Improving the Domestic Framework for Deterring State-Sponsored Cybercrime

Abstract

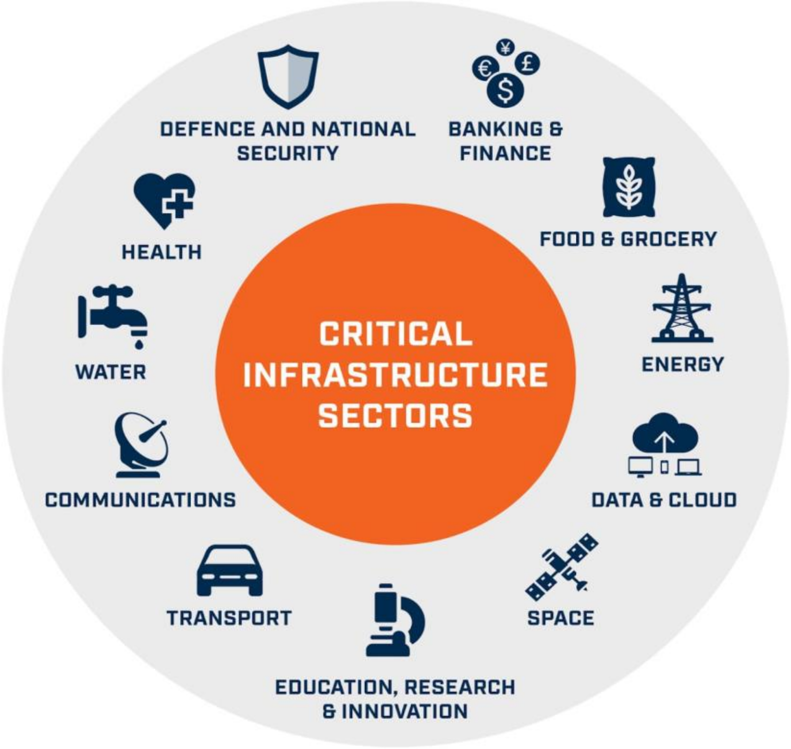
This paper analyzes the domestic legal framework applicable to state-sponsored cybercrime. The paper describes several instances where state sovereigns perpetrated cybercrimes in India. It then outlines the legal framework that the Indian government utilizes to hold accountable those who perpetrate such crimes. This Article argues that the current legal framework does not have a deterrence effect on sovereign states engaged in such activity and that prosecutors who seek to apply the current framework against state sovereigns or who misattribute the source of such attacks could negatively impact Indian foreign policy. To remedy these defects, this paper asserts that We, a nation in its 76th year of independence, need stronger laws against such cybercrimes and stronger compliance for all healthcare organizations. This also proves to be a crucial learning point for the rest of the national and state-level organizations to have better compliance and a strong cyber defense team.

I. INTRODUCTION

Ancient Indian texts like Athashastra and Nitisastra shows that since the first tribes evolved into sovereign states and began competing with one another for power and influence, they have sought to obtain advantage over the others through the gathering and use of confidential and information and the forcible destruction of a competitor and its resources.(1) Traditional diplomacy, spying, monitoring of foreign news outlets, military force, and other similar tools have long been deployed to allow sovereigns to gain and utilize such information and/or to obtain advantage over a competitor.

Since the advent of the information age, however, the nature of warfare has evolved dramatically. While traditional military confrontations continue, a new and more insidious form of conflict has emerged—**cyber warfare**. Cyberspace has emerged as a fifth potential theatre of war along with land, sea, air and space. Unlike conventional wars, where battles are fought on defined battlefields, cyber warfare occurs in the shadows, targeting critical national infrastructure, economic stability, and national security.

