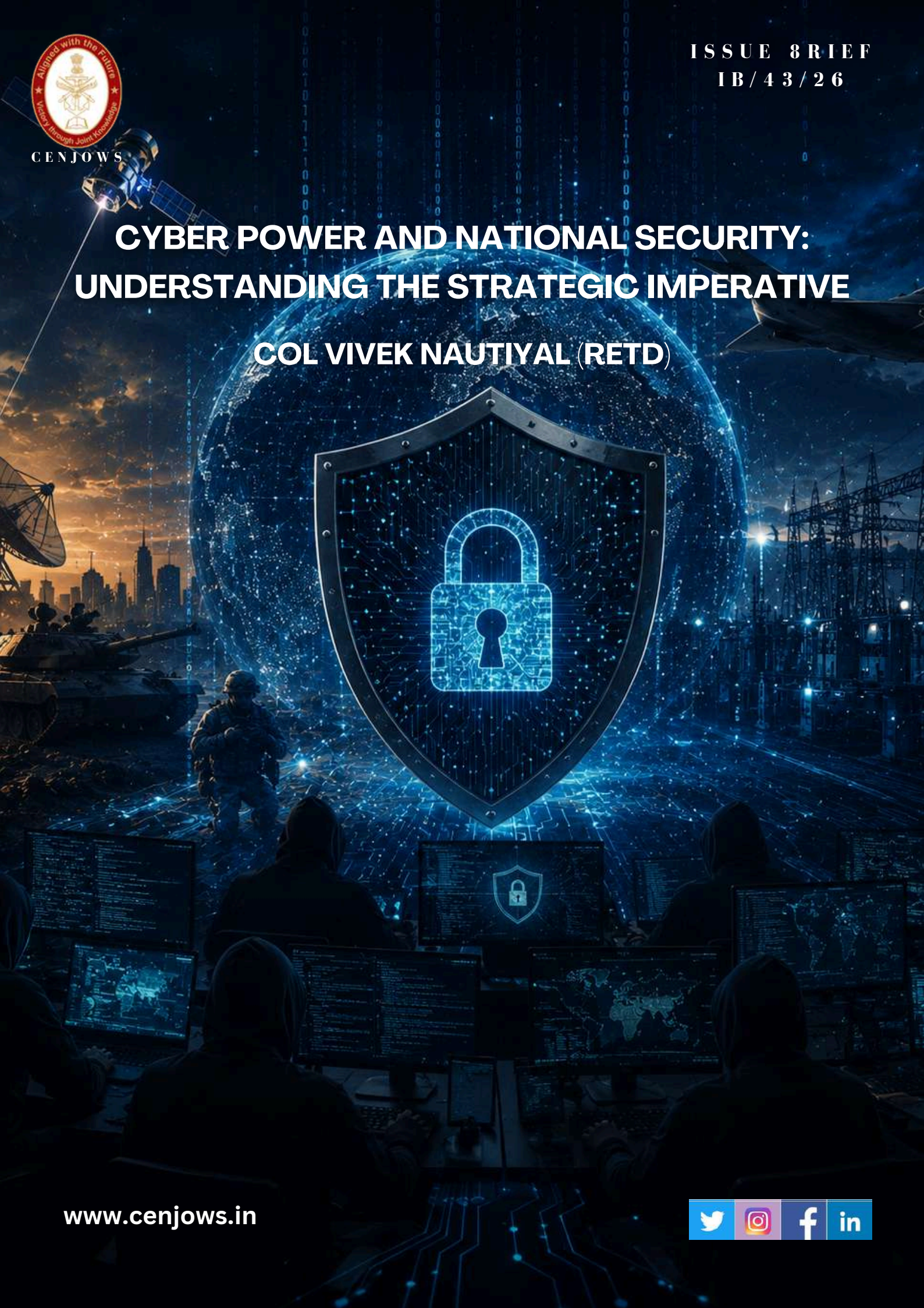
CENJOWS

ISSUE BRIEF
IB/43/26

CYBER POWER AND NATIONAL SECURITY: UNDERSTANDING THE STRATEGIC IMPERATIVE

COL VIVEK NAUTIYAL (RETD)



