Some Important Facts

There are following kinds of cyber players who harm cybersecurity:

- Cyber Criminals
- Cyber Terrorists
- Cyber Espionage
- Cyber Hacktivist

Legal Landscape in India for Cybersecurity

Laws related to Cyber Security in India	Important Facts
Information and Technology Act, 2000	• Came into force in October 2000 • Also called Indian Cyber Act • Provide legal recognition to all e-transactions • To protect online privacy and curb online crimes
Information Technology Amendment Act 2008 (ITAA)	The amendments in the IT Act mentioned: • 'Data Privacy' • Information Security • Definition of Cyber Cafe • Digital Signature • Recognizing the role of CERT-In • To authorize the inspector to investigate cyber offenses against DSP who was given the charge earlier
National Cyber Security Strategy 2020	Indian Government has come up with the National Cyber Security Strategy 2020 entailing the provisions to secure cyberspace in India.
Cyber Surakshit Bharat Initiative	MeitY in collaboration with National e-Governance Division (NeGD) came up with this initiative in 2018 to build a cyber-resilient IT set up

The Indian Computer Emergency Response Team (CERT-In) serves as the national agency for performing various functions in the area of cyber security in the country as per the provisions of section 70B of the Information Technology Act, 2000.

CERT-In (The Indian Computer Emergency Response Team)

CERT-In has been operational since January 2004.

- CERT-In comes under the Ministry of Electronics and Information Technology (MeitY).
- It regularly issues advisories to organisations and users to enable them to protect their data/information and ICT (Information and Communications Technology) infrastructure.
- In order to coordinate response activities as well as emergency measures with respect to cyber security incidents, CERT-In calls for information from service providers, intermediaries, data centres and body corporates.
- It acts as a central point for reporting incidents and provides 24 × 7 security service.
- It continuously analyses cyber threats and handles cyber incidents tracked and reported to it. It increases the Indian Internet domain's security defences.
- CERT-In is leading the implementation of CCMP across Central Government Ministries/Departments/states and critical organisations operating in Indian cyberspace.
    - The Cyber Crisis Management Plan (CCMP) for Countering Cyber Attacks and Cyber Terrorism is a framework document for dealing with cyber-related incidents.

CERT-In Functions

In the IT Amendment Act 2008, CERT-In has been designated to perform the following functions in the area of cyber security –

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

Cyber Attacks - Levels of concern

Threat Level	Condition
Level 1 Guarded Scope: Individual Organisation	Large scale attacks on the IT infrastructure of an organisation
Level 2 Elevated Scope: Multiple Organisations	Simultaneous large scale attacks onto IT infrastructure of multiple organisations
Level 3 Heightened Scope: State/Multiple States	Cyber attacks on infrastructure of critical sector and Government across a state or multiple states
Level 4 Serious Scope: Entire Nation	Cyber attacks on infrastructure of critical sector and Government across the nation.

CERT-In Issued Directions in April 2022

In April 2022, CERT-In has issued directions relating to information security practices, procedures, prevention, response and reporting of cyber incidents for a safe and trusted internet.

- In order to facilitate incident response measures, CERT-In issued directions relating to information security practices, procedures, prevention, response and reporting of cyber incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000.
- The directions cover aspects relating to –
    - synchronisation of ICT system clocks
    - mandatory reporting of cyber incidents to CERT-In (within six hours)
    - maintenance of logs of ICT systems (for 180 days)
    - subscriber/customer registrations details by Data centres, Virtual Private Server (VPS) providers, VPN Service providers, Cloud service providers
    - KYC norms and practices by virtual asset service providers, virtual asset exchange providers and custodian wallet providers.

These directions shall enhance the overall cyber security posture and ensure safe & trusted Internet in the country.

The National Cyber Security Policy

The National Cyber Security Policy, which was first drafted in the wake of reports that the US government was spying on India and there were no technical or legal safeguards against it.

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY) It aims at protecting the public and private infrastructure from cyber attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

Need for a cybersecurity policy

- Before 2013, India did not have a cybersecurity policy. The need for it was felt during the NSA spying issue that surfaced in 2013.
- Information empowers people and there is a need to create a distinction between information that can run freely between systems and those that need to be secured. This could be personal information, banking and financial details, security information which when passed onto the wrong hands can put the country's safety in jeopardy.
- This Policy has been drafted in consultation with all the stakeholders.
- In order to digitise the economy and promote more digital transactions, the government must be able to generate trust in people in the Information and Communications Technology systems that govern financial transactions.
- A strong integrated and coherent policy on cybersecurity is also needed to curb the menace of cyber terrorism.

National Cyber Security Policy Vision

To build secure and resilient cyberspace for citizens, businesses and Government.

National Cyber Security Policy Mission

- To protect information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

National Cyber Security Policy Objectives

- Encouraging the adoption of IT in all sectors of the economy by creating adequate trust in IT systems by the creation of a secure cyber ecosystem.
- Creating an assurance framework for the design of security policies and for the promotion and enabling actions for compliance with global security standards and best practices through conformity assessment.

- Bolstering the regulatory framework for ensuring a secure cyberspace ecosystem.
- Enhancing and developing national and sectoral level 24 x 7 mechanisms for obtaining strategic information concerning threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- Operating a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) to improve the protection and resilience of the country's critical infrastructure information.
- Developing suitable indigenous security technologies to address requirements in this field.
- Improving the visibility of the ICT (Information and Communication Technology) products/services' integrity by having testing and validation infrastructure.
- Creating a workforce of 500,000 professionals skilled in cybersecurity in the next 5 years.
- Providing businesses with fiscal benefits for adopting standard security practices and processes.
- Safeguarding of the privacy of citizen's data and reducing economic losses due to cybercrime or data theft.
- Enabling effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through legislative intervention.
- Developing a culture of cybersecurity and privacy.
- Developing effective public-private partnerships and collaborative engagements by means of technical and operational cooperation.
- Promoting global cooperation by encouraging shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Examples of Cyber Attacks

Cyber Attacks in India	Description of the Cyber Attacks
Coronavirus Pandemic Based Cyber Attack	Microsoft has reported that cyber crooks are using Covid-19 situation in 2020 to defraud people through phishing and ransomware in India and the world
Phishing	Union Bank of India heist in July 2016
Wannacry Ransomware	In May 2017, various computer networks in India were locked down by the ransom-seeking hackers.
Data Theft	In May 2017, the food tech company Zomato faced the theft of information of 17 million users.

Petya Ransomware	Container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected
Mirai Botnet	In September 2016, Mirai malware launched a DDoS attack on the website of a well-known security expert.