# CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

**New Delhi**

**CAPSS In Focus: 19/2025**

**25 August 2025**

# Cyber Frontier: India's Strategic Leap in Cyberspace

**Mrs Gowri R**
Research Associate, Centre for Aerospace Power and Strategic Studies

Source: PIB Delhi

**Keywords**: Joint Cyberspace Doctrine, Cybersecurity, Cyber warfare, Armed Forces

The digital age has significantly transformed conflict, security, and international order. As societies, economies, and militaries become ever more reliant on interconnected digital systems, cyberspace has emerged as a new domain of strategic competition that challenges traditional security paradigms.

The Tallinn Manual on the International Law Applicable to Cyber Warfare asserts that existing international law applies to cyber operations in the same way it applies to physical warfare. It is a non-binding study that outlines how international law relates to cyber conflicts and cyber warfare. This manual provide guidelines for determining when cyber activities constitute the use of force, armed attack, or violations of sovereignty.[1] In addition, the Budapest Convention is a binding international treaty aimed at combating cybercrime. India is not a signatory to this convention due to concerns over sovereignty, its exclusion from the drafting process, and certain legal and diplomatic reservations.[2] India is signatory to the Bletchley Declaration, which aims to promote international cooperation for the safe and responsible development of Artificial Intelligence (AI) and to foster collective action against risks in critical areas like cyberspace and cybersecurity. [3] Additionally, India actively participates in the United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) processes, focussing on responsible state behaviour and cybersecurity within the context of international security. On August 07, 2025, General Anil Chauhan, Chief of Defence Staff (CDS) and Secretary, Department of Military Affairs released India's first declassified joint doctrine for cyberspace operations.[4] [5] This article highlights the necessity of a joint doctrine for the Armed Forces regarding cyberspace operations, as well as its importance and significant impact.

**Why Joint Cyberspace Operations Doctrine**

Doctrine is essential as it provides the Armed Forces with a shared framework of principles that guide action, reduce operational friction, and maintain unity of effort across diverse missions. It institutionalises experience, turning lessons learnt into authoritative guidance that supports education, command, and organisational change. Beyond the battlefield, modern doctrine also serves as a tool for cultural integration and political communication, ensuring that military actions are coherent, adaptable, and aligned with strategic objectives.[6] Cyber warfare operates in a domain that is borderless, instantaneous, and accessible to a wide array of actors from major powers and rogue states to non-state groups and even individuals.[7] Unlike previous technological revolutions, the rise of cyberspace represents not just an extension of existing forms of conflict, but a fundamental shift in the logic and practice of international relations. When states employ cyber fait accompli to achieve unilateral gains, it becomes crucial to safeguard both military and

civil digital infrastructure. The Cyberspace Doctrine is vital for operating jointly and effectively, adapting to ever-evolving challenges, and employing cyber power with legitimacy and resilience. In addition to providing credible deterrence to adversaries, the doctrine strategically communicates our intent and clarity of operations to the world as we use cyberspace to achieve military objectives and protect our interests in this critical domain.

**Essence and Scope of the Joint Cyberspace Doctrine**

The Joint Cyberspace Doctrine establishes a unified strategic and operational framework for the Indian Armed Forces, ensuring that the Army, Navy, and Air Force coordinate their cyber capabilities under a common set of principles. The doctrine explains the importance of Cyberspace by highlighting it as a global, shared domain without territorial boundaries, setting it alongside land, sea, air, and space as a medium of full-fledged warfare. Cyberspace operations require rapid, flexible actions such as identifying vulnerabilities, deploying responses, or countering threats with quick decision-making. Unlike conventional battles, cyberspace operations achieve decisive effects such as denial, disruption, degradation, deception, and psychological impact on adversaries without physical violence by crippling networks, sowing confusion, or remotely sabotaging plans. It focuses on gaining and maintaining the initiative. Cyberspace is a domain of perpetual contest, where attackers and defenders constantly seek advantageous positions such as access to networks, data, or information without clear front lines. The doctrine highlights the nexus of civil-military implications, that a cyber-attack on civilian critical infrastructure can have cascading national, strategic, and military repercussions. As cyber networks are intertwined, there is often no clear distinction between civilian and military targets. It underscores the importance of automation, specialised skills, continuous vigilance, and a "living document" approach to demonstrate adaptability in a fast-changing threat environment.

