

WRAP Exams · wrapexams.com

Prelims PYQ, Mains model answers, and copy evaluation. Write to the desk for this paper, a doubt, or the AI waitlist.

ask@wrapexams.com · +91 85951 84903 · wrapexams.com

Q19

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 Civil Services Mains 2022 · GS III · 15 marks · Cyber Security and Money Laundering

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention.

Core demand of the question

- State the elements of cyber security
- Examine how far India has a comprehensive National Cyber Security Strategy

Revision summary

Cyber security elements are confidentiality, integrity, availability, authentication, human process, supply chain, and legal institutions.

India's notified document is the National Cyber Security Policy 2013.

A National Cyber Security Strategy was discussed around 2020; a complete public successor was not firmly in force as a single comprehensive charter by 2022.

Operational bodies include **CERT-In**, **NCIIPC** and **I4C**, plus sector regulators.

Gaps remain in MSME/hospital security, skills, supply chain and fragmented law.

Introduction

Cyber security is the protection of networks, devices, data and people from unauthorised access and disruption. It is not only a firewall. India has a **National Cyber Security Policy, 2013**, a **CERT-In**, sectoral CERTs, and years of discussion of a fuller **National Cyber Security Strategy** (a public draft conversation around **2020**). Comprehensive on paper is not the same as comprehensive in every ministry and firm.

Body

Elements of cyber security

- **Confidentiality:** secrets and personal data stay with those allowed (encryption, access control). The **Digital Personal Data Protection** trajectory later added a legal overlay; in 2022 the IT Act and SPDI rules were still the main personal-data peg.
- **Integrity:** data and software are not silently altered (hashing, signing, secure updates).
- **Availability:** systems stay up under attack (DDoS defence, backups, redundancy)-critical for power, payments and hospitals.
- **Authentication and identity:** who is at the keyboard; **Aadhaar** and e-sign help citizens but also enlarge the target.

- **People and process:** phishing is still the usual door; training, least privilege, and incident response matter as much as tools.
- **Physical and supply chain:** devices, undersea cables, and **hardware/software provenance**.
- **Legal-institutional:** offences, MLATs, **CERT-In** directions, and sector regulators (RBI for banks, **CERT-In** for incident reporting).
- **Offensive-defensive balance:** attribution, critical-information-infrastructure protection under the **NCIIPC**, and military cyber commands as a separate but related layer.

How far a comprehensive National Cyber Security Strategy?

- **2013 Policy:** the notified **National Cyber Security Policy** set aims-secure computing, 24×7 **CERT-In**, manpower, and public-private partnership. It was a **policy**, light on dated targets, budgets and ministry-by-ministry duties.
- **2020 discussion:** the National Security Council Secretariat process and a **draft National Cyber Security Strategy** around 2020 sought to update 2013 for **5G, cloud, supply chain, and a whole-of-nation** approach. A single, fully notified, publicly detailed successor strategy was still **awaited / partial** in public domain at the time of the 2022 paper-candidates should not invent a gazette date that did not exist.
- **What does exist in practice:** **CERT-In** (including 2022-type incident-reporting directions), **NCIIPC** for critical infrastructure, **I4C** (Indian Cyber Crime Coordination Centre), State cyber police, **National Critical Information Infrastructure** notifications, RBI/SEBI/IRDAI circulars, and Defence cyber capacity.
- **Gaps versus 'comprehensive':** uneven State capacity; MSME and hospital security; **supply-chain** assurance for telecom; shortage of skilled analysts; fragmented laws (IT Act 2000 amendments vs a dedicated cyber security statute); and the tension between **CERT-In logging directions** and privacy/startup cost.
- **Verdict:** India has a **policy (2013) plus a dense operational stack**, and a **strategy still more discussed than finally, fully public as one binding 2020 text**. It is **substantial but not yet one comprehensive, uniformly implemented national strategy**.

What would make it comprehensive

- One **public strategy** with roles, funds, and review dates; cyber hygiene for MSMEs; supply-chain rules; and judicial capacity-without treating every citizen log as a security win.

Flow diagram

CIA identity people supply chain -> Cyber security
 NCSP 2013 -> Cyber security
 Strategy discussion 2020 -> Cyber security
 CERT-In NCIIPC I4C -> Cyber security
 Gaps MSME supply chain skills law -> Cyber security

Conclusion

Cyber security is confidentiality, integrity, availability, identity, people, supply chain and law. India notified a 2013 policy and built **CERT-In**, **NCIIPC** and **I4C**. A full National Cyber Security Strategy was under discussion around 2020 and was not yet a complete, uniformly applied public charter by the 2022 exam window. The stack is real; the single strategy is unfinished.

Facts & figures

NCSP 2013

National Cyber Security Policy 2013: India's notified policy on secure cyberspace, CERT-In strengthening and manpower.

NCSS discussion 2020

National Cyber Security Strategy drafting/consultation around 2020 to update 2013 for new threats; not to be confused with a fully gazette-final public Act.

CERT-In

Indian Computer Emergency Response Team: national nodal agency for incident response and directions to service providers.

NCIIPC

National Critical Information Infrastructure Protection Centre: under NTRO, protects designated critical sectors.

I4C

Indian Cyber Crime Coordination Centre (MHA): platform for cybercrime reporting and State coordination.

WRAP Exams · Write. Read. Analyse. Practice. · <https://wrapexams.com/upsc/mains-answers/gs-3/2022/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/> · ask@wrapexams.com · wrapexams.com