International Journal of Advanced Scientific Research
www.allscientificjournal.com
ISSN: 2456-0421
Received: 06-12-2025, Accepted: 05-01-2026, Published: 22-01-2026
Volume 11, Issue 1, 2026, Page No. 37-39

Dos attacks as a cyber threat to Indian air power

Aanchal Madheshia
Research Scholar, Department of Defence and strategi c studies, University of Allahabad (SPM), Prayagraj, Uttar Pradesh, India

Abstract
The accelerating pace of digital transformation within modern air forces has created both opportunities and vulnerabilities. India's pursuit of network-centric warfare, supported by advanced command-and-control systems, real-time data links, and indigenous digital networks, has strengthened its air power capabilities. However, this reliance on interconnected technologies has simultaneously expanded the cyber-attack surface, exposing critical systems to threats such as Denial of Service (DoS) attacks. While often dismissed as a low-level cyber nuisance, DoS attacks have evolved into sophisticated, state-sponsored instruments of asymmetric warfare capable of degrading air defence networks, delaying operational decision-making, and paralyzing mission-critical communication. This paper examines the emerging threat of DoS attacks to Indian air power from a cybersecurity perspective. It analyses the evolving global cyber threat landscape in military aviation, explains the mechanics and operational relevance of DoS attacks, and contextualizes the risks within India's ongoing modernization drive and its emphasis on indigenisation under Atmanirbhar Bharat. The study argues that DoS attacks must be viewed not only as technical disruptions but as strategic tools that could undermine deterrence, readiness, and combat effectiveness. By situating the problem within both global trends and the specific vulnerabilities of the Indian Air Force, the paper underscores the urgent need for robust cyber resilience, doctrinal adaptation, and inter-agency coordination.

Keywords: Cybersecurity, indian air force, air power, denial of service (dos), network-centric warfare, military aviation, atmanirbhar bharat

Introduction

Air power in the twenty-first century is no longer defined merely by the number of aircraft, advanced platforms, or aerial firepower. Rather, it is increasingly characterised by the seamless integration of digital networks, real-time intelligence, and resilient communication systems. The Indian Air Force (IAF), which has embarked upon a transformative journey since 2014 to modernise its capabilities, now envisions itself as a network-centric force capable of operating in multi-domain environments. Initiatives such as the Integrated Air Command and Control System (IACCS), indigenous data link projects, and the expansion of satellite-based communication systems represent significant progress. However, these same digital dependencies have also created a paradoxical vulnerability: the growing susceptibility of Indian air power to cyber threats.

Among the spectrum of cyber threats, Denial of Service (DoS) attacks stand out as an underestimated but potentially disruptive challenge. Traditionally seen as simple attempts to overwhelm servers or networks with excessive traffic, DoS and its advanced variant, Distributed Denial of Service (DDoS), have evolved into sophisticated tools for adversaries. In military contexts, these attacks can disrupt air traffic management, paralyse command networks, and even compromise mission planning at crucial junctures. Given India's geographical and strategic challenges—ranging from hostile neighbours with proven cyber capabilities to the globalisation of cyber-attack tools—the threat environment cannot be underestimated.

This paper argues that DoS attacks against Indian air power should not be seen merely as "technical glitches" or "low-grade cyber events." Instead, they must be analysed through a strategic lens, recognising their potential to undermine national security. The paper is structured as follows: first, it outlines the broader cyber threat landscape in military aviation; second, it explains the mechanics and relevance of DoS attacks to air power; third, it contextualises vulnerabilities within the IAF's modernisation drive; fourth, it draws lessons from global militaries; and finally, it offers strategic and policy recommendations to strengthen India's cyber resilience.

Cyber Threat Landscape in Military Aviation

Modern air forces worldwide have transitioned into highly networked organisations that rely on integrated systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). While this has improved operational efficiency, it has also expanded the cyber-attack surface. The nature of cyber threats facing military aviation can be divided into four categories: espionage, sabotage, information warfare, and operational disruption.

1. **Espionage:** Adversaries may exploit vulnerabilities in data links, radar systems, or maintenance networks to steal sensitive information. For instance, the theft of F-35 design data from US contractors demonstrated how cyber intrusions could compromise air dominance.

2. **Sabotage:** Malicious code or cyber exploits can corrupt mission-critical software, disable avionics, or tamper with flight control systems. In 2019, reports suggested that malware had infiltrated NATO's drone networks, exposing vulnerabilities in unmanned aerial systems.

