Cyberwarfare

Mains Syllabus: GS III - Role of external state and non-state actors in creating challenges to internal security; Science and Technology- developments and their applications and effects in everyday life.

Why in the News?

Following the terrorist attack on tourists in Pahalgam and the subsequent Operation Sindoor, more than one million cybersecurity incidents were flagged within 10 days.

What is cyberwarfare?

- **Cyberwarefare** – It is the use of information technology for military or political purposes, including cyberattacks, espionage, and information warfare.
- **Activities** - It involves disrupting, damaging, or gaining an advantage over an adversary's digital infrastructure and information systems through cyberattacks, cyberespionage, and information warfare.
- **Methods** – It utilizes various techniques like computer viruses, denial-of-service attacks, and phishing.
- **Targets** – During cyberwarfare, any government, civilian, and military systems are targeted.
- **Actors** – While cyberwarfare can involve non-state actors, it is typically associated with actions by or on behalf of nation-states, often with political, military, or economic motivations.

Types of Cyberwarfare Attacks		
Type	**Description**	**Example Attacks**
Cyber Espionage	Unauthorized access to steal sensitive information for political, military, or economic advantage	Fancy Bear (Russian group)
Cyber Sabotage	Disruption or destruction of systems to hinder operations or cause harm	Stuxnet (Iran nuclear facilities)
Data Theft	Stealing data for intelligence, ransom, or to incite chaos	Sony Pictures hack (North Korea)
Ransomware	Encrypting data and demanding payment for its release	WannaCry (North Korea)
Denial-of-Service	Overwhelming systems to disrupt access or operations	NotPetya attack (Ukraine)

Disinformation	Spreading false information to influence public opinion or destabilize society	Election interference campaigns

What are the major targets of cyberwarfare?

- Cyberwarfare operations are designed to disrupt, damage, or gain control over critical assets and infrastructure of adversaries.
- **Critical Infrastructure** – Power plants, electric grids , airports are frequent targets, as attacks can cause widespread blackouts or disrupt public activities.
- **Internet and Communication Infrastructure** - Attacks can target the backbone of the internet, including ISPs, web servers, and network equipment, to cause widespread outages or intercept communications.
- **Military Systems** - Cyberwarfare can target military command-and-control systems, weaponry, and logistics to disrupt operations or steal classified information.
- **Financial Sector** – Attacks on banks , payment systems and stock markets are used to destabilize the economic functioning of a country.
- **Healthcare** - Hospitals and health systems are targeted due to the critical nature of their services and the sensitive data they hold, making them susceptible to ransomware and data breaches.
- **Industrial Control Systems** - Systems that manage physical infrastructure, such as factories and utilities, are targeted to cause physical damage or halt production.

Major Targets during Cyberwarfare		
Target Sector	**Examples of Assets Attacked**	**Potential Impact**
Critical Infrastructure	Power grids, water, transportation, telecom	Blackouts, service disruption, public safety
Government & Military	Agencies, military networks, weapon systems	Espionage, military disruption, data theft
Financial Sector	Banks, stock exchanges, payment systems	Economic instability, theft, loss of trust
Healthcare	Hospitals, health records	Ransomware, data breaches, patient risk
Education	Universities, research data	IP theft, data breaches, operational impact
Industrial Control	Factories, utilities, process controls	Physical damage, production halts
Private Sector	Corporations, trade secrets	Espionage, sabotage, financial loss
Internet Infrastructure	ISPs, web servers, network hardware	Outages, interception, loss of connectivity
Information/Propaganda	Media, social networks	Public opinion manipulation, unrest

What are the government measures against cyberwarfare?

India has marked a significant milestone in its cybersecurity efforts by achieving

top Tier i.e. Tier 1 status in the Global Cybersecurity Index (GCI) 2024, published by the International Telecommunication Union (ITU).

- **Defence Cyber Agency** – It a tri-service command of the Indian Armed Forces responsible for handling cybersecurity threats.
- The DCyA is tasked with formulating cyber doctrine, strategy, and policy for the defense forces, conducting joint training and exercises, and managing cyber operations.
- **Cyber Emergency Response Teams (CERT)** - To mitigate cyber threats, all the three Services have established their respective Cyber Emergency Response Teams (CERT).
- **Bharat National Cyber Security Exercise** - National Security Council in strategic partnership with Rashtriya Raksha University(RRU) organizes annually Bharat NCX to strengthens vigilance and preparedness in safeguarding our nation's invaluable digital assets.
- **National Cybersecurity Policy, 2013** - It lays down a comprehensive strategy for addressing the multifaceted challenges of cybersecurity to build a secure and resilient cyberspace in India.
- **National Cybersecurity Strategy, 2020** – It is a significant step forward in India's efforts to secure its cyberspace against evolving threats.
- It aims to create a safe, secure, and resilient cyberspace for citizens, businesses, and the government.
- **Institutional Framework** - Indian Computer Emergency Response Team (CERT-In) , Indian Cybercrime Coordination Centre (I4C) and the National Critical Information Infrastructure Protection Centre (NCIIPC) ensure a coordinated response to cyber incidents.
- **Cyber Swachhta Kendra (CSK)**- It is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space.

Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same.

What is the international law on cyberwarfare?

- **UN Charter** – It recognizes the inherent right of individual or collective self-defense if an armed attack occurs including the cyberwarfare attack.
- **Budapest Convention on Cybercrime** – It is a treaty that establishes international cooperation and provides a framework for tackling cybercrime.
- **UN Convention against Cybercrime** – Adopted in 2024, this new convention aimed at strengthening international cooperation in preventing and combating cybercrime.
- **Tallinn Manual**- This non-binding academic study interprets how international law applies to cyberwarfare, addressing sovereignty, state responsibility, and countermeasures.

Conclusion

- Cyberwarfare has become a critical domain alongside land, sea, air, and space, with the potential to cause real-world damage and influence military and political outcomes.
- As nations become increasingly reliant on digital infrastructure, the importance of robust cyber defense and international cooperation continues to rise.
- While existing international law provides foundational principles, persistent ambiguities in attribution, thresholds, and jurisdiction underscore the need for clearer norms.

References

[Business Standard | Cyberwarfare signs]