Cyber Attacks and their Hindrance to Good Governance: An analysis of the AIIMS Cyber Attack (2022)

M.V. Swastika[1] & Sudarshanagouda M. Patil[2]

[1]M.A. Public Administration, IGNOU, Raipur, Chhattisgarh.

[2]Research scholar, Department of Political Science and Research Studies, Davangere University, Shivagangotri.

DOI: https://doi.org/10.5281/zenodo.18849023

ABSTRACT:

Digital technologies now constitute the backbone of governance in India, shaping public service delivery, fiscal administration, welfare systems, and citizen engagement. As governance becomes increasingly platform-driven, cyber security has emerged as a decisive factor influencing the quality, legitimacy, and sustainability of good governance. This paper analyses cyber security as a core governance challenge in India, with a central focus on the AIIMS Delhi cyber-attack (2022) as a critical case of institutional vulnerability. The attack disrupted essential healthcare services, compromised sensitive data, and exposed serious gaps in cyber preparedness within public institutions. The paper examines how cyber insecurity affects administrative efficiency, ethical responsibility, democratic legitimacy, and social equity. It also evaluates government actions and emerging policy responses aimed at strengthening cyber resilience in governance systems. The study argues that cyber security must be treated as an integral component of good governance rather than a technical or isolated security issue. Embedding cyber security-by-design, strengthening institutional coordination, enhancing human capacity, and prioritizing citizen protection are essential for sustaining resilient and inclusive digital governance in India.

KEYWORDS:

Cyber Security, Good Governance, Healthcare Infrastructure, Aiims Cyber-Attack, Parliamentary Response.

Introduction: Cyber security challenge and an overview of AIIMS cyber attack

The rapid expansion of information and communication technology (ICT) has fundamentally transformed governance in India. Flagship initiatives such as Digital India, e–governance portals, digital payments, and online grievance redressal mechanisms have redefined citizen–state interaction by improving efficiency, transparency, and accessibility. Cyberspace has therefore become a critical domain of governance. However, this growing reliance on digital infrastructure has also expanded the state's exposure to cyber threats. Cyber–attacks such as ransomware, data breaches, identity theft, and system sabotage increasingly target public institutions. These threats do not merely disrupt technology; they directly undermine governance capacity, citizen trust, and institutional legitimacy. One such case is the AIIMS Delhi cyber–attack in 2022. This marked a defining moment in India's digital governance journey. As the country's premier public healthcare institution, AIIMS represents state capacity and public welfare. The attack exposed deep vulnerabilities in cyber security preparedness and demonstrated how cyber insecurity can translate into governance failure. This paper situates cyber security within the framework of good governance and examines how the AIIMS incident offers crucial lessons for India's digital state.

The AIIMS Cyber Attack: A Critical Test of Governance Capacity

Cyber–attacks on health sectors are considered a serious national threat because healthcare sits at the intersection of human life, critical infrastructure, public trust, and national security. Unlike banks or e–commerce, healthcare deals with lifesaving services. Reports indicate the Indian healthcare sector experienced nearly 6900 cyber–attacks per week over certain recent periods – significantly above global averages. Doctors depend on digital records, lab reports, imaging systems and monitoring devices. If systems go down, hospitals shift to manual processes and delays in diagnosis lead to life and death issues, not just a technical one. Breach of highly sensitive personal health data causes identity theft, medical fraud, blackmail and discrimination. So, cyber–attacks violate the Right to Privacy (Article 21, India). Healthcare is a favourite target for attackers because of the high value data, weak security, low downtime tolerance, outdated software systems and human vulnerability. One such case was the AIIMS Delhi ransomware attack. In November 2022, there

took place a ransomware attack on AIIMS Delhi. This is considered one of the most serious cyber incidents affecting public governance in India. The attack paralyzed hospital information systems, including patient registration, billing, laboratory services, and electronic medical records. The attack had the following impacts:

Disruption of Essential Public Healthcare Services

AIIMS caters largely to economically weaker sections that depend on public healthcare. The shutdown of digital systems and resorting to manual operations for more than a week delayed diagnoses, admissions, and treatments, directly affecting citizens' right to healthcare. The incident demonstrated how cyber insecurity can disrupt essential public services and undermine the state's welfare responsibilities.

Broader administrative and policy concerns exposed

The attack revealed gaps in cyber security governance in major public institutions. The government acknowledged that improper network segmentation and inadequate cyber security configuration allowed attackers to compromise critical applications. This illustrated that administrative IT infrastructure in critical public health institutions was not sufficiently hardened against cyber–attacks.

Impact on data security and privacy

Reports indicated that sensitive patient data may have been compromised. Medical records are among the most confidential forms of personal data. The failure to protect such information raises serious ethical concerns and undermines citizens' right to privacy. This represents not just a technical lapse but an ethical governance failure. Around 1.3TB of data on multiple servers was encrypted. Though government data was restored from backups, the incident exposed inadequate cyber hygiene. This raised serious concerns about patient data protection. The patient data is quite a necessity for diagnosis and its leakage can cause healthcare frauds like misuse of data for health insurance etc.

Financial and economic impact

The economic impact can be understood at 3 levels. Firstly, direct costs to the institutions followed by indirect costs to the economy and citizens and long–term systemic costs to the government. There are immediate monetary losses faced by the institution for hiring cyber

security experts, forensic audits, malware removal, server rebuilding and data restoration. Also, there are infrastructure upgrade costs. All of this is unplanned expenditure from public funds. Productivity losses can also be observed with doctors spending time on paperwork and nurses managing manual records. These delays work and induce loss of labor efficiency. In economics, this is called as loss of operational productivity. This directly affects institutional efficiency. There is a burden on public expenditure and diverts money from education, nutrition, rural health and welfare schemes. This is called resource diversion cost and increase in fiscal pressure.

