, and let the principals decide through stand-ins. The North Atlantic Treaty Organization's (NATO) [crisis exercises](#) have let a member represent its apex council through a cell. Israel's [Turning Point](#) ended in a cabinet decision, but its public profile drew diplomatic reactions across the border. Sweden learnt that [people play honestly only when lessons target issues](#), not personalities. The United Kingdom's (UK) Cygnus found the gaps but failed to close them, and the UK has since worked towards a [fixed reporting schedule](#). China rehearses its critical sectors in peacetime, yet its navy found [its own Red cell mirroring Blue](#). The paper applies each lesson through an Indian structure that already exists.

Existing Mechanism

Much of what the exercise needs already exists. The services wargame their war plans through multiple contingencies as a matter of routine. Each service also runs its own academia and industry outreach: the [Army Design Bureau](#) (ADB), the [Naval Innovation and Indigenisation Organisation](#) (NIIO) and the [Directorate of Aerospace Design](#) (DAD). The NSCS runs [Bharat NCX](#), a national cyber exercise with a red-on-blue track and over 200 security chiefs from government and industry. The Strategic Policy Group (SPG), chaired by the National Security Advisor (NSA), is the government's '[principal mechanism for inter-ministerial coordination](#)', and its members include the service chiefs, the Cabinet Secretary, key secretaries and NITI Aayog. The National Crisis Management Committee (NCMC), under the Cabinet Secretary, [coordinates the national response to disasters](#).

These pieces already exist in some form or the other. However, they have never been played together. Table 1 shows how each can be used.

Table 1: Existing Structures and Their Roles

Existing structure	Present Mandate	Envisaged Role
Raksha Mantri	Constitutional responsibility for national defence	Initiates each iteration; receives the report
COSC	Joint planning; service wargames	Design lead and conduct; runs the service level
ADB, NIIO, DAD and the Department of Defence Production	Link the services with defence industry, DPSUs, start-ups and academia	Bring the defence ecosystem into the wargame fold
NSCS	Runs Bharat NCX; supports the NSA	Convenes the ministerial level; supports the White cell
Strategic Policy Group	Inter-ministerial coordination under the NSA	Its members, or their nominees, form the ministerial level
National Crisis Management Committee	National crisis response under the Cabinet Secretary	Plays when the trigger is civil; tests the hand-over to the security apparatus
NSA and Cabinet Secretary	Brief the Prime Minister and the Cabinet Committee on Security (CCS)	Nominate the response cell; brief the principals
Defence and national intelligence agencies	Assess adversary intent and capability	Provide the standing core of the Red cell
NITI Aayog	Works with industry, academia and the states	Brings in other non-government elements at the ministerial level
National Defence College	Trains senior officers and officials	Provides observers and carries the lessons into courses

Rules of Engagement

As in any wargame, rules of engagement must be laid out at the outset. These draw on the lessons above. Gaps are marked against institutions, not individuals. The Red cell must be adequately empowered to give the exercise realism. The White cell's rulings are not contested during play. The conditions for an honest output are set out next.

Precedence

A military headquarters cannot summon secretaries of other ministries to play. That is why the COSC leads the design, but the NSCS convenes the ministerial level. The SPG sits above both.

Political Risk and Signalling

In the public domain, perception matters. Any publicised failure for a ministry would have political repercussions for the minister in charge. At the same time, adversary perception must be catered for, with two nuclear-armed neighbours. The apex must decide without being seen to play, and the exercise should be quiet by design.

Secrecy and Time

Findings must be classified. Cygnus shows what classification does without a scheduled follow-up. Secrecy is acceptable. Silence is not. Senior officials would not be expected to spare long for such an exercise. Hence, the conduct must cater to their schedule.