From a technical perspective, the doctrine drives innovation through Artificial Intelligence (AI), Machine Learning (ML), advanced cryptography, and cyber ranges, directly influencing capability development and cultivating a skilled cyber workforce. On a policy level, it aligns military planning with the national cybersecurity framework and international cyber norms, even while acknowledging the absence of global consensus, and it promotes inter-agency coordination through bodies like the National Security Council Secretariat (NSCS), National Technical Research Organisation (NTRO), Indian Computer Emergency Response Team (CERT-In), and the Cyber Diplomacy Division. Critically, it prepares the Armed Forces to address attribution challenges, proportionality concerns, and persistent threats such as Advanced Persistent Threats (APT), ransomware, and disinformation. Overall, the doctrine's implementation can enhance

India's cyber resilience, deterrence credibility, and ability to respond swiftly to evolving digital threats, while also shaping India's role in global cyber governance.

**Impact of Cyberspace Doctrine**

India's Joint Doctrine for Cyberspace Operations is the nation's first-ever formal doctrine dedicated to the cyberspace domain, marking a historic step in integrating cyber power into its national defence strategy. This document is both fundamental and foundational document, crafted in a manner that makes its concepts accessible and understandable to a wide range of audiences, not beyond just specialists in cyber and military fields. It outlines the responsibilities of fighting forces, detailing their roles in safeguarding national cyberspace, by conducting and integrating cyber capabilities across all domains of warfare. The document also highlights the future requirements in the development of real-time intelligence, resilient infrastructure, advanced indigenous technologies, a skilled cyber workforce, and strong civil-military collaboration. These elements are crucial for ensuring India's long-term digital sovereignty and security.

The doctrine comprehensively addresses the overlaps among cyberspace, electromagnetic, and information warfare and blending into the other domains of warfare. It amply covers all aspects from physical security to virtual hardening, focused on military cyber operations. It defines the responsibilities of various stakeholders towards the protection of civil and military critical infrastructure, emphasising coordinated efforts, considering the civil-military cross implications. With further detailing of the specific mandates and boundaries in future iterations, this framework could provide even greater clarity and help ensure seamless coordination during crisis scenarios. It amply covers potential capability development, including emerging technologies and policy imperatives. However, explicit guidance on capacity building can help provide the ecosystem with the necessary course corrections for future investments. The HR and skill development aspects have been generalised to meet the training requirements of military personnel. Meanwhile, the basic cyber training at the school or graduation level remains the responsibility of academia. However, expanding the doctrine to incorporate academia, R&D institutions in cyber training, with specific military emphasis, could help bridge the gap between civilian education and defence-specific skill demands. The doctrine is silent on the mechanisms for monitoring insider activities in the cyberspace domain, and a clearer articulation of deterrent measures against such perpetrators is essential to strengthen resilience and avert inimical threats.

In the modern era of conflicts among countries like Israel–Iran, Russia–Ukraine, India–Pakistan, and Israel–Hamas, cyber warfare has been conducted in parallel with kinetic operations, amplifying psychological impact and influencing perceptions, morale, and national decision-making on a strategic scale. Cyber warfare is persistently conducted by states and non-state actors alike,

both during the No War No Peace (NWNP) regime and in times of open conflict,[8] resulting in ongoing contest and exploitation across the cyberspace domain. India's joint doctrine for cyberspace operations stands as a fundamental guide to safeguard national interests, deter adversaries, and shape global cyber governance.

## NOTES:

[1] Michael N Schmitt, The Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013).

[2] Pragati Dwivedi, "Convention On Cybercrime In Budapest: Assessment Of India's Concerns," Institute of Legal Education, April 27, 2023, https://iledu.in/convention-on-cybercrime-in-budapest-assessment-of-indias-concerns/. Accessed on August 11, 2025.

[3] Government of the United Kingdom, " The Bletchley Declaration by Countries Attending the AI Safety Summit," GOV.UK, February 13, 2025, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. Accessed on August 11, 2025.

[4] Press Information Bureau, Government of India, "CDS Gen Anil Chauhan releases Joint Doctrine for Cyberspace Operations," Press Release: June 18, 2024, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2026240. Accessed on August 12, 2025.

[5] Integrated Defence Staff, "Doctrines," https://ids.nic.in/content/doctrines. Accessed August 12, 2025.

[6] Harald Høiback, "What Is Doctrine?," Journal of Strategic Studies 34, no. 6, 2011 (December), doi:10.1080/01402390.2011.561104. Accessed on August 11, 2025, pp. 879–900.

[7] Lucas Kello, The Virtual Weapon and International Order (New Haven: Yale University Press, 2017).

[8] Indian Air Force, "Doctrine of The Indian Air Force," https://indianairforce.nic.in/Resources/pdf/header/latest-Doctrine-22-Feb.pdf. Accessed on July 04, 2025.