INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CRITICAL INFRASTRUCTURE PROTECTION AND CYBER LAW: A DEFENCE-ORIENTED COMPARATIVE ANALYSIS OF INDIA AND JAPAN

AUTHOR - ADV. VANSHIKA SAINI* & DR. JYOTI YADAV**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – ADV. VANSHIKA SAINI & DR. JYOTI YADAV, CRITICAL INFRASTRUCTURE PROTECTION AND CYBER LAW: A DEFENCE-ORIENTED COMPARATIVE ANALYSIS OF INDIA AND JAPAN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 718-730, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I470

ABSTRACT

The Research paper takes a critical comparative analysis of cyber law framework which involve the protection of critical infrastructure of two technologically advanced democracies: India and Japan. At the time when state sponsored cyberattacks emerged the national threats to national security, the need of critical infrastructure protection has assumed paramount significance. India's framework for the cyber related crimes which is Information Technology Act, 2000 merely deals with commercial transactions rather than national security imperatives. In contrast, Japan has developed a defence oriented cybersecurity ecosystem deals under Basic Act on Cybersecurity, 2014 and supported by robust institutional coordination mechanisms.

This paper involve a doctrinal and comparative legal methodology, this involves primary sources including legislative texts, judicial decisions, and policy documents, with companion by secondary sources like International regulatory bodies. The main research problem is whether India's Cyber law framework is adequate to protect contemporary defence threats. The hypothesis advances is that India's current Cyber law frameworks suffers enforcement gaps, definitional vagueness, and failure in institutional coordination that represent it insufficient when standardised against Japan's More integrated and defence oriented Cyber security model.

The core insights indicate that India lacks critical infrastructure protection statute for the dimension of defence security of cyberspace with requisite clarity. Whereas, Japan's framework is more dedicated legislation, and proactive threat sharing mechanisms. The Paper concludes with recommendations for legislative reforms, restructuring of framework and cyber related policy innovations to enable India to strengthen up cyber law infrastructure with respect to the national security and digital ambitions.

Keywords: Cyber Law, Critical Infrastructure Protection, National Security, India, Japan, Information Technology Act 2000, NCIIPC, Basic Act on Cybersecurity, Comparative law, Defence Infrastructure.

INTRODUCTION

1. When Cyberspace become a Battlefield

In the growing digital environment, cyberspace is not merely a tool used for academics and research. Today it runs each and every sector of the society i.e. financial systems, hospital sectors, government services and so on. It is said to be the invisible string to the visible world. Various countries have recoganise the cyberspace as the fifth domain of pertaining

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

warfare- alongside land, sea, air and space, which generally changed the fundamental government thing over security, sovereignty and competition.

Unlike Traditional battlefield, cyberspace has no boundaries and no fixed geography. Internet become a source of crime and anybody in today's world can commit crime through it. Internet is the new weapon for the criminals, and criminals by being in apartment with a laptop can have the possibility to damage various aspects in humans' life. This not only impact the local public but have the tendency to impact the government.

One of the most tenacious challenge is the attribution of the problem, to figure out who is behind the attack and from where it took place. Generally in traditional warfare, there is involvement of army, territory and visibility but in the Cyber warfare there is opaque walls which hides the individual behind it, attacks conquer from the multiple countries, disguised using pseudonym, and map out to obscure the origin of the attack. Cyber domain is not well designed to deal with the ambiguity of these type situations, it apparently more focuses on the crime which involves the identity of individuals. Every country is under pressure to build there frameworks that are technically more advance, and capable of tackling the futuristic threats that take evolve rapidly than legislation itself.

2. Why Critical Infrastructure Matters

Critical Infrastructure in the simpler language, is the systems and networks which is both physical and digital that a country cannot afford to lose in of the situation. For example water treatment facilities, financial networks, nuclear plants, military command systems and telecommunications networks, their disruption would not be inconvenient, it would be extremely dangerous as it will cause direct harm to public safety, economic stability, or national security.

Now these systems have moved online over the past two decades, driven by the need of efficiency, development and growth of connected devices, they become more effective but also more exposed to all in the name of transparency. The same requirement of connectivity over the internet made modern infrastructure smarter but at the same time smartly targeted.

The risk is not merely a hypothesis, evidence related to that are as, in 2010, the Stuxnet Malware widely injected to United States and Israel, physically destroyed Iranian nuclear Centrifuges by manipulating the software controlling them. It was the first time when a cyber attack caused the physical damage to industrial equipment, and it changes the scope of cyber attack as whole, and world named it as cyber weapon. In 2015 and 2016, separate cyber attacks on Ukraine's power grid, leads to the situation where people lived without electricity in winter. In 2021, ransomware attack on the colonial pipeline disrupted fuel supplies across a large part of the eastern United States, which cause panic in the state over buying and shortage of fuel within days.

