
**E-ISSN:** 2706-8927
**P-ISSN:** 2706-8919
www.allstudyjournal.com
IJAAS 2025; 7(4): xx-xx
Received: 22-02-2025
Accepted: 27-03-2025

**Dr. Naresh Kumar**
Assistant Professor (Law), MDU-Centre for Professional and Allied Studies, Gurugram, Haryana, India

**Corresponding Author:**
**Dr. Naresh Kumar**
Assistant Professor (Law), MDU-Centre for Professional and Allied Studies, Gurugram, Haryana, India

# Modern cyber warfare and the Indian legal framework: Is India equipped?

## Naresh Kumar

**DOI:** https://www.doi.org/10.33545/27068919.2025.v7.i4c.1721

**Abstract**
The rapid evolution of technology has transformed the landscape of global warfare, introducing cyberspace as a new domain of conflict where states and non-state actors engage in strategic digital operations. This paper critically examines India's preparedness to address modern cyber warfare within its existing legal and institutional frameworks. While international efforts such as the Tallinn Manual and UN Group of Governmental Experts (GGE) reports have attempted to contextualize cyber operations under international law, the absence of binding conventions leaves states vulnerable to unregulated hostilities in cyberspace.

In India, the Information Technology Act, 2000 remains the principal legislation governing cyber activities; however, it was originally crafted for e-commerce and cybercrime, not for state-sponsored cyber operations or hybrid warfare. Through case studies including the Mumbai power grid attack (2020) and the AIIMS ransomware incident (2022), this paper highlights the inadequacies of India's cyber defence mechanisms and institutional coordination. Judicial interventions, particularly in *Shreya Singhal v. Union of India* and *K.S. Puttaswamy v. Union of India*, have strengthened digital rights and privacy, but a strategic lacuna persists in national cyber defence law and policy.

The paper concludes by recommending the enactment of a comprehensive Cybersecurity and Cyber Defence Law, formulation of a National Cyber Defence Doctrine, and enhanced international cooperation. These steps are essential to secure India's sovereignty and resilience in the age of cyber warfare.

**Keywords:** Cyber Warfare, Cybersecurity, Information Technology Act, 2000, Bhartiya Nyaya Sanhita, 2023, Tallinn Manua, International Law, National Security, Data Protection, Cyber Defence, Artificial Intelligence, Hybrid Warfare, India's Legal Framework, Cyber Terrorism, Digital Sovereignty

## 1. Introduction
The nature of warfare has undergone a paradigm shift in the 21st century. Traditional kinetic wars are being replaced or supplemented by cyber warfare—an invisible battlefield where states, non-state actors, and organised cyber units contest power through digital means [1]. Cyber warfare is distinct from cybercrime in that it is often politically or militarily motivated, targeted at critical national infrastructure, sovereignty, or national security [2].

For India, the stakes are exceptionally high. With over 850 million internet users [3]. expanding digital infrastructure, and reliance on critical information systems, the country presents itself as a high-value cyber target. Yet, the legal and institutional response remains rooted in the Information Technology Act, 2000, which was primarily designed to regulate e-commerce rather than modern cyber warfare.

## 2. Concept of Modern Cyber Warfare under International Law
The Tallinn Manual, developed under NATO auspices, offers the most authoritative non-binding interpretation of how international law applies to cyber warfare [4]. It clarifies that cyber operations causing physical damage or loss of life may constitute an "armed attack" within the meaning of Article 51 of the UN Charter [5].

Additionally, the UN Groups of Governmental Experts (GGE) have affirmed that international law—including sovereignty, non-intervention, and the prohibition on the use of force—applies to cyberspace [6]. However, there is no binding treaty governing cyber warfare, leaving states, including India, in a vulnerable position where attribution and accountability remain blurred.

### 3. Vulnerability to Cyber Warfare

India's experience demonstrates the seriousness of cyber threats:

- In October 2020, a major power outage in Mumbai was linked to suspected Chinese state-sponsored actors targeting India's power grid [7].
- In 2022, AIIMS Delhi suffered a ransomware attack, crippling hospital operations and compromising sensitive medical records of high-profile individuals [8].
- Repeated cyber intrusions into defence networks and disinformation campaigns on social media platforms highlight the risks of hybrid warfare [9].

These incidents reveal India's strategic vulnerabilities, particularly the lack of robust cyber defence legislation and mechanisms tailored to modern warfare.

### 4. Indian Legal Framework

#### 1. Information Technology Act, 2000

The IT Act, 2000, remains the cornerstone of India's cyber law. Section 66 deals with hacking, Section 66C with identity theft, and Section 66F defines "cyber terrorism," punishable with life imprisonment [10]. However, the Act was drafted for commercial transactions and cyber fraud, not state-sponsored cyber operations.

#### 2. Indian Penal Code / Bharatiya Nyaya Sanhita, 2023

The IPC (now replaced by the Bharatiya Nyaya Sanhita, 2023) contains provisions on conspiracy, sabotage, and offences against the state, but these are ill-suited for cyber-specific threats [11].

#### 3. Evidence Act, 1872

Section 65B governs admissibility of electronic evidence. In Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, the Supreme Court held that electronic records are admissible only if accompanied by a proper certificate under Section 65B [12]. This case emphasises the strict evidentiary standards applicable to cyber investigations.

#### 4. National Cyber Security Policy, 2013

Although ambitious in vision, the policy remains aspirational, lacking statutory force [13].

#### 5. Institutional Mechanisms

India has established the Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), and the Defence Cyber Agency [14]. However, these institutions remain fragmented and operate without a unified legal framework.

