# Defence & Security · GS - III

**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.**

| EXAM YEAR | PAPER | SUBJECT |
|---|---|---|
| 2022 | GS - III | Defence & Security |

| MARKS | WORD LIMIT |
|---|---|
| 15 | ~250 words |

## Answer Hint

**Cybersecurity protects networks, devices, applications and data through confidentiality, integrity, availability, authentication and accountability. India has strengthened its institutional and legal framework through CERT-In, NCIIPC and sectoral initiatives, but fragmented responsibilities, skills shortages and the absence of a publicly released comprehensive national strategy as of 2022 reveal important gaps.**

## Model Answer

### Introduction

Cybersecurity involves protecting digital systems and information against unauthorised access, disruption, manipulation and theft.

### Key Elements

Its core principles are confidentiality, integrity and availability. Other elements include authentication, access control, encryption, incident response, risk assessment, security audits, user awareness and business continuity.

### India’s Progress

India has established several important mechanisms. CERT-In coordinates responses to cybersecurity incidents, while the National Critical Information Infrastructure Protection Centre safeguards critical sectors. The Information Technology Act, 2000, and subsequent rules provide a legal framework. Cybercrime reporting systems, digital forensics and sectoral security guidelines have also improved response capacity.

**Challenges and Limitations**

Threats include ransomware, phishing, data breaches, attacks on critical infrastructure and vulnerabilities in emerging technologies. Shortages of skilled professionals, uneven security among smaller organisations, limited public awareness and coordination gaps persist. Cybersecurity responsibilities are distributed across multiple institutions and sectors. Although policy initiatives and draft proposals have existed, **a comprehensive, publicly released National Cyber Security Strategy had not been fully operationalised by 2022**.

**Way Forward**

India needs clear national objectives, defined institutional responsibilities, stronger public-private information sharing, indigenous security capabilities, skilled personnel and regular audits. Privacy safeguards and international cooperation should accompany stronger cyber resilience.

**Conclusion**

India has developed significant cybersecurity institutions, but a coherent, adequately funded and accountable national strategy is necessary to address evolving digital threats comprehensively.

BECOME IAS
AI POWERED UPSC PREP