3. **Information Warfare:** Manipulation of data streams or psychological operations through digital means can

degrade trust in command systems or confuse decision-makers during crises.

4. **Operational Disruption:** Perhaps the most relevant for this paper, operational disruption involves paralyzing networks, delaying command orders, or disabling communication channels during high-intensity operations. DoS attacks fall squarely in this category.

The Indian Air Force is not immune to these challenges. With its growing reliance on satellite communication, indigenous radar integration, and automation in air defence networks, the IAF's digital backbone has become both an asset and a potential liability. Global examples show that even technologically advanced militaries struggle with cyber resilience, suggesting that India must treat this domain with equal seriousness.

Understanding DoS Attacks in Air Power

Denial of Service (DoS) attacks are cyber operations that overwhelm a target system by flooding it with excessive traffic, rendering it unable to respond to legitimate requests. In military contexts, these attacks may be targeted at

- **Air Defence Networks:** Overloading radar or sensor systems with spurious signals could delay threat detection or create false alarms.
- **Command and Control (C2) Systems:** DoS attacks on servers managing IACCS-like platforms could slow down or paralyse the transmission of orders, disrupting time-sensitive missions.
- **Logistics and Maintenance Networks:** By targeting databases for aircraft maintenance or supply chain management, adversaries could delay sortie generation.
- **Air Traffic Control Systems:** In the broader aerospace domain, DoS attacks against civil-military ATC networks could cause chaos in the skies, complicating military operations.

What makes DoS particularly dangerous for air power is its asymmetric nature. Launching such attacks requires limited resources, but the disruption caused can be disproportionate. Moreover, with Distributed Denial of Service (DDoS), attackers leverage botnets spanning multiple countries, making attribution extremely difficult—a challenge particularly acute in geopolitically tense regions like South Asia.

The strategic implication is clear: DoS attacks can serve as a "first-strike" tool in the cyber domain, deployed to paralyse networks just before or during a conventional conflict. For an air force like India's, which depends on rapid mobilisation, precision targeting, and uninterrupted communication, even a short-duration disruption could tilt the operational balance.

Vulnerabilities in the Indian Air Force's Cyber Infrastructure

The Indian Air Force (IAF), as one of the world's largest and technologically sophisticated air forces, has steadily transitioned from a platform-centric to a network-centric force. This modernization has resulted in a proliferation of information technology (IT) systems, mission-critical networks, and digitalized command-and-control (C2) infrastructures. However, such dependence has inevitably created vulnerabilities that adversaries can exploit through cyber means, particularly denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

A central vulnerability lies in the IAF's growing reliance on satellite-based communication and ground-based control stations for network-centric operations. Sophisticated adversaries could overwhelm data links, radar feeds, or logistics networks with malicious traffic, disrupting operational readiness at crucial junctures. For example, a DDoS attack targeting the Integrated Air Command and Control System (IACCS) could degrade the IAF's ability to process real-time air surveillance and mission planning.

Moreover, the increasing adoption of indigenous software-driven platforms under the Atmanirbhar Bharat initiative introduces both strengths and weaknesses. While indigenization reduces dependence on foreign vendors, it also presents challenges related to software testing, patching, and lifecycle management. Weaknesses in these systems may inadvertently expand the attack surface.

Insider threats and supply-chain compromises further amplify risks. Hardware procured from global suppliers could be pre-loaded with malicious code or backdoors, while unauthorized access by insiders could enable coordinated DoS attacks during sensitive missions. Thus, the IAF must recognize that cyber vulnerabilities are no longer confined to IT systems alone but extend to operational technologies (OT), weapon platforms, and mission-critical communications.

Case Studies and Lessons from Global Militaries

Globally, several militaries have experienced the disruptive potential of DoS attacks. The 2007 cyberattacks on Estonia, though targeting government and civilian institutions, demonstrated how state-backed actors could employ massive DDoS campaigns to paralyze digital infrastructures. In 2015, Ukraine's power grid attack revealed how cyber operations can disable critical national infrastructure, with potential parallels in the aviation sector.

The United States Air Force has consistently highlighted DoS threats in its cyber strategy. In 2019, simulated red-team exercises demonstrated that even advanced systems like the F-35 Joint Strike Fighter could be indirectly compromised by overwhelming mission-planning software servers with artificial traffic. The key lesson here is that DoS attacks do not necessarily have to directly penetrate classified systems they can paralyze the peripheral, yet indispensable, support architecture.

