

Cybersecurity, Meaning, Types, Importance, Initiatives

July 10, 2026 • vajiramandravi.com



Cybersecurity refers to technologies, processes, and rules created to protect computer systems, servers, networks, programs, devices, and data from cyber-attacks. It aims to protect against the **unauthorised access** to data and **misuse** of technologies. India's growing reliance on digital technologies, increasing use of the internet, lack of awareness, and vulnerability of the Critical Information Infrastructure have made it a target of a wide range of cyber threats. According to a **CERT-In report**, over **3.94 lakh** cyber security incidents were reported in 2020 in India, an increase of **63%** from the previous year. These incidents included phishing attacks, website intrusions, malware attacks, and ransomware attacks.

Types of Cyber Threats

Based on the type of perpetrators and their motive, cyber threats can be arranged into four types.

- **Cybercrime:** These are **criminal activities** carried out through a computer network, wherein a computer/device/server might be the target or used in carrying out criminal activities.
 - The main motive of cyber criminals is **financial gain** or to cause disruption.
- **Cyber-Espionage:** The act of using a computer network to gain **unlawful access** to **confidential information** from other computers/servers is called cyber espionage. It is executed to extract classified

information from government organisations.

- Cyber-espionage is cyber-enabled illegal abstraction of data, intellectual properties (IPs), and trade secrets worth billions of dollars.
- In March 2021 cyber intelligence firm Cyfirma reported that the **Chinese hacking group APT 10**, also known as Stone Panda, had targeted the Bharat Biotech and the Serum Institute of India (SII), whose coronavirus shots were being used in the country's immunisation campaign.
- **Cyberwarfare:** Cyberwarfare refers to using cyberspace to carry out acts of warfare against other countries. It includes attacks like **distributed denial of services, defacing of websites**, and so on.
 - Now cyberspace is considered the **fifth dimension of warfare**, after land, ocean, air, and space. More than **140 countries** have developed or are in the process of developing their patenting and proficiency in cyberwarfare.
 - For example, NATO has designated cyberspace as an 'operational domain', like air, land, and sea. The US has a separate **Cyber Command**.
- **Cyberterrorism:** It involves an attack over a computer network to secure the political objectives of terrorists to cause fear among the masses and target the government/s.
 - Usually cyberterrorism aims to invade cybernetworks responsible for the maintenance of national security and destroy information of strategic importance.
 - Methods used are usually the destruction of cybernetwork, denial of service attacks, and data exfiltration.
 - It is capable of causing loss of life, creating international economic chaos, and affecting environmental casualties by hacking into various critical infrastructures.

Methods Used for Cyberattacks

The following are some common methods used to threaten the cybersecurity of a nation.

- **Malware:** It is malicious software that a cybercriminal/hacker creates to disrupt/damage computer/s or derive financial benefits. It is often spread by way of an unsolicited email attachment or download link. The types of malware are as follows:
 - **Virus:** It is a self-replicating program that attaches to a clean file and spreads in a computer system infecting other files.
 - **Trojans:** It disguises as legitimate software. Users are tricked into uploading Trojans onto their devices where they cause damage or collect data.
 - For example, **Emotet** was a sophisticated trojan that was used to steal data and load other malware.
 - **Spyware:** It is a program that secretly records what a user does, and then this information is misused.
 - **Ransomware:** It locks down a user's files/data, the user can not access them unless a ransom is paid. Example - **Wannacry** and **Petya**.
 - **Adware:** It is advertising software that can be used to spread malware.
 - **Botnets:** It is a network of infected computers that is used by cybercriminals to perform tasks online.
- **SQL injection:** It is a type of cyber-attack used to steal data from a database.
 - Vulnerabilities in data-driven applications are exploited to insert malicious code into a database.

- **Phishing:** Phishing is when attackers send spam emails or text messages that contain links to malicious websites.
 - The websites may contain malware (for example, **Dridex malware**) which can sabotage systems and organisations.
- **Man-in-the-middle attack:** In this, a cybercriminal intercepts communication between two individuals in order to steal data.
 - **For example**, on an unsecured WiFi network, data that is being passed from the victim's device can be intercepted.
- **Denial-of-service attack:** It prevents a computer system from fulfilling legitimate requests by overwhelming the networks and servers with excessive traffic.
 - In **April 2023**, a coordinated DDoS cyberattack was launched in India against six major airports and healthcare institutions by a hacker group named **Anonymous Sudan**.
- **Romance scams:** Cybercriminals use dating sites, chat rooms, and apps, duping victims into compromising personal data.
- **Cyber Threat evolution:** Types of cyber threats have grown sophisticated with time as shown in the diagram below.

