Unit 5. National Cyber Security Policy 2013 – In a nutshell

The National Cyber Security Policy 2013 aims at (1) facilitating the creation of secure computing environment (2) enabling adequate trust and confidence in electronic transactions and (3) guiding stakeholders actions for the protection of cyberspace.

What is National Cyber Security Policy 2013 all about?

The National Cyber Security Policy document outlines a roadmap to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

The need to protect information

National Cyber Security Policy 2013 should be seen as about **protecting of information**, such as personal information, financial/banking information, sovereign data etc.

- Information empowers, and in order to empower people with information, we need to **secure the information/data**.
- There is a need to **distinguish between data which can freely flow and data which needs to be protected**.
- The "National Cyber Security Policy" has been prepared in consultation with all relevant stakeholders, user entities and public.
- This policy aims at facilitating the creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders actions for the protection of cyberspace.
- The National Cyber Security Policy document outlines a roadmap to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.
- The policy recognises the need for objectives and strategies that need to be adopted both at the national level as well as international level.

The objectives and strategies outlined in the National Cyber Security Policy

1. Articulate our concerns, understanding, priorities for action as well as directed efforts.
2. Provide confidence and reasonable assurance to all stakeholders in the country (Government, business, industry and the general public) and global community, about the safety, resiliency and security of cyberspace.
3. Adopt a suitable posturing that can signal our resolve to make determined efforts to effectively monitor, deter and deal with cyber crime and cyber attacks.

Salient features of the National Cyber Security Policy 2013

In brief, the National Cyber Security Policy covers the following aspects:

- **A vision and mission statement** aimed at **building a secure and resilience cyberspace for citizens, businesses and Government.**

- Enabling goals aimed at reducing national vulnerability to cyber attacks, preventing cyber attacks & cyber crimes, minimising response & recovery time and effective cybercrime investigation and prosecution.
- Focused actions at the level of Govt., public-private partnership arrangements, cyber security related technology actions, protection of critical information infrastructure and national alerts and advice mechanism, awareness & capacity building and promoting information sharing and cooperation.
- Enhancing cooperation and coordination among all the stakeholder entities within the country.
- Objectives and strategies in support of the National Cybersecurity vision and mission.
- Framework and initiatives that can be pursued at the Govt. level, sectoral levels as well as in public-private partnership mode.
- Facilitating monitoring key trends at the national level such as trends in cyber security compliance, cyber attacks, cyber crime and cyberinfrastructure growth.

Cyber Security related updates:

- A National and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through**National Critical Information Infrastructure Protection Centre (NCIIPC)**.
- **Computer Emergency Response Team (CERT-In**) has been designated to act as a nodal agency for coordination of crisis management efforts. CERT-In will also act as an umbrella organisation for coordination actions and operationalization of sectoral CERTs.
- A mechanism is proposed to be evolved for obtaining strategic information regarding threats to information and communication technology (ICT) infrastructure, creating scenarios of response, resolution and crisis management through effective predictive, prevention, response and recovery action.