### 5. Judicial Approach

Judicial pronouncements have indirectly shaped India's cyber law discourse.

In Shreya Singhal v. Union of India, (2015) 5 SCC 1, the Supreme Court struck down Section 66A of the IT Act as unconstitutional, protecting free speech from vague cyber restrictions [15].

In K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, the Court recognised the right to privacy as a fundamental right under Article 21, laying the foundation for robust data protection in cyberspace [16].

In Anvar P.V., the Court underscored the necessity of strict compliance with Section 65B, significantly impacting the evidentiary framework for prosecuting cyber offences [17].

Together, these judgments illustrate judicial awareness of digital rights but fall short of addressing state-sponsored cyber warfare.

### 6. Comparative Perspective

- **United States:** The U.S. Cyber Command (USCYBERCOM) is integrated with the Department of Défense. The Computer Fraud and Abuse Act criminalise cyber intrusions [18].
- **European Union:** The GDPR and the EU Cybersecurity Act (2019) provide a robust regime for data protection and resilience [19].
- **China:** Cyber warfare is embedded within military doctrine, focusing on information dominance and asymmetric capabilities [20].
- **Russia:** Known for hybrid warfare, Russia has combined cyber operations with disinformation campaigns, particularly in Ukraine [21].

Compared to these powers, India's response is piecemeal, lacking a dedicated cyber warfare doctrine.

### 7 Limitations in India's Current Framework

- **Outdated IT Act:** Designed for e-commerce, not cyber warfare [22].
- **Absence of Comprehensive Cybersecurity Law:** No statute specifically addresses cyber defence or offensive strategies.
- **Attribution Issues:** Identifying state-sponsored attackers remains a grey area.
- **Weak Enforcement:** Lack of forensic capacity and coordination among agencies [23].
- **Global Isolation:** India is not a signatory to the Budapest Convention on Cybercrime, limiting international cooperation [24].

### 8. Recommendations

- **Comprehensive Cybersecurity Law:** Enact a statute tailored to cyber warfare, AI, and protection of critical infrastructure [25].
- **National Cyber Defence Doctrine:** Clearly define offensive and defensive strategies within the legal framework.
- **Critical Infrastructure Protection Act:** Mandate sector-specific cyber standards and reporting obligations.
- **Strengthen Forensics and Capacity Building:** Train judicial officers, prosecutors, and cyber experts.
- **International Engagement:** Consider joining or proposing alternatives to the Budapest Convention.
- **Regulation of Disinformation and AI:** Address deepfakes and AI-driven cyber threats while upholding Article 19(1)(a) [26].

### 9. Conclusion

Cyber warfare is no longer hypothetical; it is a pressing national security concern. While India has taken steps through CERT-In, NCIIPC, and the Defence Cyber Agency, reliance on the IT Act, 2000, is inadequate. The judiciary has advanced privacy and digital rights, but legislation must catch up with technological realities. A comprehensive cyber defence law, backed by robust enforcement and

international cooperation, is essential if India is to safeguard its sovereignty in the digital era [27].

**References**


1. Singh S. Cybersecurity and cyber warfare in the 21st century. Indian Defence Review. 2021;36:1-10.
2. Kshetri N. Cybersecurity and international relations. Journal of International Affairs. 2015;68:1-15.
3. Telecom Regulatory Authority of India. Telecom subscription data. New Delhi: TRAI; 2023.
4. Schmitt MN, editor. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press; 2017.
5. United Nations. Charter of the United Nations, Article 51. San Francisco: United Nations; 1945.
6. United Nations. Group of Governmental Experts report on developments in the field of information and telecommunications in the context of international security. New York: United Nations; 2015.
7. Chaudhuri PP. Mumbai power outage and Chinese cyber operations. Hindustan Times. 2020 Oct 16.
8. AIIMS ransomware attack. The Hindu. 2022 Dec 1.
9. Chadha V. Hybrid warfare in the Indian context. New Delhi: Institute for Defence Studies and Analyses (IDSA); 2021.
10. Information Technology Act, 2000, § 66F (India).
11. Bharatiya Nyaya Sanhita, 2023, Chapter VI (India).
12. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
13. Ministry of Electronics and Information Technology (MeitY). National Cyber Security Policy. New Delhi: Government of India; 2013.
14. Indian Computer Emergency Response Team (CERT-In). Annual Report. New Delhi: CERT-In; 2022.
15. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
16. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
17. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
18. United States Congress. Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Washington (DC): Government Printing Office; 1986.
19. European Union. EU Cybersecurity Act, Regulation (EU) 2019/881. Brussels: European Parliament and Council; 2019.
20. Kania E. China's strategic thinking on cyber warfare. Santa Monica (CA): RAND Corporation; 2019.
21. NATO Strategic Communications Centre of Excellence (StratCom COE). Russia's hybrid warfare tactics. Riga: NATO StratCom COE; 2018.
22. Gupta A. Outdated IT Act and the need for reform. Economic & Political Weekly. 2020;55(42):1-4.
23. National Critical Information Infrastructure Protection Centre (NCIIPC). National critical information infrastructure audit report. New Delhi: NCIIPC; 2021.
24. Council of Europe. Convention on Cybercrime (Budapest Convention). Budapest: Council of Europe; 2001.
25. Reddy P. India's missing cybersecurity law. The Print. 2022 Jul 15.
26. Rajagopal R. Deepfakes and Indian law. Supreme Court Cases (Journal). 2021;6:45-52.
27. Raja Mohan C. India and cyber sovereignty. The Indian Express. 2023 May 20.