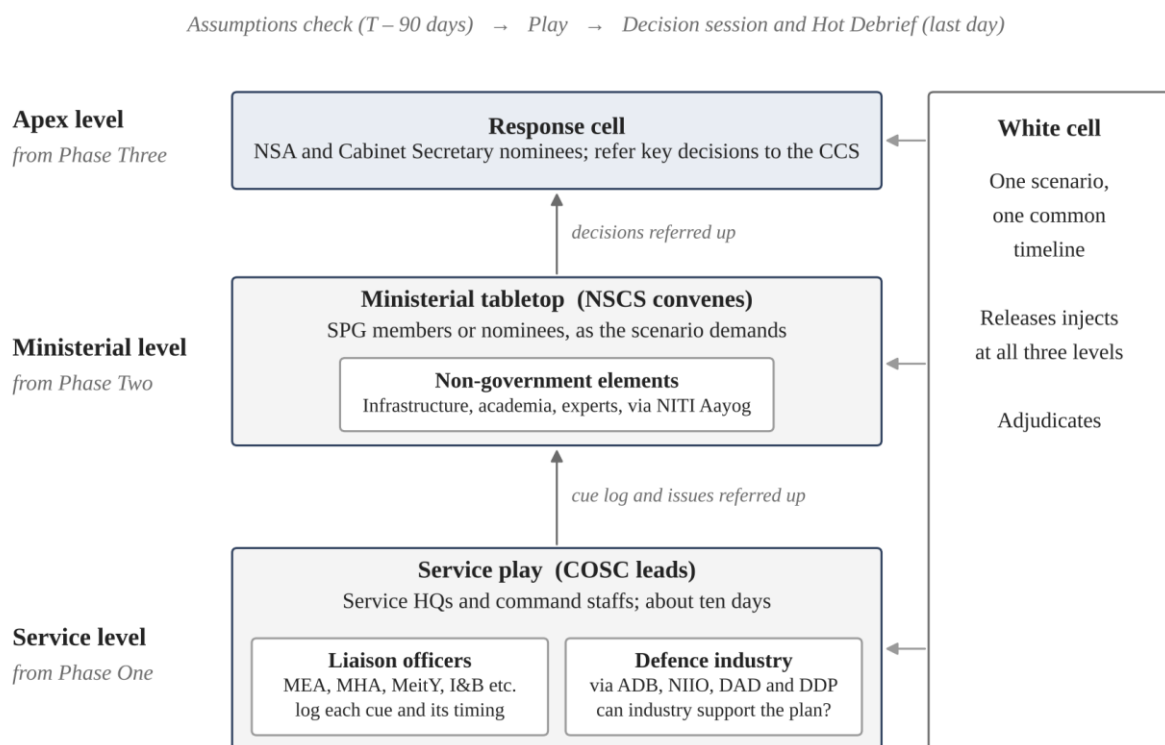
The Conduct

Lead and Cadence

The three levels remain as in Part 1: service, ministerial and CCS. The RM initiates the process, the COSC leads on design and conduct, and the NSCS convenes the ministerial level. The service design bodies and the Department of Defence Production bring in the defence industry, and NITI Aayog brings in other non-government elements. The plan should be one full iteration biennially, set by a standing CCS decision. No fresh legislation is required.

Three Levels, One Scenario

All three levels play the same scenario on one common timeline, and injects, the developments released to force a decision, cut across them. The service level plays for about ten days. The ministerial level joins in Phase Two, in concentrated sessions. Participation is decided by the scenario, *not by representation*. The apex level sits only at the end, for executive decision-making. Figure 1 shows the arrangement.

Figure 1: Three Levels, One Scenario

Diplomatic, cyber, or information actions take their cue from military action. Liaison officers from the Ministries of External Affairs (MEA), Home Affairs (MHA), Electronics and IT (MeitY) with the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC), Information and Broadcasting (I&B) and others the scenario demands sit with the service level. They log when their ministry would have been cued and annotate what it would have done and how long it would have taken. That log becomes the exercise brief for the ministerial level. The service level shows when the cue comes. The ministerial level shows whether anyone answers it.

Non-government elements join at both levels. At the service level, the ADB, NIIO, and DAD, along with the Department of Defence Production (DDP), bring in the defence industry, defence public sector undertakings (DPSUs), start-ups, and academic labs. At the ministerial level, NITI Aayog brings in critical infrastructure operators and field experts. China compels its firms to rehearse. India will have to do it by consent and contract. Firms play only the parts relevant to their sector, under non-disclosure terms. Each side sees only its own plans. That keeps the play honest. The classified report is 'Eyes Only' for the decision-makers.

Composition of the Cells

Each cell has one responsibility, and one nominating authority. Table 2 sets it out.

Table 2: Composition of the Cells

Cell	Drawn from	Nominated by	Role
White cell	Exercise director from the armed forces, joined by an NSCS co-director from Phase Two; military wargaming staff; NSCS staff; specialists in law, economics, cyber and transport for adjudication	NSA and Chief of Defence Staff (CDS)	Writes the scenario, runs the timeline, releases injects, adjudicates
Blue cell: service level	Operations and planning staff of the Service HQs; Department of Military Affairs; staff of the commands the scenario engages	COSC	Plays the military response
Liaison officers: service level	Joint secretary or director-level officers from MEA, MHA, MeitY (with CERT-In and NCIIPC), I&B and others the scenario demands	Their ministries, through the NSCS	Log each cue, the action it calls for and the time it would take
Defence industry: service level	Representatives of DPSUs, private defence firms, start-ups and academic labs, through	Service HQs and the DDP	Assess whether industry can support the service plan, and how fast