Similarly, India also been the victim of such attacks where, in 2020, a Chinese Cyber Intrusion was detected, which targeted administrative network of the Kundankulam Nuclear Power Plant in Tamil Nadu. The plants operators earlier denied the breach but later on confirmed it. The incident raised serious questions how well India's most sensitive infrastructure is actually protected and whether the legal and institutional framework is equipped to respond.

Modern Military operations depend entirely on secure digital systems for various activities such communication between units, logistic and supply chain managements, weapon guidance, sharing intelligence. If the system get compromise before or during the conflict, the consequences go far beyond the data loss which may include leaking sensitive information, exposing of operational and organisational structure, command and control systems can be disabled when needed the most and so on which is far beyond the normal

person thinking. Therefore, protecting the critical infrastructure is not just bureaucratic move or commercial concern, but at core a question on country whether it can depend itself.

3. The Threat Landscape Today

Cyber threats environment has changes significantly even in the last five years. Threats have become more targeted, more damaging and more patient enough to wait and surface. The most serious threat which was called Advanced Persistent threats by the cybersecurity analyst, in nature it is long, carefully planned intrusion campaigns rub by state backed up groups. These are the smart operations which involve months and years of slow and quiet access in to system, before executing the attack, attacker study the systems, steal data and plant malware which can be activated later.

It is believed that groups sponsored by Russia, China and North Korea have the capability and intent to target critical infrastructure in other countries. Groups such as APT28, attributed to Russian military intelligence, have previously targeted European energy and electoral organisations, whilst China's military sponsored APT41 has targeted defence contractor, telecommunications companies, and healthcare systems around the world. With that, lazarus group, associated with North Korea, has been behind some financial cyber attacks, including theft of hundreds of million dollars from banks.

Ransomware is now a big threat to public infrastructure, even when it starts out as a criminal operation that wants to make money. Utilities, hospitals, and city water systems have all been affected. The ransomware attack on AIIMS Delhi in November 2022 was a clear example of this. The attack brought the hospital's digital systems to a standstill for weeks, forcing staff to go back to using paper records and affecting millions of patient files. AIIMS is one of the most important public hospitals in India. The attack showed how weak the country's health infrastructure is, even though it is not officially considered critical infrastructure under current Indian law. Cyber spying on military communication networks, defence research institutions, and diplomatic channels adds another layer of danger to an already serious situation.

4. India's Exposure and the Gaps in Its Law

India's role in all of this is important and, in some ways, contradictory. It is the world's largest democracy, one of the fastest-growing digital economies, and a military power that is becoming more important and has real goals for the region and the world. There are more than 800 million people who use the internet. The government provides a huge number of services online. Digital infrastructure is very important to its financial system. And its military is quickly becoming more modern, relying more and more on networked systems and digital logistics.

All of that makes India a high-value target. The Information Technology Act of 2000, which governs cyber activity in India, was written in a very different time and for very different reasons. It was based on a UN template that was made to make electronic transactions legal and help e-commerce grow. The main concern was not national security. The effects on defence were hardly thought about.

Sections 69 and 70 of the IT Act are the only parts that deal with critical infrastructure. They are not very broad and are not very well enforced. The NCIIPC is in charge of protecting important information infrastructure, but there is no law that gives it clear and binding power over private operators of important systems. CERT-In is in charge of responding to incidents, but it doesn't have the legal tools to force the kind of quick, coordinated action that a serious attack would need. Over the years, many expert groups have suggested that there should be a separate law for protecting critical infrastructure. None has come to pass. That gap is one of the biggest and most long-lasting problems with India's national security system.

5. The Core Problem: A Scattered and Insufficient Framework

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The main issue this paper looks at is that India's cyber law and critical infrastructure protection are not well-organised. The IT Act, the NCIIPC, CERT-In, and other notifications and directions are all there, but they don't make a complete system. There are real vulnerabilities because there are grey areas between institutions, coordination failures during incidents, and legal ambiguities.

Japan is a good example of the opposite. Japan passed the Basic Act on Cybersecurity in 2014 after taking a long, hard look at its cybersecurity situation in the early 2010s. That law put all of the government ministries, defence agencies, and private sector operators under one coordinated framework. It made the NISC the main group in charge of oversight and coordination. It put a clear philosophy—proactive cyber defense—into the plans of both the military and civilians. Japan has also kept updating its national cybersecurity strategy on a regular basis, treating it like a living document instead of something that was done once.

When you compare India and Japan, you are not saying that India should just do what Japan has done. The two countries have different strategic situations, different legal traditions, and different constitutional frameworks. But the comparison shows something important: a planned, well-organised legal system leads to much better results than a broken one. That lesson is very important for India, and it is very important that people act on it.