According to a report by the **Center for Strategic and International Studies** (**CSIS**), state-sponsored cyberattacks have increased by 60% over the last six years, with China, Russia, Iran, and North Korea among the top perpetrators. (2) India, as a rising global power with a burgeoning digital economy, finds itself increasingly in the crosshairs of state-sponsored cyber attacks. According to Singapore-based cybersecurity firm **Cyfirma** report in 2023, State-sponsored cyberattacks against India have increased by 278% in three years, almost 72% of which were state-sponsored. (3)


DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
HEALTH
FOOD & GROCERY
WATER
CRITICAL INFRASTRUCTURE SECTORS
ENERGY
COMMUNICATIONS
DATA & CLOUD
TRANSPORT
SPACE
EDUCATION, RESEARCH & INNOVATION

India's critical infrastructure has been targeted (Fig. 1) (4) In India, Cyfirma found that services companies were at the receiving end of 14.3% of cyberattacks between March 2021 and September 2023. This was followed by manufacturing at 11.6%, and healthcare and education at around 10% each. Retail, including online platforms, saw 9.8% of attacks while government agencies saw 9.6%. Banking and financial services institutions, automobiles, and airlines saw 9.5%, 8.3%, and 6.1% of attacks.

Fig. 1

According to the **Cloudsek** Threat Landscape Report, India was the second most targeted country for cyber-attacks in 2024 after USA. (5) These datasets highlight that the country's rapid digitisation journey may have left gaps in cyber hygiene.

This paper therefore analyses the domestic and legal framework addressing state sponsored cyber attacks in India, highlight its insufficiency and makes some policy recommendations.

II. DESCRIPTION OF SOVEREIGN INVOLVEMENT IN CYBERCRIME

A. Cyber Attack on Kudankulam Nuclear Power Plant and ISRO, 2019

The Nuclear Power Corporation of India Ltd. (NPCIL) confirmed on Oct. 30 2019 a cyberattack against the Kudankulam Nuclear Power Plant in Tamil Nadu, India's biggest nuclear power plant. An Indian private cybersecurity researcher had tweeted about the breach three days earlier, prompting Indian authorities to initially deny that it had occurred before admitting that the intrusion had been discovered in early September and that efforts were underway to respond to it.

According to last Monday's *Washington Post*, Kudankulam is India's biggest nuclear power plant, "equipped with two Russian-designed and supplied VVER pressurized water reactors with a capacity of 1,000 megawatts each. Both reactor units feed India's southern power grid. The plant is adding four more reactor units of the same capacity, making the Kudankulam Nuclear Power Plant one of the largest collaborations between India and Russia."

While reactor operations at Kudankulam were reportedly unaffected, this incident served as yet another wake-up call that the nuclear power

A Russian cyber security company, Kaspersky Labs, had said on September 23 that "banks and research centres in India" were targeted by *Dtrack* "in the beginning of September 2019". Dtrack is usually used for reconnaissance purposes and as a dropper for other malware payloads. Previous Dtrack samples have been usually spotted in politically-motivated cyber espionage operations and in attacks on banks. It is considered as a 'new type' of malware, which was deliberately created for data theft and spying.[5] A custom version of Dtrack, named AMTDtrack also being discovered last month Kaspersky's detailed analysis indicated that it had similarities to another related virus called 'ATM DTrack'. This was used to steal financial information from bank ATMs and has been found in many financial institutions and research centers. In October 2016, a major breach was detected at an Indian private bank's ATM network that quickly spread through the entire banking system. In a few months the government had to recall an estimated 2.9 to 3.2 million credit and debit cards that had been compromised by the ATM DTrack virus.[6]

