1. Coming soon-Indian Cyberspace

Context:

- Cyber security incidents observed by the Indian Computer Emergency Response Team (CERT-In) went up almost four times from 2017 to 2018.
- **India's global rank on the cyber security index slipped to 47 in 2018 from 23 in 2017,** according to the **UN Agency ITU (International Telecommunication Union).**

Brief Background:

- Cybersecurity threats may manifest within a technical context like an unpatched software vulnerability, a malicious software or link, but mostly emanate from fear, carelessness, greed or sheer carelessness—the basic human vulnerabilities.
- This would only get further amplified with the onset of 5G, artificial intelligence, augmented reality, robotics, quantum computing and the Internet of Things.
- There is a need to secure, strengthen and synergise the policy toolkit in this realm. Besides the Information Technology Act, 2000, and the upcoming data privacy law, the government has begun discussions on the National Cyber Security Strategy (NCSS) 2020.

What should be the Contours of the NCSS?

- **Tech is global, policy is local:** It is a set of common and interoperable set of standards that make the 'packets' of data traverse the global cyberspace crisscrossing continents, oceans and even the space, but a government's writ runs basically on its jurisdiction.
- India should consider joining or leveraging existing frameworks like the Convention on Cybercrime and the Paris Call because cyber security has become a geopolitical issue.
- **Security by Design, Budgeting by default:** It is high time that 10% of every IT budget in the government be earmarked for cyber security, as recommended by the NASSCOM Cyber Security Task Force
- **Security vs Privacy: A False Binary:** Rather than being contrary to each other, security and privacy actually reinforce each other. After all, there cannot be any data privacy without data security. Hence, the NCSS and the data protection framework must be consistent with each other.

- **Prevention is better than Cure:** nine out of 10 data breaches can be mitigated if we all take care of basic cyber security like using licensed and updated software, using different and difficult passwords for different services and devices, multi-factor authentication and strong encryption. We need innovative solutions to scale up awareness.
- **Bidirectional Partnership:** The government should share its own assessment back with the private sector to create incentive for the latter to proactively share their intelligence on threat vectors without jeopardising contractual obligations or intellectual property
- **Pragmatic, Predictable, Flexible:** Underlying principles must go along with the strategic objectives and provide sufficient guidance and flexibility to sector regulators within their respective ecosystem.
- **For example,** the cyber security guidelines or frameworks issued by RBI, SEBI, IRDAI and PFRDAI can be greatly synergised under the aegis of the Financial Stability and Development Council (FSDC), thereby bringing greater sanity for the regulators as well as the regulated entities.
- In addition, every regulation must emerge through public consultation and be backed up with a regulatory impact assessment, whether it is about cross-border data flows or Restricting Encryption.

Source: Financial Express