RESEARCH OBJECTIVES

This Research have five clear objectives that together aim to provide clear picture of cyber law connects to Critical infrastructure protection, with primary focus on Japan and India.

The first and foremost objective is determine whether the India's existing cyber law, mainly the IT Act, 2000 along with its amendments and related rules, genuinely have the capability of protecting critical infrastructure from serious cyber threats.

The second objective is to closely examine Japan's Cybersecurity legal framework, especially the primary act which is Basic act on Cybersecurity, 2014, the role of NISC and how japan integrated cybersecurity into defence planning. It is to understand the both the countries comparatively.

The third objective is to identify how India and Japan have outline the priorities in the field of cyber law, how their institutions are set up and the laws interpreted in the real world. This will help in understanding the differences why one system is better prepared than the others.

The forth objective is to look at what India's judiciary system contributed to cyber law, particularly Supreme Court judgments which touched digital rights, state security and control over cyber space.

The fifth and the final objective is to put clear and practical recommendations for reforming India's legal and institution frame work. These will draw on lessons from Japan but by keeping India's legal traditions, strategic position and institutional realities in mind.

HYPOTHESIS

The core argument of this paper is that India's Cyber law framework is not fully ready to tackle the modern cyber threats to critical infrastructure. Some of the reasons to this context are, India doesn't have dedicated law built specifically for critical infrastructure protection, enforcement of law is quite weak and lack of coordination in the institutions, and the existing law was designed with business and administration in mind, not defence.

The IT Act's sections on critical infrastructure i.e. Section 70 and Section 70 A are vague. The NCIIP has no strong statuary backing. Whereas, Japan's framework brings every aspect under one clear law, which makes the case for serious reform in India.

LITERATURE REVIEW

Western Scholars have written a lot about cyber law and critical infrastructure, but some of the

work doesn't fit the Asian context well. Virginia Greiman has argued that the current international laws those about armed conflict, don't cover state sponsored cyberattacks. This generally means that the countries have to fill these gaps by its own. And India Faces the exact problem, since its laws are not defence focused.

The ITU has pushed members to strengthen cyber laws and share information across borders. India Participates in these global forums but the growth is slow or stagnant.

Domestic Scholars like R.K Vyas has been one of the few Indian scholars to seriously examine the IT Act from the perspective of National Security, where his main finding is that IT act was never designed to tackle security threats. Amendments of 2008 and 2022 CERT –IN directions have added complexities without creating a clear and well oragnised framework.

If we looks at Japan Scholars like Odebade, he pointed out how the country moved from reacting to cyberattacks towards a practical approach to deal with, Basic Act on Cybersecurity 2014 was key step towards it. Japan's alliance with United States has also pushed it to build cyber systems that can work alongside the American ones.

The gap in the existing research is vibrant that there is very little work that compares India and Japan specifically on defence and national security cyber law, while also looking at judiciary decisions and how their legal systems actually work. This paper tries to fill that gap.

RESEARCH METHODOLOGY

I. Doctrinal Research

This research adopts the doctrinal methodology, which involves systematic examination, analysis of primary legal sources, statues, regulations, judicial decisions and official policy documents, with this secondary sources like scholarly commentaries. This doctrinal approach is appropriate because the main questions of the paper are more reclined towards the structure, content and legal frameworks, and their analysis requires the application of legal reasoning.

The doctrinal approach of research proceeds at three levels. At the first level it involves an examination of the relevant legislation of India and Japan, IT Act 2000 and Basic Act on cybersecurity respectively with amendments. Second level involves analysis and interpretation of judicial decisions in regards. Third level involves examination of policy documents which includes policy documents, national cybersecurity strategies, committee reports, and regulatory guidelines.

II. Comparative Legal Method

The comparative dimensions of the research employs comparative study between the countries with respect to their legal framework, comparison doesn't involve the negative perspective but dealt with positive ones. This method allows the study to formulate in new direction and with critics in mind.

III. Sources

- **Primary –** The Information Technology Act, 2000(as amended); the Information Technology (Amendment) Act, 2008; rules and regulations made under the IT Act, IT rule, 2009; CERT-In directions 2022; National Cyber Security Policy, 2013; decisions of the supreme court of India Shreya Singhal v. Union Of India (2015); Justice K.S. Puttaswamy v. Union of India 2017; and Anuradha bhasin v. Union of India 2020; Basic Act on Cybersecurity 2014; cybersecurity strategies (2013,2018,2021); and official reports of the NISC.
- **Secondary –** Journal articles, policy papers, observer research, reports from international organisations, reports from ITU, UN group reports.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CHAPTER 1: UNDERSTANDING CYBER LAW AND WHY CRITICAL INFRASTRUCTURE NEEDS PROTECTION

1.1 How Cyber law has changed over time.

To understand Cyber Law it can be said that Cyber Law in its purest form is simply the set of rules that governs how people, or companies, and Governments act and behave in digital spaces - How they create information, how they share it or how it is used online and stored. Its scope is vast and draws from various areas and subjects of law which includes Criminal Law, Contract Law, and Constitutional Law, and it has grown significantly as the Internet has become the everyday essential.