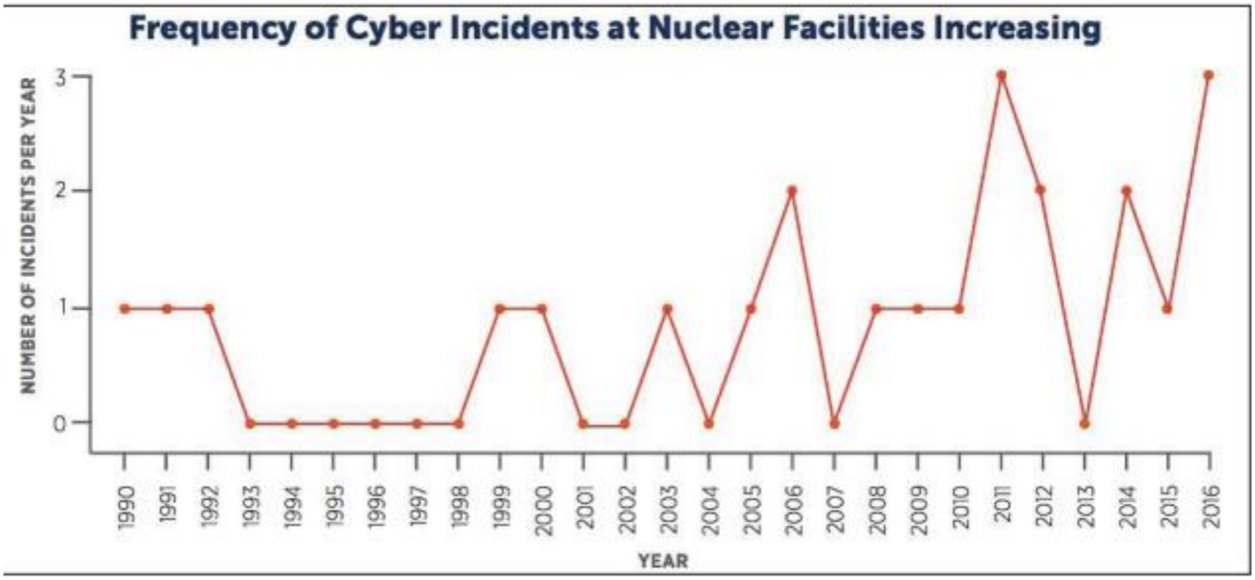


Fig. 2

B. Chinese Cyber Exploitation in India's Power Grid, 2020

In June 2020, Chinese and Indian troops clashed in a surprise border battle in the remote Galwan Valley, which marked a significant deterioration in Sino-Indian relations.

Four months later and more than 1,500 miles away in Mumbai, India, trains shut down and the stock market closed as the power went out in a city of 20 million people. Hospitals had to switch to emergency generators to keep ventilators running amid a coronavirus outbreak that was among India's worst.

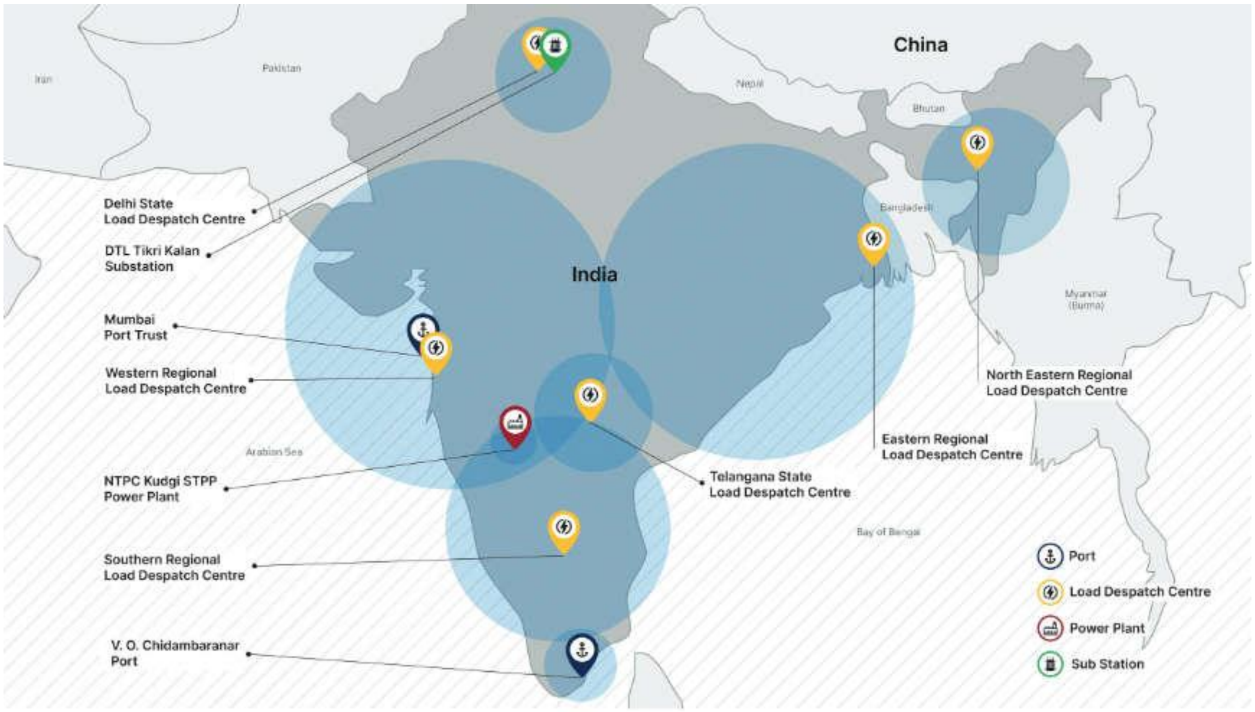
Now, a new study by **'Recorded Future'**, a U.S. based private intelligence firm, lends weight to the idea that these two events may well have been connected, as part of a broad Chinese cyber campaign against India's power grid, timed to send a message from Beijing about what might happen if India pushed its border claims too vigorously.