Need for Cyber Security in India

Amongst contemporary security vulnerabilities, **cyber threats** to the economy, security, public service delivery, critical infrastructure, etc. have emerged as critical to India. Cyber threat is a huge challenge that is capable of disturbing and destroying the economic and social order. The following are the major reasons why cyber security is needed:

- **Nature of Cyberthreat:** These are hard to detect and **difficult to investigate** because of their **anonymity**. Besides being **inexpensive** and **easy** to commit, they are hard to prove with certitude.
- **Evolving nature:** Cyber criminals are embracing increasingly **innovative** and highly **inventive** techniques.
 - **Ransomware as a Service:** Recent instances of **Ransomware attacks where RaaS** was used.
 - **Cybercrime-as-a-service:** This new model emerged in 2023. E.g. **LockBit, Akira, Luna Moth**
 - **Misuse of AI:** In 2023 **WormGPT**, a blackhat version of ChatGPT was found to be used to generate malicious content, including phishing emails, malware code, fake news, and social media posts.
- **High level of Vulnerability:** The Critical Information Infrastructure (CII) and other state computer resources are not fully protected and have become easy targets.
 - **Example:** The **AIIMS ransomware** attack of **2022** affected a large number of patients' data.
- **Used by terror organisations:** Cyber terrorists can use the same techniques as traditional cyberattacks, such as **DDoS** attacks, **malware**, **social engineering**, and **phishing**.
- **The impetus to digitisation:** The government has been promoting internet-based services making them more vulnerable to cybercrimes.
 - Online payments via **BHIM UPI** are prone to fraud, surveillance, profiling, violation of privacy, etc.
- **Interface with Public Services:** Attacks in cyberspace may result in the disruption of critical public services like railways, defense systems, communication systems, banking, and others.

- The **2020 Mumbai power outage** was allegedly due to a **Chinese cyber-attack** carried out through malware.
- **Cyber warfare against India:** State-sponsored cyberattacks against India went up by **278%** between 2021 and 2023, with the service sector, including IT and BPO, facing the highest share of attacks, according to the **2023 India Threat Landscape Report** by **Cyfirma**.
- **Rising cybercrime in India:** As per the **NCRB report** the number of Cybercrime incidents in India was as follows:

Year	2020	2021	2022
Number of Cybercrime incidents	50035	52974	65893
Percentage rise over the previous year	11.8%	5.9%	24.2%

- **Major types of cybercrime in India:** During 2021, **37.6%** of the cases were reported under **Computer-related offenses** followed by **fraud** at **26.4%** and Publication/ transmission of obscene / **sexually explicit acts in electronic form** in **12.5%** of cases.

Initiatives Taken for Cyber Security

To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has adopted the following measures:

Legal Measures

- **Information Technology Act, 2000:** The Act deals with the protection of CII, declaration of a 'protected system', cyberterrorism, hacking, violation of privacy, fraud, and other cyber crimes.
- **Digital Personal Data Protection Act (DPDP), 2023:** The act aims to balance the rights of individuals with the need to process digital personal data for legal purposes. It applies to the processing of digital personal data within India, as well as the processing of personal data outside India if it is for offering goods or services in India. The act grants individuals rights such as:
 - The right to obtain information about processing
 - The right to seek correction and erasure of personal data
 - The right to nominate another person to exercise rights in the event of death or incapacity
- **National Digital Communications Policy, 2018:** The major focus areas of the policy are as follows:
 - To connect, propel, and secure India (**Secure digital sovereignty** of India)
 - **Universal broadband connectivity** at 50 Mbps to every citizen
 - Provide 1 Gbps internet connectivity to all Gram Panchayats
 - Ensure connectivity to all uncovered areas
 - Attract investments of USD 100 Billion in the Digital Communications Sector
- **National Cyber Security Policy, 2013:** It aims to concretise resilience against cyber threats in all sectors. A crisis management plan has been instituted.