If we go back in past, cyber law has evolved through three broad stages. The first stage timeline is 1990s and early 2000s, A significant era in terms of cyber law concerning mainly over Ethical online business. Laws such as Information Technology Act, 2000 - was designed to give legal standing to all forms of digital contracts and Electronic Signatures.[1433] The aim was commercial centric rather security oriented.

After the major terrorist attack held on 9/11 in 2001, governments increased their security in terms of cybercrime and cyber terrorism. Meanwhile India also updated its existing IT Act in 2008, adding stricter clause and stronger penalties for cybercrime and expanded the government powers to monitor digital communications.[1434] The Budapest Convention on Cybercrime, adopted by Council of Europe in 2001, showcases same global advancements in regards to it.[1435]

Currently, Cyber Law has entered its Third Stage. The focus has increased beyond penalising and prosecuting criminals toward protecting National Infrastructure and Managing State-Sponsored Threat. This is where Japan has outperformed India and India needs to level things like Japan.

1.2 Cyber Law as a National Security tool.

The perception about Cyberspace has changed drastically amid continuous intervention from criminal organisations. Cyberspace in no longer just a place for commercial activities or communication. Governments, armed groups, and criminal organisations all compete within it for control over system, information and ability to cause disruption. This situation has forced countries to understand the real use case of cyber law and what cyber law actually is.

Three significant things follow from this shift - First, Cyber Law cannot be sit in isolation - It needs to go hand in hand with defence law, intelligence law, and emergency powers to form a coherent national security framework which acts as a defensive shield. Second, Enforcement of Cyber law shouldn't be only on the shoulders of police and civilian regulators. Defence and Intelligence Wings specialised and trained with extensive technical capabilities to detect and respond to state level teams or various QRTs need to be legally empowered to act. Third, the law needs to be flexible. Cyber threats are dynamic and evolve quickly, and an old statute drafted five years back may already be outdated in most probable cases.

1.3 What Cyber attacks mean for the Military.

Modern militaries run on digital systems - all the communications, logistics, weapons guidance, or even intelligence sharing. All these are potential targets. The concept of cyber warfare is growing and it is now not just a speculative thought rather it is an operational reality. The United States, the United Kingdom, China and Japan - all these nations have a specialised unit in their military, comprising of cyber units, dedicated wholly to cybersecurity because they understand that cyber operations can achieve same effect comparable to conventional military action.[1436]

India also acknowledged it and Indian military, in a Joint Doctrine of 2017 acknowledged that

[1433] Information Technology Act 2000 (Act No 21 of 2000); UNCITRAL Model Law on Electronic Commerce (1996).

[1434] Information Technology (Amendment) Act 2008 (Act No 10 of 2009).

[1435] Council of Europe, Budapest Convention on Cybercrime (2001).

[1436] MN Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd edn, 2017).

cyberspace is a key domain of future conflict, but acknowledging the problem in a policy document and building a legal framework to support it are two very different things.[1437] India, although have in paper accepted the possibilities and importance of cyberspace, but still the latter part remains incomplete.

CHAPTER 2: WHAT THE LAW ACTUALLY SAYS- INDIA'S FRAMEWORK AND ITS WEAKNESSES

2.1 The It Act and what it was Built For

The Information Technology Act, 2000 is India's main cyber law, the purpose of it was to support the growth of e-commerce and e-governance, but not to protect national security infrastructure.[1438] This act has given legal recognition to digital signatures and electronic contracts, which was indeed genuinely useful, but the purpose has shaped everything about how the act and the law works and the perception and image was clearly telling that national security was never the priority.

The 2008 amendments although added some security related provisions and clause and also expanded government surveillance powers, but the underlying architecture or the core of the law remain the same. The concept was still same built for the commercial regulation, with some points stretched to cover security needs, it was not designed for.[1439]

2.2 The key sections and where they fall short

If we look at the sections, we can clearly see that section 69 gives the government, the power to intercept or monitor digital communication in the interest of national security or public order.[1440] This sounds safe and broad but the procedural safeguards attached to it - A review committee process - have been criticised as inadequate. Also, the Supreme Court confirmed in the Puttaswamy case that privacy is a fundamental right.[1441] This section also does not address modern encryption effectively with significantly limits its practical usefulness.