Cell	Drawn from	Nominated by	Role
	ADB, NIIO and DAD; officials of the DDP		
Blue cell: ministerial level	SPG members or their nominees, at secretary or additional secretary rank, from the ministries the scenario touches; the NCMC when the trigger is civil	NSA, through the Cabinet Secretary	Plays the government's response, in the roles they hold
Non-government elements: ministerial level	Senior executives of critical infrastructure operators (telecom, ports, power, logistics, data centres); domain academics; field experts and retired practitioners; all vetted and under non-disclosure terms	NITI Aayog, vetted by the NSCS	Assess what they can do towards the plan's assumptions, and how quickly
Response cell	Senior officials from the NSCS and the Cabinet Secretariat who know the principals' thinking	NSA and Cabinet Secretary	Stands in for the CCS; refers the decisions that matter to the principals
Red cell	A standing core from the defence and national intelligence agencies with adversary expertise; retired practitioners; vetted China and Pakistan specialists; cyber and information-warfare specialists	CDS and NSA	Plays the adversary as the adversary would; free to win
Observers	A few faculty from the National Defence College and leading defence think tanks	Exercise director	Watch and record; notes go to the Hot Debrief

The Red cell keeps its standing core between iterations. An adversary assembled afresh from people who most often sit with Blue would respond like Blue itself. The Chinese Navy observed the same, as its Red cell drifted into mirror-imaging.

The Scenario

Part 1 located the problem in compressed timelines. Recent conflicts have been protracted, but the first 72 hours still set the terms for what follows. The scenario must test every assumption that bears on that window. The White cell checks the assumptions that individual plans rest on, at least three months before the conduct. The trigger for a conflict may not be kinetic. The scenario should test a non-kinetic trigger as readily as a kinetic one. The Red cell must read India as Beijing or Rawalpindi would, not as New Delhi assumes it will.

How It Plays Out

Take a hypothetical scenario, for illustration. In Phase One, the service level plays a clash on the northern border. The same morning, malware shuts down traffic control on a major railway zone. This creates problems for Army mobilisation. The MeitY liaison officer logs the hour CERT-In would have been cued. The MEA officer logs the hour a demarche would have gone. A defence industry representative is asked how fast spares can be surged by road instead. Everything goes into the log.

In Phase Two, the ministerial level plays the same scenario. On Day one, the NCMC responds to the contingency, treating it as a technical fault. By evening, the Red cell adds a surge of disinformation linking the outage to the military. Who would coordinate with the NCMC once its technical fault turns out to be an act of war? Military movement stalls even on Day two. A data centre operator is asked whether the backup control system can run on its servers. The operator answers that it would take two days. The plan had assumed four hours. Day three, the attribution is still unclear. MEA wants to wait. The services want to signal. The question goes to the response cell, which refers it to the principals.

This brings the decision session to one concrete question. Who would be responsible for railway cyber defence once the crisis becomes a security threat? Three gaps are noted in the register: when the NCMC hands over to the security apparatus, whether the backup control assumption holds, and what legal cover a private data centre needs. Each gap is given an owner and a deadline.

Resilience

Coordination addresses decision-making authority, communication protocols, and timelines. Resilience examines the system's operational sustainability when part of it is targeted. The White cell must induce contingencies that take out a node, a port, a data centre, or a rail junction, and measure the capacity lost, the workaround found, and the time to recover. A bridge is not proven by walking across it on a fine day. It is proven by loading it until it creaks.