On Feb. 28, 2021 **The New York Times (NYT),** based on an analysis by '**Recorded Future'**, reported that a Chinese entity penetrated into India's power grid at multiple load dispatch points. Chinese malware intruded into the control systems that manage electric supply across India, along with a high-voltage transmission substation and a coal-fired power plant.

Stuart Solomon, Recorded Future's chief operating officer, said that the Chinese state-sponsored group, which the firm named **Red Echo**, "has been seen to systematically utilize advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure."[1]

Within India's power sector, RedEcho conducted suspected network intrusions targeting at least four out of the country's five Regional Load Despatch Centres (RLDCs), alongside two State Load Despatch Centres (SLDCs). RLDCs and SLDCs are responsible for ensuring real time integrated operation of India's power grid through balancing electricity supply and demand to maintain a stable grid frequency.[2]

The hacking group, RedEcho, has used a kind of malicious software called **ShadowPad**, which was previously associated with China's People's Liberation Army (PLA) and the Chinese Ministry of State Security (MSS), according to Recorded Future.


China
Iran
Pakistan
Nepal
Bhutan
Bangladesh
India
Myanmar (Burma)
Delhi State Load Despatch Centre
DTL Tikri Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
North Eastern Regional Load Despatch Centre
Eastern Regional Load Despatch Centre
Arabian Sea
NTPC Kudgi STPP Power Plant
Telangana State Load Despatch Centre
Bay of Bengal
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port
Port
Load Despatch Centre
Power Plant
Sub Station

Suspected Indian power sector victims of RedEcho targeted intrusions Recorded Future, Google Maps
https://www.businessinsider.in/tech/news/chinese-cybercriminals-are-targeting-the-indian-power-sectoraccording-to-a-report/articleshow/81274093.cms

China's Capabilities

China is ranked second in the National Cyber Power Index, behind only the U.S., while India is ranked 26 of the 30 countries analyzed [3]. China is an acknowledged master in cyber espionage activities. In addition to traditional state espionage, Chinese hackers are pilfering intellectual property from every major Fortune 500 company. If China can break through the reasonably good cyber network defenses of these organizations and Pentagon, it can be assumed that Chinese malware is present in most of India's critical information infrastructures. Until recent years, China’s focus had been on information theft. But Beijing has been increasingly active in placing code into infrastructure systems, knowing that when it is discovered, the fear of an attack can be as powerful a tool as an attack and can be seen as a deterrent.

But did it work?

The official response from the Government of India in New Delhi was typically bureaucratic. The Ministry of Power on 01 March, 2021 said, “Observations from all RLDCs & NLDC shows that there is no communication and data transfer taking place to the IPs mentioned. There is no impact on any of the functionalities carried out by Power System Operation Corporation (POSOCO) due to the referred threat. No data breach/ data loss has been detected due to these incidents.”

For India, the attacks were a wake-up call. Although there were no major power outages directly linked to RedEcho’s campaign, the fact that key elements of the power grid had been infiltrated was enough to prompt immediate action.

For India, the attacks were a wake-up call. Although there were no major power outages directly linked to RedEcho’s campaign, the fact that key elements of the power grid had been infiltrated was enough to prompt immediate action.

C. Ransom ware cyber-attack on AIIMS server, 2022

The All India Institute of Medical Sciences (AIIMS), a top public medical research facility and hospital with headquarters in New Delhi, India, announced a sophisticated cyber-incident on its servers on 23 November 2022. Several patient care services were rendered unavailable as a result of the incident, including registration, admission, billing and discharge. Several news sources claim that this cyber event, which affected the e-services of the AIIMS (New Delhi) starting at 7:00 a.m. on 23 November 2022, was of the ransomware variety. The testing runs of the e-hospital server were successful, and the majority of the lost data had been recovered during the previous few days, according to AIIMS authorities’ confirmation on 6 December 2022.