Institutional Measures

- **National Cyber Security Coordinator (NCSC):** It coordinates with different agencies at the national level for cyber security matters.
- **National Critical Information Infrastructure Protection Centre:** Under Section 70A of the IT Act, it is designated as the National Nodal Agency for CII protection.
- **Defence Cyber Agency:** The union government has established it to deal with matters of cyberwarfare and cybersecurity.
- **Indian Computer Emergency Response Team (CERT-In):** Section 70B of the IT Act provides for the constitution of CERT-In to maintain India's cybersecurity and counter cybersecurity threats.
 - It issues alerts and advisories about the latest cyber threats as well as coordinated counter-measures.
- **Cyber Swachhta Kendra:** Botnet Cleaning and Malware Analysis Centre has been launched for the detection of malicious programs and provides free tools to remove them.
- **National Cyber Coordination Centre:** It was set up to generate necessary situational awareness of cyber security threats and enable timely information sharing for proactive, preventive, and protective actions by individual entities.
- **Indian Cyber Crime Coordination Centre(I4C):** The Ministry of Home Affairs has set up the **I4C** to deal with all types of cybercrime in the country, in a coordinated and comprehensive manner. It includes:
 - **National Cyber Forensic Laboratory:** It provides cyber forensic assistance to State/UT Police.
 - **National Cyber Crime Reporting Portal:** to report cyber crimes.
 - **Citizen Financial Cyber Fraud Reporting and Management System:** for immediate reporting of financial frauds and to stop siphoning off funds by fraudsters.
 - **Massive Open Online Courses (MOOC) platform:** namely the 'CyTrain' portal has been developed for the capacity building of public officials.

Other Measures

- **Chief Information Security Officers:** Guidelines have been issued for CISOs for securing applications/infrastructure and compliance in different organisations.
- **Cyber Auditing:** All the new government websites and applications are audited prior to their hosting and on a regular basis after hosting.
- **Cyber Crime Prevention for Women and Children (CCPWC) Scheme:** The government has released grants to States/UTs for setting up a Cyber Forensic cum Training Laboratory and organising capacity-building programs on cyber awareness and cyber crime investigation.

Suggested Measures to Enhance Cyber Security in India

According to the **World Economic Forum's Global Cybersecurity Outlook 2024**, there is a widening gap among organisations concerning cyber resilience. To make conditions bad, cyber-skills and talent shortages increase vulnerability to threats. The following are major measures that can be taken in India:

- **End-user protection:** It is an individual (the end-user) who accidentally uploads malware or another form of cyber threat. The following measures can be taken:
 - Implement firewall and threat detection software.
 - Install security patches and updates.

- Regularly update software.
- Scan files from unknown sources.
- **Cyber Insurance:** According to **IRDAI**, cyber insurance is an insurance policy designed to protect the policyholders from cybercrimes. It is a risk management and mitigation strategy that has a corollary benefit of improving the adoption of preventive measures. It can help move from cyber risk mitigation to cyber risk prevention.
- **Legislative Reforms:** India must consider enacting the **Indian Cybersecurity Act**, dedicated to dealing with present-day cybersecurity challenges such as cyberterrorism and spam, and empowering investigating agencies.
- **Administrative Reforms:**
 - **Multiplicity of Organisations:** Multiple government organisations handle cybersecurity in India, resulting in **overlapping jurisdictions** and confusion among organisations. The jurisdictional limits must be detailed through legislation to the extent possible.
 - **Clear jurisdictions:** There should be a regular review to keep cybersecurity updated as per the continuously evolving cyberspace.
 - The **National Cyber Security Coordinator** must proactively coordinate the activities of the cybersecurity agencies.
- **Awareness Programmes:** The government must consider launching a cyber literacy program.
- **Indian Cybersecurity Service:** As recommended by **IDSA**, the government should establish the Indian Cybersecurity Service as an all-India civil service.
- **Infrastructural Investments and Upgradation:** In addition to protecting IP, and trade secrets and preserving India's data sovereignty, it is imperative to secure financial transactions and communications taking place through cyber networks. The following measures can be taken:
 - **Sectoral CERTs:** These must be operationalised in more fields.
 - **Recovery capability:** the government must develop disaster recovery capabilities against cyber attacks.
 - **Cyberspace safety fund:** to meet all cybersecurity contingencies of India.
- **Strengthening capacity:**
 - **Cyber forensics:** It is the process of using electronic equipment to gather data as evidence for a crime. There is a lack of proper training, technology upgradation as well as devices with enforcement agencies.
 - **Increasing capacity of Police:** Police lack the capabilities to investigate cyber crimes and frauds occurring on a daily basis.
 - According to Delhi Police in 2023-24 almost **200 people** fell prey to cyber frauds every day and the number is rising.

Cybersecurity UPSC PYQs

Question 1. What are the different elements of cyber security? Keeping in view the challenges in cyber security examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (UPSC Mains 2022)

Question 2. Keeping in view India's internal security, analyze the impact of cross-border cyber attacks. Also, discuss defensive measures against these sophisticated attacks. **(UPSC Mains 2021)**

Question 3. Discuss different types of cybercrimes and measures required to be taken to fight the menace. **(UPSC Mains 2020)**

Question 4. What is the CyberDome Project? Explain how it can be useful in controlling internet crimes in India. **(UPSC Mains 2019)**

Source: <https://vajiramandravi.com/upsc-exam/cyber-security/>

© Vajiram & Ravi. For personal use only.