China's People's Liberation Army (PLA) has emphasized "Integrated Network and Electronic Warfare" (INEW), where DoS attacks form a crucial element of soft-kill strategies. By overwhelming adversarial networks, the PLA aims to deny situational awareness and delay combat responses. These doctrinal insights indicate that DoS attacks are not merely a nuisance but have been doctrinally weaponized by major powers.

For India, these cases underscore the need to anticipate, simulate, and prepare for cyber denial scenarios. Just as missile defence systems account for saturation strikes, cyber defences must consider the volumetric intensity of DoS assaults on air power infrastructure.

Strategic Implications for India

DoS attacks on the IAF carry implications beyond temporary disruption. In a conflict scenario, the timing of such attacks could neutralize India's escalation dominance by degrading its ability to launch or sustain offensive and defensive missions. For instance, crippling the IACCS or air defence networks even for a few hours during a crisis with China or Pakistan could tilt the operational balance.

At the strategic level, DoS threats erode deterrence credibility. If adversaries perceive India's cyber defences as porous, they may be emboldened to launch pre-emptive digital strikes to neutralize air superiority. Additionally, DoS attacks blur the threshold of conflict they may be conducted below the conventional war threshold yet achieve significant military and political gains.

The doctrinal implication is that cyber resilience must become as critical as kinetic capabilities in the IAF's modernization roadmap. Current reliance on reactive patching or vendor-driven solutions is insufficient. Instead, resilience requires an integrated approach combining redundancy, artificial intelligence (AI)-enabled detection, cyber deception, and offensive cyber capabilities to deter adversaries.

Policy Recommendations

1. **Institutionalize Cyber Wargaming:** The IAF should conduct regular red-team simulations specifically targeting DoS scenarios on mission-critical networks. These exercises must include joint participation from the Defence Cyber Agency (DCA) and private industry experts.

2. **Strengthen Redundancy and Diversification:** Critical systems like IACCS must not rely on single communication channels. Multiple redundant pathways, including satellite-independent terrestrial lines, should be established to mitigate DoS disruptions.

3. **AI-Powered Detection Systems:** Machine learning algorithms capable of identifying unusual traffic patterns can enable real-time mitigation of volumetric DoS attacks.

4. **Secure Supply Chains:** Indigenous development of hardware and software must incorporate stringent vetting, code audits, and independent validation to reduce risks of hidden vulnerabilities.

5. **Offensive Cyber Doctrine:** India must adopt a clear doctrine for offensive cyber capabilities, including retaliatory DoS and counter-DDoS operations. This deterrent posture can dissuade adversaries from exploiting vulnerabilities.

6. **International Partnerships:** Collaboration with trusted partners such as the US, France, and Israel on cyber defence technologies can accelerate the IAF's resilience. Joint exercises like Cyber Defence Exchanges must include air power-specific scenarios.

Conclusion

Denial-of-service attacks represent one of the most underappreciated yet potent threats to modern air power. For the Indian Air Force, the danger lies not only in the sophistication of adversarial tools but also in the expanding digital footprint of its own modernization. As the IAF embraces network-centric warfare and indigenization, the risks of cyber denial will continue to grow.

To safeguard deterrence credibility and operational readiness, the IAF must integrate DoS resilience into its modernization doctrine. Cyber defence cannot remain a peripheral IT function; it must be treated as a combat capability on par with fighter squadrons and missile defence systems. By adopting proactive measures, strengthening institutional frameworks, and leveraging global best practices, India can ensure that its air power remains resilient in the face of twenty-first-century cyber threats.

References

1. Giles K. Handbook of Russian Information Warfare. NATO Defense College, 2017.
2. Lindsay JR. Stuxnet and the Limits of Cyber Warfare. Security Studies,2013:22(3):365-404.
3. Libicki MC. Cyberdeterrence and Cyberwar. RAND Corporation, 2009.
4. Nye JS. Deterrence and Dissuasion in Cyberspace. International Security,2017:41(3):44-71.
5. Rid T. Cyber War Will Not Take Place. Oxford University Press, 2013.
6. Singer PW, Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.
7. Stokes M. China's Evolving Conventional Strategic Strike Capabilities. Project 2049 Institute, 2011.
8. US Department of Defense. Military and Security Developments Involving the People's Republic of China. Washington, DC: DoD, 2020.