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Cyber Power and National Security: Understanding the Strategic Imperative

Col Vivek Nautiyal (Retd) is a senior fellow at CENJOWS

Abstract

Cyber power has emerged as a decisive instrument of statecraft in the twenty-first century, reshaping the contours of national security, deterrence and conventional military strategy. This paper examines the definition and key elements of cyber power, explores the contested terrain of cyber deterrence and coercion, situates cyber capability within the broader framework of comprehensive national power, and analyses its inextricable linkages with conventional and hybrid warfare. Drawing on global precedents and India's evolving cyber posture, the paper argues that a coherent and integrated approach to cyber power is indispensable for India to safeguard its strategic interests in an increasingly contested digital environment.

Introduction: The Age of Cyber Power

The domain of national power has historically been defined by the capacity to deploy military force, exercise economic leverage, and project diplomatic influence. In the opening decades of the twenty-first century, a fourth and transformative dimension has been added to this calculus: cyber power. No domain better illustrates the blurring of

traditional boundaries between war and peace, or between state and non-state actors, than cyberspace. It is a domain in which a handful of lines of code can disable a nuclear enrichment facility, disrupt democratic elections, cripple financial markets, or black out an adversary's power grid. All this without a single soldier crossing a border.

The global strategic environment has made this reality starkly evident. Russia's simultaneous kinetic and cyber assault on Ukraine, which began in February 2022, China's persistent grey-zone intrusions into the networks of rival states, and the proliferation of sophisticated ransomware campaigns targeting critical infrastructure have collectively demonstrated that cyber operations are central to contemporary statecraft and no longer a peripheral or futuristic concern.[i]

For India, a nation sandwiched between two nuclear-armed adversaries, both of which possess evolving offensive cyber capabilities, the necessity to understand, develop and wield cyber power as a component of national strength has never been more urgent. This paper lays the conceptual groundwork for that project by examining cyber power in its full strategic complexity.

Defining Cyber Power: Scope and Elements

What is Cyber Power?

Scholars and practitioners have defined cyber power in various ways, each reflecting different priority. A widely cited formulation draws on Joseph Nye's concept of power in international relations: cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across all the instruments of national power.[ii]

The International Institute for Strategic Studies (IISS), in its landmark report “Cyber Capabilities and National Power: A Net Assessment”, adopts a multi-dimensional framework that evaluates states across seven categories: strategy and doctrine; governance, command and control; core cyber-intelligence capability; cyber empowerment and dependence; cyber security and resilience; leadership in cyberspace affairs; and offensive cyber capability. This framework underscores that cyber power is simultaneously technical and political, defensive and offensive, as well as institutional and operational.[iii]

A more operational definition, articulated in India's own “Joint Doctrine Indian Armed Forces” (JDIAF - 2017), describes cyber power as "the ability to use cyberspace freely and securely to gain an advantage over the adversary while denying the same to him in various operational environments."[iv] This formulation is particularly apt for a defence-focused audience, as it captures both the enabling and the coercive dimensions of the concept.

The Elements of Cyber Power

Cyber power rests on the following interlocking pillars:

- Technical capability, i.e., the ability to develop, deploy, and sustain sophisticated tools for both offensive operations and defensive resilience, is the most visible dimension.
- Equally important are institutional structures, i.e., the agencies, command authorities, legal frameworks, and inter-agency coordination mechanisms that translate raw technical potential into coherent national capability.
- A third element is the intelligence underpinning: the ability to understand adversary networks, attribute attacks with credibility, and develop situational awareness across the digital environment. The IISS assessment makes it clear that a "core cyber-intelligence capability is the primary foundation of cyber power", and without it, neither defence nor offence can be effective.[v]
- Fourth, and often underappreciated, is the dimension of human capital: the cadre of trained professionals who can operate at the cutting edge of an ever-evolving technological frontier.
- Finally, to sustain long-term strategic relevance, cyber power requires a conducive ecosystem, a vibrant technology sector, thriving academia-industry linkages, and a culture of cybersecurity awareness.

