National Cyber Security Policy: Notes for UPSC Exam

In this article, you can read about the National Cyber Security Policy, which was first drafted in the wake of reports that the US government was spying on India and there were no technical or legal safeguards against it. Cybersecurity is an important topic in the UPSC exam syllabus.

The National Cyber Security Policy is a policy document drafted by the Department of Electronics and Information Technology (DeitY) in 2013 aimed at protecting public and private infrastructure from cyber attacks. The guideline also seeks to protect personal information of internet users, financial and banking information, and sovereign data.

Need for a cyber security policy

- Before 2013, India did not have a cyber security policy. The need for it was felt during the NSA spying issue that surfaced in 2013.
- Information empowers people and there is a need to create a distinction between information that can run freely between systems and those that need to be secured. This could be personal information, banking and financial details, security information which when passed onto the wrong hands can put the country's safety in jeopardy.
- This Policy has been drafted in consultation with all the stakeholders.
- In order to digitise the economy and promote more digital transactions, the government must be able to generate trust in people in the Information and Communications Technology systems that govern financial transactions.
- A strong integrated and coherent policy on cyber security is also needed to curb the menace of cyber terrorism.

National Cyber Security Policy Vision

To build a secure and resilient cyberspace for citizens, businesses and Government.

National Cyber Security Policy Mission

- To protect information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.

- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

National Cyber Security Policy Objectives

- Encouraging the adoption of IT in all sectors of the economy by creating adequate trust in IT systems by the creation of a secure cyber ecosystem.
- Creating an assurance framework for the design of security policies and for the promotion and enabling actions for compliance to global security standards and best practices through conformity assessment.
- Bolstering the regulatory framework for ensuring a secure cyberspace ecosystem.
- Enhancing and developing national and sectoral level 24 x 7 mechanisms for obtaining strategic information concerning threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- Operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to improve the protection and resilience of the country's critical infrastructure information.
- Developing suitable indigenous security technologies to address requirements in this field.
- Improving visibility of the ICT products/services' integrity by having testing and validation infrastructure.
- Creating a workforce of 500,000 professionals skilled in cyber security in the next 5 years.
- Providing businesses with fiscal benefits for adopting standard security practices and processes.
- Safeguarding of the privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
- Enabling effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through legislative intervention.
- Developing a culture of cyber security and privacy.
- Developing effective public private partnerships and collaborative engagements by means of technical and operational cooperation.
- Promoting global cooperation by encouraging shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

For more articles and UPSC preparation material follow the links given in the table below: