Self-Reliance in Cybersecurity

For Prelims: <u>Self-Reliance</u> in Cybersecurity, India Mobile Congress, <u>India's digital infrastructure</u>, National Security, Electronic Equipments, <u>National Cyber Security Strategy 2020.</u>

For Mains: Self-Reliance in Cybersecurity, Awareness in the fields of IT, Space, Computers, robotics, nano-technology, bio-technology.

Source: IE

Why in News?

Recently, the Prime Minister of India has emphasised the importance of <u>Self-Reliance</u> in <u>Cybersecurity</u> during the 7th edition of the **India Mobile Congress.**

 PM's emphasis on self-reliance in the entire cybersecurity value chain, including hardware, software, and connectivity, reflects the growing concern about the security of <u>India's digital</u> <u>infrastructure.</u>

What is Cybersecurity?

- Cybersecurity is the practice of protecting computer systems, networks, devices, and data from theft, damage, unauthorised access, or any form of malicious intent.
- It encompasses a wide range of technologies, processes, and practices designed to safeguard digital information and the infrastructure that stores, processes, and transmits it.

What is Self Reliance in Cybersecurity?

- About:
 - Self-reliance in cybersecurity refers to a nation's ability to develop and maintain its own capabilities, technologies, and expertise to protect its digital infrastructure, data, and information systems without relying heavily on foreign technology or external assistance.
 - It emphasizes the development and deployment of indigenous cybersecurity solutions and practices, reducing dependence on external sources for cybersecurity tools and expertise.
- Need for Self Reliance in Cyber Security:
 - National Security: Many of a nation's critical infrastructure systems, such as energy grids, transportation networks, and communication systems, rely on digital technology.
 - Modern military operations are heavily dependent on digital technology.
 - Any compromise in cybersecurity can **result in significant disruptions**, posing a direct threat to national security.
 - Geopolitical Considerations: Over-reliance on foreign technology, particularly from

countries with which India may have strained relations such as China, can pose a security risk.

- Since India imports the majority of electronic raw materials from China, which is a cause for concern for India.
- Achieving self-reliance reduces the **vulnerabilities associated with depending on technology** from external sources.
- **Technological Independence**: Self-reliance necessitates the creation of secure and reliable hardware, software, and networking components.
 - This encourages innovation and research in the field of cybersecurity.
 - Relying on foreign technology may expose the supply chain to vulnerabilities. Self-reliance allows India to have greater control over the entire technology supply chain, reducing potential risks.

What are the Challenges Related to Cybersecurity in India?

Profit-Friendly Infrastructure Mindset:

- Post liberalisation, the <u>Information Technology (IT)</u>, <u>electricity</u> and <u>telecom sector</u> has witnessed large investments by the private sector. However, their inadequate focus on cyber attack preparedness and recovery in regulatory frameworks is a cause of concern.
- All operators are focused on profits, and do not want to invest in infrastructure that will not generate profits.
- Absence of Separate Procedural Code:
 - There is no separate procedural code for the investigation of cyber or computer-related offences.
- Trans-National Nature of Cyber Attacks:
 - Most cyber crimes are trans-national in nature. The collection of evidence from foreign territories is not only a difficult but also a tardy process.
- Expanding Digital Ecosystem:
 - In the last couple of years, India has traversed on the path of digitalising its various economic factors and has carved a niche for itself successfully.
 - Latest technologies **like** <u>5G</u> **and the** <u>Internet of Things (IoT</u>) will increase the coverage of the internet-connected ecosystem.
 - With the advent of digitalisation, paramount consumer and citizen data will be stored in digital format and transactions are likely to be carried out online which makes India a breeding ground for potential hackers and cyber-criminals.

• Limited Expertise and Authority:

- Offenses related to <u>crypto-currency</u> remain under-reported as the capacity to solve such crimes remains limited.
- Although most State cyber labs are capable of analysing hard disks and mobile phones, they are yet to be recognized as 'Examiners of Electronic Evidence' (by the Central Government). Until then, they cannot provide expert opinions on electronic data.

How is India Making Strides in Technology Development?

Domestic Supply Chain Partners:

- India is actively working to **diversify its supply chain partners**, especially in the technology sector. This diversification is essential, given the dominance of Chinese players in the manufacturing ecosystem.
- The government seeks to establish more trusted and secure supply chains to prevent malware and cyber threats.
- 5G and Mobile Broadband:
 - The government awarded **100 5G Use Case labs to educational institutions across the country**, indicating its commitment to advancing 5G infrastructure.
 - India has transitioned from the **5G rollout stage to the 5G reach-out stage**. The median mobile broadband speed has increased threefold in just one year.
 - India's emphasis on becoming a leader in 6G technology underscores the country's ambition to stay at the forefront of technological advancements.

Broadband Speed:

• India's position in terms of broadband speed has significantly improved, moving from **118th**

to 43rd globally which indicates the growth of high-speed internet access in the country.

- Electronics and Smartphone Manufacturing:
 - There has been significant progress in electronics and smartphone manufacturing.
 - Semiconductor manufacturing is a critical component of the technology supply chain and plays a pivotal role in hardware production.
- Startup Ecosystem:
 - India's startup ecosystem has been flourishing, with a rapid increase in the number of startups.
 - The transformation from having 100 startups before 2014 to approximately 100,000 startups today.

What are the Initiatives Related to Cybersecurity?

- Global Initiatives:
 - Budapest Convention on Cybercrime:
 - Internet Governance Forum (IGF)
 - UNGA Resolutions
- Indian
 - National Cyber Security Strategy 2020
 - National Critical Information Infrastructure Protection Centre (NCIIPC)
 - Indian Cyber Crime Coordination Centre (I4C).
 - National Cyber Crime Reporting Portal
 - <u>Computer Emergency Response Team India (CERT-In)</u>
 - India's draft Digital Personal Data Protection Bill 2022

Way Forward

- The Vision Encourage research and development in the field of cybersecurity. Establish partnerships between government agencies, academic institutions, and private sector companies to promote innovation and the development of indigenous cybersecurity technologies.
- Provide support, funding, and incentives to cybersecurity startups and small and medium-sized enterprises (SMEs) working on innovative cybersecurity solutions. These startups can play a significant role in creating homegrown technologies.

PDF Reference URL: https://www.drishtijas.com/printpdf/self-reliance-in-cyber-security