This paper examines how these elements combine to serve national security objectives and derives concrete strategic imperatives for India.

Cyber Deterrence and Coercion: Theory and Practice

The Deterrence Problem in Cyberspace

Classical deterrence theory holds that a state can prevent adversarial action by credibly threatening unacceptable costs in retaliation. The concept, refined during the nuclear era, rests on three pillars: capability, credibility, and communication. Transposing this logic to cyberspace, however, is far from straightforward, and the academic and policy communities remain deeply divided on whether meaningful cyber deterrence is achievable.[vi]

The core problem is attribution. Unlike nuclear missiles, which leave unmistakable signatures, cyber operations are often cloaked in deliberate ambiguity. Adversaries exploit proxy networks, false flags and the inherent opacity of code to evade accountability. As scholars have noted, the conditions for successful coercion, which is effective communication, credible threat, and assured cost imposition, are all compromised in the cyber domain when classified capabilities must remain hidden to remain effective.[vii]

A second problem is the escalation dynamic. Unlike conventional deterrence, where escalation ladders are relatively well-defined, cyber operations inhabit a grey zone in which the line between espionage, coercion, sabotage, and acts of war is perpetually blurred. The pre-positioning of malicious code in adversary networks, what strategists call "persistent engagement", can simultaneously serve deterrence and provocation purposes, with unpredictable consequences.[viii]

Strategies for Cyber Deterrence

Despite these challenges, states have developed workable, if imperfect, approaches to cyber deterrence. The United States has pursued a strategy of deterrence by denial, i.e., hardening critical infrastructure and military networks to the point where the costs of a cyberattack outweigh the attacker's expected gains. Simultaneously, it employs deterrence by punishment through offensive cyber operations designed to impose costs on adversaries and through persistent engagement in forward-deployed cyber operations. The US Department of Defence's 2023 Cyber Strategy explicitly commits

to "integrated deterrence" as a core concept, weaving cyber capabilities into the broader architecture of military and diplomatic power.[ix]

China represents a contrasting model. Beijing has largely abandoned deterrence orthodoxy in favour of a doctrine of persistent grey-zone operations by using cyber intrusions for espionage, intellectual property theft, and infrastructure pre-positioning to achieve strategic effects short of the threshold of armed conflict. The 2024 exposure of the Volt Typhoon threat actor, a Chinese state-sponsored group that had embedded itself in US critical infrastructure networks, illustrated how cyber coercion can be practised through pre-positioned capability rather than active disruption.[x]

Israel and Russia demonstrate further variants: Israel employs offensive cyber operations as a substitute for kinetic action against adversary weapons programmes, while Russia integrates cyber operations seamlessly with information warfare and military action as part of a broader hybrid warfare doctrine.[xi] The common thread is that cyber deterrence is not a standalone posture but must be embedded within a comprehensive strategic framework.

Compellence and the Limits of Cyber Coercion

Beyond deterrence lies the more difficult question of compellence, which means, using cyber operations to compel an adversary to change its behaviour. The empirical record here is sobering. Despite the proliferation of cyber operations globally, sustained strategic compellence through cyber means alone has rarely succeeded. Cyberattacks tend to impose tactical costs rather than alter adversarial decision-making at the strategic level.[xii]

This does not diminish the value of offensive cyber capabilities; rather, it underlines that they are most effective when employed as part of a combined-arms approach, i.e., alongside diplomatic pressure, economic leverage, military signalling, and information operations. The lesson for India is clear: cyber power must be integrated, not siloed.

Cyber Power as a Component of Comprehensive National Power

The Concept of Comprehensive National Power

National power is conventionally assessed across its diplomatic, informational, military, and economic (DIME) dimensions. In the cyber age, each of these dimensions is both amplified and contested by digital technology. Cyber capabilities now serve as force multipliers across the entire DIME framework: they enable espionage and diplomatic leverage, disrupt adversarial economies, enhance military effectiveness, and shape information environments.

The concept of Comprehensive National Power (CNP), originally developed in Chinese strategic thought but now widely adopted in strategic studies, explicitly incorporates a state's technological and digital capabilities as determinants of national strength. The state that commands superior cyber capabilities hold structural advantages across virtually every domain of competition.[xiii]

The Economic Dimension

The economic dimension of cyber power is perhaps the most immediately tangible. Digital infrastructure underpins modern economies: financial systems, supply chains, energy grids, logistics networks, and manufacturing processes are all critically dependent on connected systems. A successful cyberattack on this infrastructure can cause economic damage far exceeding the cost of deployment, making cyber operations an asymmetric tool of coercion available even to relatively weaker states.

For India, with a digital economy valued at over US$190 billion and a government commitment to accelerating digitisation through programmes such as Digital India and the production-linked incentive schemes, the economic attack surface is vast and growing. The IISS assessment specifically highlights India's strength as an information and communications technology (ICT) powerhouse and its vibrant tech startup sector, while noting that this same digital dependency creates significant vulnerabilities.[xiv]

The Military Dimension

Militarily, cyber power has become a force multiplier of the first order. Modern military operations depend entirely on networked command and control, satellite navigation,

real-time intelligence fusion, and logistics management systems, all of which are vulnerable to cyber disruption. A state that can degrade an adversary's network-centric warfare capabilities has effectively blunted that adversary's conventional military advantage before a shot is fired.

Conversely, a state whose own military is highly digitised without commensurate cyber defences has created a critical vulnerability. India's ongoing military modernisation and theaterisation process, while strategically necessary, must therefore be accompanied by a rigorous programme of cyber hardening. As India's armed forces become more technologically sophisticated, their cyberattack surface expands proportionally.

The Diplomatic and Informational Dimensions

Diplomatically, cyber capabilities serve both offensive and defensive purposes.

- Offensive: signals intelligence gathered through cyber operations provides leverage in negotiations, foreknowledge of adversarial positions, and the ability to shape strategic environments.
- Defensive: the ability to protect diplomatic communications and governmental decision-making from cyber intrusion is a prerequisite for sovereign independence in the information age.

The informational dimension has grown substantially in salience. Disinformation campaigns, algorithmic manipulation of public discourse, and the weaponisation of social media platforms have become routine instruments of statecraft. As research has documented, nearly half of all global elections between 2023 and 2024 were subject to AI-driven disinformation campaigns, an illustration of how the information domain has become a contested battlespace extending far beyond military boundaries.[xv]

Linkages with Conventional and Hybrid Warfare

The Evolution of Hybrid Warfare

Hybrid warfare, which includes the deliberate blending of conventional military operations, irregular tactics, cyber operations, information warfare, and economic coercion to achieve strategic objectives, has become the dominant modality of great-

power competition in the contemporary era. The defining characteristic of hybrid warfare is strategic ambiguity. By operating across and between recognised domains of conflict, adversaries' complicate attribution, response, and escalation management.[xvi]

Russia's conduct in Ukraine offers the most extensively studied contemporary example. The near-simultaneous cyberattack on the ViaSat KA-SAT satellite network, which disrupted Ukrainian military command and civilian communications across 13 countries, was launched in coordination with the opening kinetic assault on February 24, 2022. This demonstrated with clinical precision how cyber operations can serve as a strategic enabler for conventional military action, degrading adversarial command structures before ground forces make contact.[xvii]

Cyber Operations as Force Multipliers

The integration of cyber operations into conventional military planning operates at multiple levels. At the strategic level, pre-positioned malware in adversarial infrastructure (e.g., power grids, water treatment systems, financial networks, etc) provides coercive leverage and the ability to impose immediate costs in the event of conflict. At the operational level, electronic and cyber warfare capabilities can degrade or deceive adversarial sensor networks, communication systems, and integrated air defence architectures. At the tactical level, compromised command and control systems can generate confusion, delay responses, and create battlefield advantages.