As the incident quoted in the Indian Express Newspaper dated 8 June 2022, Chinese hackers launched a ransomware attack on the servers of the AIIMS, the premier medical institute in Delhi. The hack against AIIMS, Delhi, occurred on 23 November and the Delhi Police then filed a complaint of extortion and cyber terrorism on 25 November. It further stated that five of the 100 physical servers had been successfully breached by hackers. Hackers were able to breach 5 physical servers from a pool of 100, which included 40 physical and 60 virtual servers. Because of this ransomware attack that occurred last month, the confidential medical information of millions of patients at AIIMS Delhi was in danger. After this event, the case was handled by a special unit of the Delhi Police in December. According to the investigations, two emails’ IP addresses that were discovered in the headers of files that the hackers had encrypted were from Hong Kong and the Henan province of China. The senders, according to sources, utilised the email service provider ProtonMail. The top cybersecurity organisation in the nation, the Indian Computer Emergency Response Team (CERT-In), discovered that the hackers used two ProtonMail web addresses, ‘dog2398’ and ‘mouse63209’. According to the sources, CERT-In and Interpol were used to send the encoded web files to these two ProtonMail IDs during the investigation. After further analysis, they discovered that ‘dog2398’ and ‘mouse63209’ were created in Hong Kong during the initial first week of November. They also discovered that Henan Province in China sent another encrypted file. Additionally, sources claimed that three ransomware infections—Wammacry, Mimikatz and Trojan—had been found on the targeted servers.

CERT-In, Delhi Cybercrime Special Cell, Indian Cybercrime Coordination Centre, Intelligence Bureau, CBI and National Investigation Agency are all looking into the ransomware incident that may have exposed the records of nearly four crore patients (Liu et al., 2021). The event was examined by the CERT. According to an early investigation, servers were penetrated by unknown threat actors in the AIIMS information technology network as a result of faulty network segmentation, which led to operational interruptions owing to the non-functionality of essential applications, the author added. The complete data for online hospital services has been restored on new servers after being recovered from a backup server that was unaffected. After two weeks following the cyberattack, the majority of the capabilities of the online hospital application, including new patient registration, appointments, new admissions, discharge work, etc., have been restored.

Critical data at risk? NIC e-Hospital at AIIMS is using 24 servers for various hospital modules and four of these servers were infected with ransomware – primary and secondary database servers of e-Hospital, primary application and primary database servers of laboratory information system (LIS). The medical records and other critical PII information of many renowned people of the country and the world are on the server of AIIMS New Delhi. The data breach has reportedly compromised the data of nearly 3–4 crore patients, including sensitive data and medical records of the President, Prime Minister, former Prime Minister, and many other VIPs ministers. The exploited databases contain Personally Identifiable Information (PII) of patients and healthcare workers, and administrative records kept on blood donors, ambulances, vaccination, caregivers and employee login credentials. It highly likely that risks are quite high that the ransomware attack has exposed personal data and medical records of thousands of patients who have been treated at the institute.

III. DOMESTIC LEGAL FRAMEWORK APPLICABLE TO STATE-SPONSORED CYBERCRIME

India's domestic legal framework for addressing state-sponsored cyber attacks is still evolving, but several laws and regulations can be applied. These laws are largely focused on cybercrimes, national security, and foreign relations, and while they don't directly address state-sponsored attacks, they provide a foundation for responding to such incidents. Below is an analysis of the legal provisions that can be applied:

1. Information Technology Act, 2000 (IT Act)

The Information Technology Act, 2000, serves as the primary legislation governing cybercrimes and electronic commerce in India. It includes provisions that can be applied in cases of cyber attacks, though the Act does not explicitly address state-sponsored cyber attacks.

