Cyberwarfare

Posted at: 20/05/2025

Cyberwarfare: A Rising Threat in the Digital Age

Why in the News?

Following the recent **terrorist attack on tourists in Pahalgam**, and the subsequent **Operation Sindoor**, India witnessed an alarming spike in cyber threats. Over **one million cybersecurity incidents** were reported within just ten days, highlighting the growing integration between traditional threats and cyber-based warfare.

What is Cyberwarfare?

Cyberwarfare refers to the use of **information technology tools and techniques by state or non-state actors** to engage in hostile activities in cyberspace. These can be aimed at **disrupting, sabotaging, stealing**, or **manipulating information** and digital infrastructure for military, political, or economic purposes.

Key Characteristics:

- **Purpose:** Military, political, or economic advantage.
- **Scope of Activities:** Cyberattacks, cyberespionage, disinformation campaigns.
- **Methods Used:**
    - Malware, computer viruses, phishing attacks
    - Denial-of-Service (DoS) attacks
    - Ransomware and botnet deployment

- **Target Domains:** Government systems, military networks, infrastructure, private corporations, media, and public opinion.

- **Actors Involved:** Primarily **nation-states**, though **non-state actors**, hacktivist groups, and criminal syndicates may also participate.

Types of Cyberwarfare Attacks

Type of Attack	Description	Example
Cyber Espionage	Unauthorized access to steal confidential data for political or military gain	Fancy Bear (Russian state-linked group)
Cyber Sabotage	Disruption or destruction of systems to cause damage or hinder operations	Stuxnet attack on Iran's nuclear facilities
Data Theft	Theft of personal, corporate, or classified data for espionage or ransom	Sony Pictures hack (attributed to North Korea)
Ransomware	Encryption of data with demand for payment to restore access	WannaCry (linked to North Korea)
Denial-of-Service	Overwhelming digital infrastructure to disrupt services	NotPetya attack on Ukraine
Disinformation Campaigns	Spreading false or manipulated information to influence public opinion or destabilize societies	Election interference operations

---

Major Targets of Cyberwarfare

Cyberattacks are increasingly aimed at vital infrastructure and institutions that support the core functioning of society and the state.

Sector	Assets Targeted	Potential Impact
Critical Infrastructure	Power grids, water systems, telecom, transport	Blackouts, service disruption, public safety concerns
Military & Defense	Networks, logistics, weapon systems	Espionage, disruption of operations, compromise of national security
Financial Systems	Banks, stock exchanges, digital payments	Economic instability, theft, loss of trust in institutions
Healthcare Sector	Hospitals, medical records, diagnostics	Ransomware attacks, data breaches, endangering patient care
Education & Research	Universities, research labs	Intellectual property theft, data breaches
Industrial Control Systems	Factories, utilities, process automation	Physical damage, production halts, economic losses
Private Sector Corporates	Trade secrets, digital infrastructure	Financial loss, reputational damage, sabotage
Internet Backbone	ISPs, servers, network hardware	Disrupted connectivity, surveillance, data interception

Sector	Assets Targeted	Potential Impact
Information Ecosystem	Media houses, social platforms	Misinformation, polarization, erosion of democratic discourse

India’s Response to Cyberwarfare Threats

India has made notable strides in bolstering its cybersecurity framework:

1. Recognition and International Standing

- India has been ranked in the **Tier 1 category of the Global Cybersecurity Index (2024)** by the **International Telecommunication Union (ITU)**, indicating strong cybersecurity preparedness.

2. Key Institutional Mechanisms

- **Defence Cyber Agency (DCyA):**
  A tri-service command tasked with developing cyber strategy, conducting offensive and defensive cyber operations, and securing military communication infrastructure.

- **Cyber Emergency Response Teams (CERTs):**
  Established in all three Armed Forces to respond to threats specific to military and defense infrastructure.

- **CERT-In (Indian Computer Emergency Response Team):**
  The nodal agency under the Ministry of Electronics and IT, responsible for tracking, forecasting, and responding to national cyber incidents.

- **Indian Cybercrime Coordination Centre (I4C):**
  Supports law enforcement in tracking and responding to cybercrimes at state and national levels.

- **National Critical Information Infrastructure Protection Centre (NCIIPC):**
  Secures critical infrastructure sectors like energy, banking, and transportation.

3. Policy and Strategy

- **National Cybersecurity Policy, 2013:**
  First comprehensive framework aimed at securing India's cyberspace.

- **National Cybersecurity Strategy, 2020 (Proposed):**
  Focuses on:

- Building secure digital infrastructure
- Promoting cyber hygiene among citizens
- Enhancing cyber threat intelligence and cooperation

4. Awareness and Training Initiatives

- **Bharat National Cyber Exercise (Bharat NCX):**
  Conducted annually by the **National Security Council** in collaboration with **Rashtriya Raksha University** to simulate cyberattack scenarios and train stakeholders.
- **Cyber Swachhta Kendra (Botnet Cleaning Centre):**
  Citizen-centric service offering tools to detect and remove malicious software from systems, extending the vision of a "Clean Cyber India."

Cyberwarfare and International Law

Despite the transnational nature of cyberwarfare, there is no universally binding legal framework. However, several instruments guide state behavior:

Framework/Instrument	Description
UN Charter (Article 51)	Allows self-defense in case of armed attack, extended to significant cyberattacks
Budapest Convention on Cybercrime	First international treaty to address cybercrime through legal and cooperative mechanisms
UN Convention against Cybercrime (2024)	Aims to enhance global cooperation in combating cybercrime, with broader participation
Tallinn Manual	Academic study interpreting how international law applies to cyber operations; though non-binding, it's influential

---

Conclusion

Cyberwarfare has emerged as the **fifth dimension of warfare**, alongside land, air, sea, and space. It has the potential to cause **severe real-world consequences**—from blackouts to election interference—and reshape modern conflicts.

As India’s digital dependence grows, so too does its exposure to cyber threats. Therefore:

- Strengthening domestic cyber defense infrastructure,
- Promoting cyber diplomacy for international cooperation,

- Updating legal frameworks for modern cyber challenges, and
- Building a skilled cybersecurity workforce

are imperative to safeguard national security and sovereignty in the digital age.