Section 70 is supposed to protect Critical infrastructure. It allows the government to designate computer system and label them as "protected systems" with criminal penalties of up to 10 years imprisonment for unauthorised access. But there are three problems undermining it.[1442] First, the designation process has been used improperly and many or most obviously critical systems have never been flagged formally designated. Second, section 70 only addresses unauthorised access and has no clause for other serious threats like disruption, insider attack or Malware prepositioning. Third, it does not fit with proverb - precaution is better than cure that means it creates no proactive security obligation for system operators. It only punishes after a breach has already occurred and criminal penalties mean very little when the attacker is a foreign government safely beyond Indian jurisdiction.

Section 70A created the NCIIPC in 2014, tasked with protecting Critical Information Infrastructure. The NCIIPC operates under the NTRO has developed useful guidelines and coordinate with some public and private sector bodies. [1443] NTRO is a technical intelligence organisation rather than as an independent statutory agency. Its guidelines are advisory for most private operator and lakh authority to compel compliance or the budget to attract Top technical talent in a competitive market.[1444]

2.3 What the Courts have said

Important Landmark cases that shaped India's Cyber Law Landscape -

In Shreya Singhal versus union of India, 2015, a prominent case where the court struck down

[1437] Joint Doctrine Indian Armed Forces (Headquarters Integrated Defence Staff, 2017).
[1438] RK Vyas, *Cyber Law and Practice: A Guide for Legal Professionals* (Wadhwa & Co, 2nd edn, 2018).
[1439] A Pillai, 'Critical Information Infrastructure Protection in India: Legal Framework and Challenges' (2021) 63(3) Journal of the Indian Law Institute 287.
[1440] Information Technology Act 2000, s 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.
[1441] Information Technology Act 2000, s 70; S Goel, 'The Adequacy of Section 70 of the Information Technology Act for Critical Infrastructure Protection' (2019) 12(4) NUJS Law Review 441.
[1442] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
[1443] Information Technology Act 2000, s 70A.
[1444] National Critical Information Infrastructure Protection Centre, 'About NCIIPC' (Government of India) https://www.nciipc.gov.in accessed 15 January 2024; Observer Research Foundation, 'India's Cyber Security Landscape: What Needs to Change?' (ORF Occasional Paper No 237, 2020).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

section 66A of the IT act had been used to silence online criticism and political dissent.[1445] The court held that restrictions on online speech must meet the constitutional standard as restrictions on any other form of expression. That means it has to be considered with same restrictions as to any other form of expression. This was an important protection for Civil liberties but the question remains same, the decision was still about civil liberties, not about national security dimension of cyber law.

In Justice K.S. Puttaswamy v Union of India 2017, a nine judge bench confirmed that privacy is a fundamental right under the Constitution.[1446] This has directly impacted cyber law - any interference from government or surveillance from government or monitoring of digital systems must now be legally justified.

In Anuradha Bhasin V Union of India 2020 the Court ruled that indefinite internet shutdowns are unconstitutional.[1447] Any restrictions on internet access, including those that might be imposed during a cyber attack on critical infrastructure must be temporary, proportionate, and subject to review. This sets, important boundaries for how the government can use emergency powers in a cyber crisis.

All these decisions by the court clearly shows that the decisions are for safeguarding individuals interest but still not showcased the government's affirmative duty to defend critical infrastructure or on the legal framework for defence oriented cyber operations.

2.4 Enforcement Problems

In India, the enforcement is the main problem. Laws are drafted in a paper but enforcement on the ground level is still a tedious job. India has too many agencies with overlapping responsibilities. CERT-In, NCIIPC, the National Cyber Coordination Centre, the Cyber and Information Security Division of the Ministry of Home Affairs, and defence and intelligence agencies — each with its own mandate and culture, and insufficient mechanisms to make them work together.[1448]

There is also a serious skills shortage. Qualified cyber security professionals are in far higher demand than the government can meet and public sector salaries cannot compete with private technologies company. This means that government has to allocate some funds and provide technical assistance and training to individuals engaged in this job and bait them with good salary so that they don't work reluctantly.

The privatisation is also an issue, a large portion of India's critical infrastructure - telecom, finance, energy, healthcare is in private hands. Protecting it depends on private operator cooperating with government agencies.[1449]

India's National Cyber Security policy dates from 2013 - over decade ago before, Ransomware became a geopolitical weapon and before AI-enhanced cyber attacks became a real threat.[1450] The Defence Cyber Agency set up in 2019, is a positive development, but still lacks a clear statutory mandate and defined relationship with civilian cyber agencies.[1451]

CHAPTER 3: JAPAN'S APPROACH – WHAT A COHERENT FRAMEWORK LOOKS LIKE

3.1 The Basic act on Cybersecurity

Japan's basic act on cybersecurity, passed in 2014, is the foundation of everything Japan does in cyberspace.[1452] It was a response to various serious cyber attacks that happened on Japanese government and its corporate networks, and it reflected a deliberate and crucial decision to stop patching a fragmented and divided system instead build something coherent from the ground up.