Key Sections:

- **Section 66 (Cyber terrorism):** This section criminalizes acts of cyber terrorism, which are defined as any act using computer resources that leads to or threatens national security, integrity, sovereignty, or economic stability. A state-sponsored cyber attack targeting India's critical infrastructure could fall under this provision.
- **Section 43 (Penalty for damage to computer system, etc.):** This section imposes penalties for unauthorized access to computer systems, data theft, and damage to computer networks. State-sponsored cyber attacks that involve unauthorized access or damage to Indian systems could lead to penalties under this provision.
- **Section 70 (Protected System):** This section designates critical government infrastructure as "protected systems," which are subject to special security regulations. A state-sponsored cyber attack on such systems would be a violation of this provision, and the attackers would be liable for severe penalties.
- **Section 66F (Cyber Terrorism):** This section specifically targets cyber terrorism, including state-sponsored activities intended to cause harm to the nation's integrity or security. It criminalizes activities that disrupt or destroy critical infrastructure and communication systems through cyber means.It was added through

Analysis:

The IT Act offers a broad framework for dealing with cyber crimes, including those perpetrated by state actors. However, the Act does not specifically address the nuances of state-sponsored attacks, which may require international collaboration and more specific provisions for attribution, proof, and redressal.

2. Bhartiya Nyaya Sanhita (BNS)

The BNS contains several provisions that can be used to prosecute individuals or entities involved in cyber-related crimes, including those related to state-sponsored attacks. Although the BNS was not specifically designed for cybercrimes, several sections can be extended to cover cyber-related offenses.

Key Sections:

- **Section 147 (Waging or attempting to wage war against the Government of India):** If a state-sponsored cyber attack is deemed as an act of war or an attempt to destabilize the nation, it could fall under this section. The section imposes severe penalties, including life imprisonment or death, in the case of waging war against India.
- **Section 152 (Conspiracy to commit offense punishable under section 147):** This section criminalizes conspiring to wage war against India. If a state-sponsored cyber attack is part of a conspiracy to disrupt India’s sovereignty, it may be addressed under this provision.

Analysis:

The IPC provides general criminal liability for acts that can be connected to cyber terrorism, espionage, or activities undermining national security. However, issues like attribution, digital evidence, and international cooperation remain challenging when dealing with state-sponsored cyber incidents.

3. The National Security Act (NSA), 1980

The NSA is used for preventive detention in cases of threats to national security. It empowers the Indian government to detain individuals without trial if they are deemed to be a threat to the security of the nation.

Analysis:

In cases where state-sponsored cyber attacks threaten national security or public order, the NSA can be used to detain individuals linked to these activities. However, its applicability to non-human actors or cyber infrastructures may be limited.

4. The Unlawful Activities (Prevention) Act (UAPA), 1967

The UAPA addresses terrorism and unlawful activities in India, particularly actions that threaten the sovereignty, integrity, and security of the country. It includes provisions for the prosecution of individuals or groups associated with terrorist activities.

Key Sections:

- **Section 3 (Declaration of unlawful associations):** If a state-sponsored cyber attack is perpetrated by a group that is designated as a terrorist organization, this section can be used to ban the group and seize its assets.
- **Section 16 (Punishment for Terrorist Acts):** This section imposes penalties for any act of terrorism, including cyber terrorism, which is defined as an act intended to cause death or disruption on a large scale.

Analysis:

The UAPA could be employed to prosecute state-sponsored cyber attackers if their activities can be classified as terrorism or related to terrorist organizations. The challenge, however, would lie in proving the involvement of a state actor, which often requires robust international cooperation and intelligence-sharing.

5. Cybersecurity Laws & Regulations

India has also formulated specific regulations for cybersecurity, particularly under the Ministry of Electronics and Information Technology (MeitY). These regulations aim to protect critical national infrastructure and develop frameworks to secure India's cyberspace.

- **National Cyber Security Policy (2013):** This policy aims to create a secure and resilient cyberspace for India. It includes directives for responding to cyber incidents, managing vulnerabilities, and developing national cybersecurity capabilities.
- **Indian Computer Emergency Response Team (CERT-In):** CERT-In is responsible for coordinating responses to cyber attacks and incidents, including those that may be state-sponsored. It works closely with international organizations to mitigate cyber threats.

Analysis:

These cybersecurity initiatives form a crucial part of the national strategy to defend against cyber threats, including state-sponsored attacks. However, they mainly focus on incident response and mitigation rather than legal redressal or punitive measures.