The concept of "persistent engagement" in US Cyber Command doctrine reflects this integration. By maintaining a continuous forward presence in adversarial networks, US cyber forces seek to shape the environment, deter attacks, and maintain the initiative, rather than waiting to respond to cyber incidents as they occur. The Chinese model achieves a similar effect through its doctrine of "system-of-systems warfare", which explicitly integrates cyber, electronic, space, and information operations to paralyse adversarial military networks in the opening hours of a conflict.[xviii]

The India-Specific Dimension

For India, the hybrid warfare threat is not hypothetical but active and ongoing. The 2020 Galwan Valley confrontation with China was accompanied by a sharp surge in

Chinese cyber operations against Indian networks, including a widely reported attempt to disrupt the Mumbai power grid in October 2020. Chinese-state-sponsored actors have continued to probe Indian critical infrastructure, military networks, and governmental systems in the years since. Pakistan, meanwhile, employs proxy hacker groups, often in coordination with state intelligence, to conduct cyber disruption during periods of bilateral tension.[xix]

The April 2025 attempted intrusions into four Indian defence-affiliated facilities by Pakistan-based actors, in the context of heightened border tensions, illustrate the direct linkage between conventional military posturing and cyber operations in the South Asian theatre. These incidents underscore that cyber and conventional threats cannot be managed in isolation. India's military planning must treat cyber as an integral domain of joint operations, not a specialist niche.

The release of India's Joint Doctrine for Cyberspace Operations by the Chief of Defence Staff in August 2025 marked a significant step in acknowledging this reality. By explicitly integrating offensive and defensive cyber capabilities and emphasising "threat-informed planning" and "real-time intelligence integration," the doctrine signals India's intent to develop credible cyber deterrence as a component of its overall military strategy.[xx]

India's Cyber Power: An Assessment

Against this backdrop, where does India stand in the global cyber power hierarchy? The IISS assessment places India in the third tier of cyber powers, alongside Indonesia, Iran, Japan, Malaysia, North Korea, and Vietnam. The report notes that while India has demonstrated regional cyber-intelligence reach and some offensive capability principally focused on Pakistan, it has made only modest progress in developing a coherent policy and doctrine for cyberspace security commensurate with the threat it faces from China.[xxi]

There are, however, grounds for cautious optimism in recent developments. In 2024, India secured Tier 1 status in the International Telecommunication Union's Global Cybersecurity Index, with the assessment recognising the country's legal, technical, capacity development, and cooperation measures as areas of relative strength.[xxii] The September 2024 amendment to the Allocation of Business Rules clarified India's

cybersecurity administration structure, designating the National Security Council Secretariat as the nodal coordination authority and establishing a National Cybersecurity Secretariat.[xxiii] The release of the National Cyber Security Reference Framework in late 2024, focused on seven critical sectors, provides a structured governance framework for the first time since the 2013 National Cyber Security Policy.[xxiv]

The Defence Cyber Agency (DcyA), a tri-service organisation integrating the Army, Navy, and Air Force cyber capabilities, has progressively matured since achieving full operational status in 2021. Its Exercise Cyber Suraksha series, most recently conducted in June 2025 with over 100 participants from national-level agencies, represents a systematic effort to build operational readiness and inter-agency coordination.[xxv]

However, significant gaps persist. India has yet to articulate a comprehensive National Cyber Security Strategy to replace the 2013 policy. The IISS assessment's observation that India's institutional reform has been "slow and incremental" retains some validity, even as recent years have seen acceleration. Most critically, as the Daily Pioneer has observed, India currently lacks a credible deterrence-by-punishment capability against China in the cyber domain, a gap that demands urgent strategic attention.[xxvi]

The Way Forward: Towards an Integrated Cyber Power Strategy

The foregoing analysis points towards several imperatives for India's cyber power strategy, each of which is examined below.

First, India must move towards a whole-of-nation approach to cyber power, one that integrates governmental, military, industry, and academic capabilities under a coherent strategic framework. The experience of leading cyber powers, the United States, Israel, and the United Kingdom, demonstrates that national cyber strength cannot be delivered by government alone. It requires deep public-private collaboration, a thriving innovation ecosystem, and sustained investment in human capital.

Second, India needs doctrinal clarity. The August 2025 Joint Doctrine for Cyberspace Operations is a welcome step, but a comprehensive National Cyber Security Strategy

that articulates India's deterrence posture, rules of engagement, escalation management framework, and red lines in cyberspace remains essential.

Third, the DCyA must be empowered and expanded towards an Indian Cyber Command: a dedicated, tri-service organisation with the stature, resources, and institutional authority to develop and employ cyber capabilities at the strategic level. China's April 2024 establishment of separate Cyberspace Force (CSF) and Aerospace Force (ASF), recognising that cyber warfare demands dedicated military professionals, offers an instructive precedent.[xxvii]

Fourth, India must resolve the civil-military disconnect in cyber governance. The current architecture, with Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), the DCyA, the National Cyber Coordination Centre (NCCC), and multiple ministerial entities each holding partial mandates, requires consolidation under a clearly designated apex authority with both strategic direction and operational coordination roles. The September 2024 Allocation of Business (AoB) amendment designating the National Cybersecurity Coordinator (NCSC) as the nodal point is a start, but implementation must follow at speed.

Finally, and most fundamentally, India must appreciate that cyber power is not a technical problem with a technical solution. It is a strategic problem that demands strategic leadership, institutional commitment, sustained investment, and cultural change across government, military, and industry. The stakes, India's security, prosperity, and strategic autonomy in the digital age, could not be higher.

Conclusion

Cyber power has emerged as a defining determinant of national security in the contemporary era, inseparable from economic strength, military effectiveness, diplomatic leverage, and informational influence. For India, a rising power in a volatile neighbourhood, building credible and integrated cyber power is not optional: it is a strategic imperative.

This paper has traced the conceptual foundations of cyber power, examined the challenges and evolving strategies of cyber deterrence and coercion, situated cyber

capabilities within the framework of comprehensive national power, and analysed the inextricable linkages between cyber operations and conventional and hybrid warfare. Together, these threads point to a single, urgent conclusion: India must move with deliberate speed to build an integrated, whole-of-nation cyber power architecture, one that unifies its governmental, military, industry, and academic strengths under a coherent strategic framework. The organisational design, doctrinal imperatives, human capital development, and strategic partnerships required to realise this vision are examined in the recommendations above and must now be translated into institutional action.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

[i] CyberPeace Institute. "Cyber Dimensions of Hybrid Warfare." April 2025. https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare/

[ii] PIR Center. "Why Has the Concept of Cyber Power Become So Prevalent in National Doctrines and Strategies Recently?" August 2024. https://pircenter.org/en/editions/14-2024-why-has-the-concept-of-cyber-power-become-so-prevalent-in-national-doctrines-and-strategies-recently-are-there-any-limitations-or-risks-of-using-this-concept/

[iii] International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." IISS Research Paper. 2021. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf

[iv] Headquarters Integrated Defence Staff. "Joint Doctrine Indian Armed Forces (JDIAF) 2017." Ministry of Defence, Government of India. 2017. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf

[v] International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." IISS Research Paper. 2021. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf

[vi] Stimson Center. "Beyond Denial: Toward a Credible Cyber Deterrence Strategy." December 2025. https://www.stimson.org/2025/beyond-denial-toward-a-credible-cyber-deterrence-strategy/

[vii] PIR Center. "Why Has the Concept of Cyber Power Become So Prevalent in National Doctrines and Strategies Recently?" August 2024. https://pircenter.org/en/editions/14-2024-why-has-the-concept-of-cyber-power-become-so-prevalent-in-national-doctrines-and-strategies-recently-are-there-any-limitations-or-risks-of-using-this-concept/

[viii] Journal of Strategic Studies. "Minding the Gap? The Strategic Logic of Cyber Coercion in Theory and Practice." Taylor & Francis. 2025. https://www.tandfonline.com/doi/full/10.1080/01402390.2025.2565191

[ix] US Department of Defence. "2023 DoD Cyber Strategy Summary." September 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[x] Geopolitical Monitor. "Unsecured Fronts: How Hybrid Warfare Influences Strategic Competition." June 2025. https://www.geopoliticalmonitor.com/technology-apathy-and-proximity-the-holy-trinity-of-hybrid-warfare/

[xi] National Security Archive / Digital Front Lines. "The Evolution of Cyber Operations in Armed Conflict." 2023. https://digitalfrontlines.io/2023/05/25/the-evolution-of-cyber-operations-in-armed-conflict/

[xii] Stimson Center. "Beyond Denial: Toward a Credible Cyber Deterrence Strategy." December 2025. https://www.stimson.org/2025/beyond-denial-toward-a-credible-cyber-deterrence-strategy/

[xiii] Defence Strategists. "Understanding Cyber Warfare in the Context of Hybrid Warfare Strategies." July 2024. https://defensestrategists.com/cyber-warfare-in-the-context-of-hybrid-warfare/

[xiv] International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." IISS Research Paper. 2021. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf

[xv] Capitol Technology University. "Nation-State Cyber Warfare: How Cybersecurity Professionals Defend the New Digital Battlefield." November 2025. https://www.captechu.edu/blog/how-cybersecurity-professionals-defend-the-new-digital-battlefield

[xvi] Washington Post. "Cyberattacks Are Just One Part of Hybrid Warfare." March 2023. https://www.washingtonpost.com/business/energy/2023/03/07/cyberattacks-are-just-one-part-of-hybrid-warfare-quicktake/a4db0c76-bd19-11ed-9350-7c5fccd598ad_story.html

[xvii] National Security Archive / Digital Front Lines. "The Evolution of Cyber Operations in Armed Conflict." 2023. https://digitalfrontlines.io/2023/05/25/the-evolution-of-cyber-operations-in-armed-conflict/

[xviii] Defence Strategists. "Understanding Cyber Warfare in the Context of Hybrid Warfare Strategies." July 2024. https://defensestrategists.com/cyber-warfare-in-the-context-of-hybrid-warfare/

[xix] National Strategy. "Cyber Deterrence in the Indian Context: Constraints, Credibility and Escalation Risks." February 2026. https://www.natstrat.org/articledetail/publications/cyber-deterrence-in-the-indian-context-constraints-credibility-and-escalation-risks-251.html

[xx] ibid

[xxi] International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." IISS Research Paper. 2021. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf

[xxii] ibid

[xxiii] Carnegie Endowment for International Peace. "Mapping India's Cybersecurity Administration in 2025." September 2025. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

[xxiv] Carnegie Endowment for International Peace. "Interpreting India's Cyber Statecraft." March 2025. https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft?lang=en

[xxv] Press Information Bureau. "Defence Cyber Agency Begins Exercise to Bolster Cyber Resilience at National Level." June 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2136618

[xxvi] Daily Pioneer. "Why Cyber Power Matters for India's Future Deterrence." 2025. https://dailypioneer.com/news/why-cyber-power-matters-for-india-s-future-deterrence

[xxvii] ibid