[1445] Shreya Singhal v Union of India (2015) AIR 1523 SC.
[1446] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
[1447] Anuradha Bhasin v Union of India (2020) 3 SCC 637.
[1448] Parliamentary Standing Committee on Information Technology, '12th Report: Cyber Crime and Cyber Security' (Lok Sabha Secretariat, 2018).
[1449] Ministry of Electronics and Information Technology, 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000' (CERT-In Directions, 28 April 2022).
[1450] National Cyber Security Policy 2013 (Department of Electronics and Information Technology, Government of India).
[1451] N Subramanian, 'Bridging the Gap: Cyber Law Reform in India and the Imperative of a Dedicated Critical Infrastructure Protection Statute' (2022) 34(1) National Law School of India Review 55.
[1452] Basic Act on Cybersecurity (Act No 104 of 2014) (Japan); BO Odebade, 'Japan's Cybersecurity Law: A Study of the Basic Act on Cybersecurity and Its Implications for National Security' (2020) 14(2) Asian Journal of International Law 112.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The act unlike India does not try to regulate e-commerce or digital contracts - those are handled under other laws. It focuses entirely and wholly on cybersecurity as a national policy priority. The focus on the obligations of government agencies and critical infrastructure operators makes it much more sharper instrument than India's IT Act.

The Act established the Cybersecurity Strategy Headquarters, headed by the Chief Cabinet Secretary equivalent of a senior cabinet minister with membership from all relevant government departments.[1453] This type of positioning at the top of the government sends a clear signal about Japan's vision and sincerity towards Cybersecurity and also creates political accountability that has no equivalent in India's Structure.

3.2 The NISC and how it coordinates

The NISC is Japan's central body for cybersecurity and its coordination. It keeps an eye on government networks, coordinates the response to major incidents and oversees critical infrastructure protection across different sectors and manages international cybersecurity cooperation.[1454]

NISC is not just different from NCIIPC in terms of scope but also in legal authority. The NISC has a clear statutory mandate under the basic act. It has rights and explicit legal authority to gather information from both government and private entities about cyber incidents. It coordinates critical infrastructure protection through sector specific liaison councils - a regular forum where government agencies, regulators and private operators share intelligence and coordinate responses.[1455] This is the kind of privatisation and public private cooperation that Indian framework talks about or majorly in written form but has not actually built or enforced.

3.3 How Japan protects critical infrastructure

Japan flagged thirteen critical infrastructure sectors which includes communications, aviation, railways, electricity, gas, government services, healthcare, water, logistics, chemicals, petroleum, and financial card services. For every sector, a lead government agency is responsible for setting security standards, conducting risk assessments, and coordinating incident response. This is pretty much clearer than India's case by case designation mechanism operationally.

Japan's framework covers the full lifecycle of threat management: prevention through security standards and supply chain requirements, response through coordinated incident management; and recovery through business continuity planning. On the other hand India's framework creates no proactive security obligations- it only punishes after breach has occurred. The system is primarily reactive and not focusing on building systemic resilience.

3.4 How Cyber Defence connects to Japan's military

The Japan's Self-Defence Force Cyber Defence Unit was formed in 2014 and has witnessed a large expansion since then.[1456] Japan has also announced its 2022 National Security Strategy, which includes its plan for expanding its cyber defence forces and developing active cyber defence capabilities, including the authority to launch a cyber operation targeting an adversary's systems in response to a cyber attack on Japanese territory.[1457]

Japan and the US alliance has also been a contributing factor to Japan's expanding cyber defence forces. In 2019, both nations agreed that a cyber attack qualifying as an armed attack would trigger mutual defence commitments under the Japan-US Security Treaty.[1458] This kind of strategic security assurance would not be possible through

[1453] Basic Act on Cybersecurity (Act No 104 of 2014) (Japan), art 25.
[1454] National Cyber Security Incident Readiness and Strategy Centre, 'NISC Overview' (Government of Japan) https://www.nisc.go.jp/eng/index.html accessed 15 January 2024.
[1455] NISC, 'Cybersecurity Policy for Critical Infrastructure Protection (4th edition)' (Government of Japan, 2017).
[1456] National Security Strategy of Japan (Government of Japan, December 2022).
[1457] T Matsuda, 'Active Cyber Defence in Japan: Constitutional Constraints and Strategic Imperatives' (2023) 18(1) Asia Pacific Journal of Law and Policy 34.
[1458] Cybersecurity Strategy (Cabinet Decision, 28 September 2021) (Japan).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Japan's own means. India does not currently have a similar agreement, although countries like the Quad are forcing a similar situation to come into place.

CHAPTER 4 COMPARING THE TWO SYSTEMS AND WHAT INDIA SHOULD DO

4.1 The Legislative gap

The basic and most fundamental difference between India and Japan is designing of their foundational laws. Indian IT Act tries to sum up everything at once - e-commerce, cybercrime, surveillance, critical infrastructure protection and in the end none of these things works as well as how a focused law would. The critical infrastructure provisions have never received the legislative attention their strategic importance demands, because they share space with commercial and administrative provisions that have anciently been the Act's main concern.