Digital Personal Data protection act 2023

I4C

Challenges in Addressing State-Sponsored Cyber Attacks:

1. **Attribution**: One of the most significant challenges in handling state-sponsored cyber attacks is attribution. It can be difficult to definitively prove that a nation-state is behind a cyber attack due to the anonymous and borderless nature of cyberspace.
2. **International Law**: Cyber attacks, particularly state-sponsored ones, may require international cooperation and adherence to frameworks like the UN's norms on responsible state behavior in cyberspace. However, India's legal system does not yet fully integrate such international norms, and this creates gaps in enforcement.
3. **Sovereignty vs. Diplomacy**: State-sponsored cyber attacks often involve foreign governments, which complicates the legal response. The response may involve diplomatic measures or sanctions rather than domestic legal action.

The Indian Computer Emergency Response Team (CERT-In)	- Address the cyber threat in the country. - Played a crucial role in reducing the cyber threat case in India

Cyber Surakshit Bharat	The aim is to secure India’s cyber security domain Launched by the Ministry of Electronics and Information Technology in partnership with the National Electronic Governance Division (NeGD)
National Critical Information Infrastructure Protection Center (NCIIPC)	-Providing cyber security, especially in the defence sector, public health sector and economic sector.
Appointment of Chief Information Security Officers	-App, infrastructure, compliance safety and security
Personal Data Protection Bill	Data localization Cyber safety of people in India Making social media companies accountable in the country
Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)	Initiative taken under the Digital India drive -Protect the internet services and the cyber domain of the country
National Cyber Security Policy	-Working on the policies and laws related to cybersecurity

V. SUGGESTED LEGISLATIVE OR OTHER PROPOSAL

Indian Cybersecurity Act

In 2008, the Information Technology Act was amended to incorporate provisions concerning cyberterrorism. However, from 2008 to 2021, exploitation of cyberspace by terrorists has undergone a systematic transformation. The conglomeration of time and evolution of destructive technologies has made cyberterrorism intricately complex and devastatingly lethal to deal with. Cyberterrorists use innovative methods to exploit cyberspace for youth radicalisation and to propel cyberattacks causing massive destruction. The evolution of destructive technological order aiding cyberterrorism warrants a new modernised legal order, with empowered law enforcement agencies, to protect Indian cyberspace against possible cyberthreats and preserve its cyber sovereign interest.

India must consider enacting a new cybersecurity legislation,133 Indian Cybersecurity Act, dedicated to deal with present-day cybersecurity challenges and regulate all aspects of cybersecurity, including cyberterrorism. Further, in view of the future consolidation of cyberterror attacks, a new legislation would additionally provide more effective, deterrent and stringent legal framework against cyberterrorism.

Multiplicity of Organisations

Multiple government organisations handle cybersecurity operations of India,134 resulting in overlapping jurisdictions and operations among organisations. Some reformatory steps—like creating the National Cyber Security Coordinator under National Security Council Secretariat (NSCS) and bringing central agencies under its control—have been adopted. However, it is important to provide the exigent task of cybersecurity exclusively to three central agencies, namely, CERT-In, NCIIPC and Defence Cyber Agency, with well-delineated and defined jurisdictional limits of operations and responsibilities. Instead of creating a parallel hierarchical structure which results in unwarranted overlapping of work, the jurisdictional limits of operations must be detailed through legislation to the extent possible. Further, there must be a regular review of the jurisdictions of organisations to keep India’s cybersecurity mechanism updated as per the continuously evolving cyberspace. Since what today is not a CI might become intrinsically critical for preserving national security tomorrow, the National Cyber Security Coordinator must proactively coordinate the activities of the cybersecurity agencies to intensify capabilities of India to counter cyberterrorism.

International Cybersecurity Cooperation: Harmonisation of Domestic Laws

The transnational character of cyberspace warrants a global cooperative effort to counter cyberterrorism.170 To thwart the menace of potentially ruinous cyberterrorism, countries must work towards developing a universally acceptable and effective strategy of defence and countermeasures for cyberterrorism. Many countries have progressively effectuated their cyber defences and adopted deterrence strategies to supplement their cyber defences. However, it becomes difficult to counter the threats of cyberterrorism merely on strategic national policies since cyberspace is globally homogenised and attacks may emerge overseas. International cooperation between states, therefore, is an effective cornerstone to develop an effective combat mechanism and legal framework to counteract cyberterrorism. Inadequate international regulations and uncoordinated legal mechanisms of states on cyberterrorism act as the biggest deterrent in devising an effective global strategy against cyberterrorism.

A dedicated cyber security ministry

Like in australia