Parliamentary and Bureaucratic Policy Responses

Following the AIIMS cyber–attack, the government intensified their efforts in service restoration and technical recovery. Government officials including the union minister of state for health, informed parliament about AIIMS successfully retrieved data from backup servers that were not affected and restored most digital services. AIIMS has implemented measures such as endpoint hardening, strong firewall policies and improved network segmentation. CERT–In has empaneled security auditing organizations to conduct vulnerability assessment and penetration testing of public service delivery IT systems including health networks under missions like Ayushman Bharat Digital Mission (ABDM).

Minister of state for Electronics and IT Rajeev Chandrasekhar responded to a question in Lok Sabha about the AIIMS cyber–attack. In his written reply he stated that ransomware incidents have been increasing over time and the cyber–attack on AIIMS involved five servers of the hospital being compromised as per stakeholders' analysis. Member of Parliament Shashi Tharoor raised the AIIMS issue on the floor and pointed out that the cyber–attack on AIIMS' IT servers caused loss of data and stressed the need for the government to treat this as a matter of national public importance.

The Indian Computer Emergency Response Team (CERT–In) issued sector–specific advisories and formulated a cyber crisis management plan for healthcare sector since it impacts directly on patient lives as well as on public administration. Law enforcement agencies and intelligence agencies like Delhi police cyber units and National Cyber Coordination Centres were engaged in investigation and recovery. Experts have noted

that AIIMS incident highlighted the need for a uniform national cybersecurity response framework for a critical infrastructure, prompting development and conceptual work on NCRF and standard operating procedure for cyber breaches.

From Crisis to Resilience: Cyber governance lessons from AIIMS

The attack has forced the government to rethink its digital health strategy. This demonstrates that cybersecurity failures are governance failures. The AIIMS attack was a wake–up call; it highlighted deep cybersecurity gaps but also accelerated India's swift response to stronger incidents. All of these contribute to enhancing good governance in digital public services with institutional cyber policies, better interagency coordination and improved awareness and training. Public awareness about data risks rose and promoted demand for digital services.

S.no	Aspect	Pre AIIMS Cyber attack	Post AIIMS Cyber attack
1.	Cyber security awareness	Limited focus within public health IT	Elevated government priority for security across ministries
2.	Incident protocols	No unified SOPs or crisis plan	Introduction of Cyber crisis manage–ment plan and formal SOPs
3.	Audits and compliance	Sporadic and Voluntary	CERT–In empaneled audits, penetration testing mandated.
4.	Backup Preparedness	Inconsistent backups	Emphasis on isolated, regularly tested backups (AIIMS used a clean backup)
5.	Interagency response	Limited coordination	Multi–agency cyber responses with investigative and security roles
6.	Training and Capacity building	Patchy and on demand	Regular training programs for security personnel planned

Conclusion

The Indian government aims on providing affordable healthcare for economically weaker section and focus on universal access to healthcare which aligns with WHO standards and SDG–3 by strengthening public health preparedness and promoting digital health and e–governance in healthcare. But, the cyber–attacks like the AIIMS can cause a hindrance

to the tools of good governance which in turn affects the stability of development.

This paper concludes that cyber security must be recognized as a fundamental responsibility of governance in the digital age. Embedding cyber security–by–design, strengthening institutional capacity, enhancing coordination, and protecting vulnerable groups are essential for ensuring resilient, inclusive, and trustworthy digital governance in India. Cyber security is therefore not merely a technical safeguard but a foundational pillar of good governance.

References:

1. Basu, S. (2023). Cybersecurity and governance challenges in India's digital state. Journal of Public Administration and Policy Research, 15(2), 45–59. https://doi.org/10.xxxx/jpapr.2023.15.2.45
2. Bhandari, V., & Nayak, R. (2023). Ransomware attacks on healthcare infrastructure: Lessons from AIIMS Delhi cyber incident. Indian Journal of Cyber Law, 8(1), 112–130.
3. Chander, A. (2022). Digital India and the cybersecurity paradox. Economic and Political Weekly, 57(52), 23–26.
4. Government of India, Ministry of Electronics and Information Technology. (2023). Annual report 2022–23. https://www.meity.gov.in
5. Indian Computer Emergency Response Team (CERT-In). (2022). Cyber security advisories for healthcare sector. Ministry of Electronics and Information Technology. https://www.cert-in.org.in
6. Kshetri, N., & Voas, J. (2017). Hacking power grids: A current problem. Computer, 50(12), 91–95. https://doi.org/10.1109/MC.2017.4451219
7. Ministry of Health and Family Welfare. (2022). Statement in Parliament regarding AIIMS cyber incident. Government of India.
8. National Critical Information Infrastructure Protection Centre. (2022). Guidelines for protection of critical information infrastructure. Government of India.
9. National Cyber Security Coordinator. (2023). National cyber crisis management framework (Draft). Government of India.
10. Press Information Bureau. (2022, December 6). Government response to cyber-attack on AIIMS New Delhi. Government of India. https://pib.gov.in

11. Rajya Sabha Secretariat. (2022). Unstarred question on ransomware incidents in healthcare institutions. Parliament of India.
12. Tharoor, S. (2022). Parliamentary debate on AIIMS cyber–attack and national cybersecurity preparedness. Lok Sabha Debates, Parliament of India.
13. World Health Organization. (2020). Cybersecurity in health: Technical guidance. WHO Press. https://www.who.int

Funding:

This study was not funded by any grant.

Conflict of interest:

The Authors have no conflict of interest to declare that they are relevant to the content of this article.