On the contrary, Japan's Basic Act on cybersecurity focuses on single goal - it governs cybersecurity as a national policy priority. That focus had given clarity and operational coherence that India's multipurpose statute simply cannot match. [1459]

Japan's sector-specific designation of thirteen crucial infrastructure sectors, each with a designated lead authority, is also significantly clearer than India's case by case executive designation under section 70. Japan's sector specific model produced more proportionate results and effective regulation.[1460]

4.2 Reactive v. Proactive

As mentioned earlier - India's framework creates no proactive security obligations- It only punishes after breach has been done. The system is primarily reactive and the main legal tools are criminal prosecution, incident reporting, and after the fact designation. They all are responses not strategies to prevent. Meanwhile Japan's Framework is built totally on assumption and calculated decision that cyber threats are permanent and sophisticated, and the duty of law is to build systematic resilience across whole of the government and infrastructure.[1461]

On private sector engagement, the difference is equally austere. Japan has institutionalised public-private cooperation through sector-specific liaison councils that meet and discuss regularly, share intelligence, and coordinate responses. India recognise the significance of public-private partnership in policy documents but has not built the institutional machinery to make it work.

4.3 Defence Readiness

Japan has a doctrine of active cyber defence, legislative support for its Cyber Defence Unit, and a strategic alliance with the United States which provides operational and strategic deterrence. There is a structured and legally based flow of intelligence between civil and military cyber forces.

India has a Defence Cyber Agency which lacks a statutory basis and has an operational relationship with CERT-In and NCIIPC which is based on ad hoc arrangements. India has no publicly stated doctrine of active cyber defence and the legal basis of offensive and pre-emptive action in the defence of critical infrastructure is undefined.[1462] These are not minor issues – they are structural flaws which could have significant implications in a crisis situation.

4.4 What India should do?

The comparison with Japan suggests several concrete reforms. India needs a Critical Infrastructure Protection law. The IT Act cannot be stretched further to perform this role, and what India needs is a dedicated Critical Infrastructure Protection law that defines critical infrastructure sectors, sets out obligations on both public and private sector entities, and establishes the institutional machinery. This has

[1459] Subramanian (n 20).
[1460] NISC (n 24).
[1461] Vyas (n 6); Pillai (n 7).
[1462] Parliamentary Standing Committee on Information Technology (n 16)

been recommended several times by various expert committees[1463]. The only question one asks is how long India needs to wait before taking action, given the threat environment that India currently faces.

The NCIIPC needs to be reconstituted as an independent statutory body with clear regulatory authority. The current structure, which comes under the NTRO, does not give it enough independence or leverage to force action from private sector entities.[1464]

India needs a new National Cyber Security Policy, and the current one from 2013 simply cannot be considered relevant in today's threat environment. [1465]The new one needs to factor in defence considerations and establish lines of coordination between civilian cyber agencies and the Defence Cyber Agency.

The Defence Cyber Agency needs a proper legal mandate. Its role, its interface with civilian cyber agencies, and its role in case of a major cyber incident need to be defined in law rather than left to informal arrangement.

Finally, India's increasing cooperation through the Quad mechanism and bilateral relationships with both the United States and Japan needs to be taken forward into more formal frameworks for cyber intelligence sharing and joint infrastructure defence.[1466] Japan's use of alliances in deterrence demonstrates how much more value such partnerships could give India. India has no difficulty understanding what's at stake; what's now required is the legislative will to act upon what India already knows.

Key findings

The research yield five principle findings that collectively sustain the central hypothesis that follows:

First, the information technology act, 2000 that incorporate as an anger to India's Cyber of framework is proved to be structurally in adequate for protecting critical infrastructure against any resumed or contemporary future defense threats. This is an non-incidental, but an architectural inadequacy as this IT act was never designed for national security governance, but for commercial facilitation and Cyber Crime prosecution. The substitution of dedicated legislation is not possible as a regulatory supplement in this subject, demanding matters.

Second, many agencies such as CERT-In, NCIIPC, NCCC and defend Cyber agencies are operating while overlapping mandates with or without a unifying statutory framework, this leads to critical fragmentation thus India's institutional architecture is in a need for critical infrastructure protection. Absence of the DCA informal, legal mandate is particularly alarming as it creates hazardous ambiguities that leads to danger during active cyber incidents.

Third, India has not addressed the defense specific dimensions of cyber governance though it's supreme court has developed many progressive jurisprudence protecting Digital rights with the help of Puttaswamy, Shreya Singhal, and Anuradha Bhasin. Privacy rights and national securities surveillance, having some unresolved tension, leads to imperative creating legal uncertainty that then determines effective critical infrastructure protection.