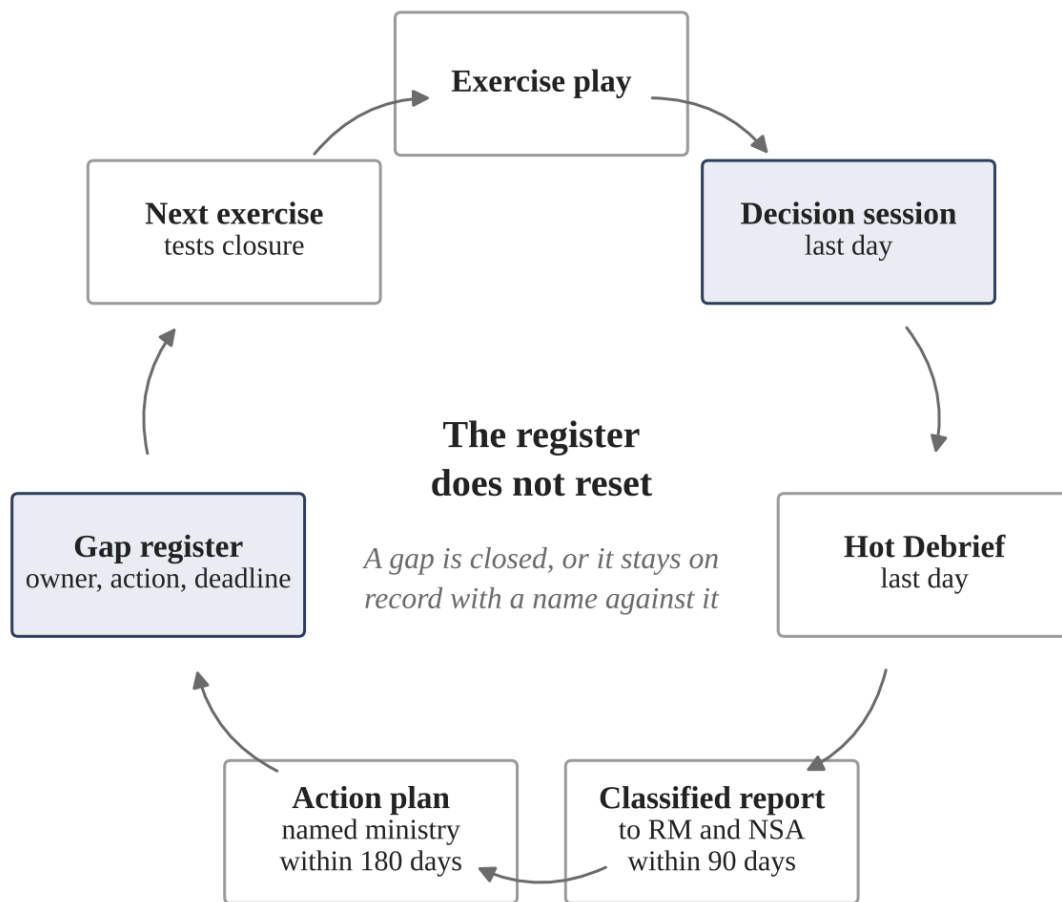
The Apex Level

The apex level follows the delegated model set out in Part 1. A response cell stands in for the CCS and refers the decisions that matter to the principals, out of sight. The NSA or the Cabinet Secretary distils the findings into a brief and response options. The Prime Minister takes part in person [only in major iterations](#). Ministers are not seen to play, and the exercise does not collapse if one is called away. Play closes with a decision session. At least one decision is taken in the room: a resource, a directive or an owner.

The Schedule and the Gap Register

The report may record that a decision waited nine hours between two ministries. It must not name the officer. A Hot Debrief, an informal review while memory is fresh, follows on the last day. Within 90 days, a classified report goes to the RM and the NSA, and within 180 days an action plan names the ministry responsible for each gap. The Cabinet Secretary, who already [coordinates the implementation of SPG decisions](#), monitors it. A sanitised lessons note goes to the training institutes and planning staff, so that the learning reaches the next set of players.

Every gap enters a register with an owner, an action and a deadline. Officials rotate. The register does not. Like an aircraft's logbook, every snag is entered, someone signs for it, and the next crew reads it before flight. The next exercise opens by checking the last one's gaps. Figure 2 shows the cycle.

Figure 2: The Schedule and the Gap Register

The Legal Question

One gap can be clearly stated at the outset. India's wartime requisition powers have come only with active conflict. The laws established in 1962 [lapsed in 1968](#). Similarly, those established in 1971 [expired in 1977](#). Partial provisions still exist, such as telecom under the [Telecommunications Act, 2023](#), and disaster response under the [Disaster Management Act, 2005](#). Every point where a player says "we would need legal cover for that" finds a place in the register. Over a few iterations, that becomes a clear brief for the Ministry of Law.

Conclusion

The real value of any exercise lies in the follow-up actions. No exercise of this nature should be judged by the scale of its conduct; it must lead to decisions that close the identified gaps. The exercise would gain its true value if it changes how those involved prepare.

This framework does not propose any statutory change or new institution. It merely envisages existing mechanisms to play once every two years against a specified timeline. If the second iteration finds fewer gaps than the first, then it suggests that progress has been made. If it doesn't show progress, the register would show the reason why. Either way, it is imperative to exercise and identify the gaps before the next crisis.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Aerospace Power and Strategic Studies [CAPSS])