Fourth, Japan's Basic Act on Cybersecurity demonstrably outperforms India's framework across every dimension examined whether it's legislative, institutional integration, proactive security, and public-private coordination and defence integration.

Fifth, CERT-In directions of 2022, welcomes incident reporting but separately cannot serve as a substitute for primary legislation. Mare regulatory instrument cannot supply the definitional precision, statutory authority, or institutional architecture where comprehensive critical infrastructure protection regime require.

[1463] Parliamentary Standing Committee on Information Technology (n 16); Observer Research Foundation (n 12).
[1464] National Critical Information Infrastructure Protection Centre (n 12).
[1465] National Cyber Security Policy 2013 (n 19).
[1466] International Telecommunication Union, Global Cybersecurity Index 2020 (ITU, Geneva, 2021); Carnegie Endowment for International Peace, 'Timeline of Cyber Incidents Involving Financial Institutions' (Carnegie Endowment, 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Conclusion

This paper has undertaken a meticulous comparative analysis of India's and Japan's Cyber Law frameworks. The central argument is that India's IT Act based framework is structurally deficient and that of Japan offers actionable lessons for reforms and has been sustained throughout.

The necessity of this conclusion is not merely scholastic. India is a high priority target for hostile cyber operations and also can be seen through major incidents like territorial disputes with China, Growing Indo-Pacific prominence, and its hasting digital expansion collectively magnify both the likelihood and outcome of sophisticated attacks on critical systems. The 2020 intrusion of The Kudankulam Nuclear Plant, The AIIMS Delhi ransomware attack of 2022, and other reported intrusions are not isolated incidents – they represent a sustained, strategically motivated campaign against India's most sensitive Infrastructure.

The Indian structure and framework which is fragmented and commercially oriented legal architecture is not only merely insufficient but dangerous. The absence of a dedicated Critical Infrastructure Protection statute, the DCA's undefined legal mandate, the institutional coordination gaps between civilian and military cyber agencies, and the obsolescence of the 2013 National Cyber Security Policy together constitute a structural vulnerability that adversaries are actively exploiting.

The comparison to Japan is not to discourage India rather it is to instruct and inspire India. Japan's superior framework is not a result of overnight struggles or is not an overnight transformation. It has taken over a decade with continuous legislative reforms and institutional redesign. India possesses the institutional capacity, technical expertise, and strategic motivation to undertake an equivalent reform process. What has been absent, thus far, is the requisite political will and legislative ambition.

This research concludes with both a perfect solution rather diagnosis and a prescription. Cyber Law framework of India needs fundamental reforms, grounded in a coherent strategic philosophy that combines proactive critical infrastructure protection with national defence policy.

Recommendations

1. **Legislative Reforms**
   On the priority bases there must be enactment of Critical Infrastructure Protection Act.
   Japan's sectoral approach must be considered while drafting that statue as Japan's statue precisely designate to critical sectors like power, water, telecommunications, finance, healthcare, transportation, nuclear and the defence. It should establish clear frameworks for system designation, incident reporting, and regulatory enforcement.
   The IT Act Comprehensively amended according to the current scenarios and conditions. Core definition should be updated, vagueness should be explained and artificial intelligence should be included. Section 70 must be expanded beyond unauthorized access to cover the full threat spectrum for instance disruption, denial of service, data integrity attacks, supply chain compromise and pre-installed malware.
   In Addition, a dedicated legal framework for cyber operations should be enacted, proper task force must be appointed to tackle defence oriented cyber activities. This frameworks must be defined as DCA's authority, which keep eyes on all type of activities of cyberspace particularly related to defence.
2. **Institutional Reforms**
   A national cyber security authority NCSA should be established by India as a unified statutory body that consolidate the functioning of CERT – in, NCIIPC and that of NCCC. The NCSCA mirroring

Japan's NISE is positioned under the Prime Minister's office should be holding explicit authority to collect intelligence threat issues, binding security, that give directions to critical infrastructure operations, and have coordination with the national response to major cyber incidents.

A statutory mandate must be received by the different Cyber agency through a dedicated legislation, which is in a clear relationship to the NCSA defined through protocols that government intelligence sharing, joint incident response and active defense authorities. A specific command authority should be placed by the legal framework across heightened tension, FaceTime during the active conflict scenarios, thus eliminating the current gaps that are currently pleaded in a coordinated response.

Each designated critical sector should have a sector specific public/private liaison council that is modeled upon Japan's established partnership. Meeting of the councils should be held regularly that then share classified threat intelligence enable private operators to contribute meaningfully, coordinate security standards to regulate policy. A mandatory participation should be must for the designated critical infrastructure operators, and also be supported by legal protections as it incentivise candidate vulnerability disclosure.