Indigenising India's Cyber Space

What is the issue?

\n\n

With emerging cyber threats and national security challenges, it is crucial for India to indigenise the IT infrastructure of its military.

\n\n

What are India's aims in this regard?

\n\n

\n
- The following were spelt out at different instances as priorities in the cyber space -
\n

\n\n

\n
i. a Digital Armed Force and the increasing importance of dominating the cyber space
\n
ii. preparing for rivalries in cyber space
\n
iii. the role of the services in encouraging the development of domestic capabilities
\n

\n\n

\n
- The first vision is on its way to realisation as the government has sanctioned recently the raising of a cyber agency.
\n

\n\n

\n
- This will steer the planning and conduct of cyber warfare in the military.
\n
- Hopefully, once the doctrine has matured, the cyber agency will be expanded

to a much-needed cyber command.
\n
- But the goal of building domestic capability remains largely unfulfilled.
\n

\n\n

What is the emerging global threat?

\n\n

\n
- Under the PRISM programme, the US National Security Agency (NSA) collected data from internet communications.
\n
- Leaked documents showed the close involvement of US technology companies like Microsoft, Google, Yahoo, Facebook and Apple.
\n
- The NSA was collecting data directly from the servers of US service providers.
\n
- Microsoft had actively helped the NSA to avoid its own encryption of web chats on Outlook.com.
\n
- It also permitted PRISM to access its cloud storage service SkyDrive, and monitor Skype chats.
\n
- Microsoft denied these allegations, but the evidence was overwhelming.
\n
- Likewise, a recent Bloomberg report highlighted China’s intelligence services' similar moves.
\n
- It ordered subcontractors in China to plant malicious chips in Supermicro server motherboards bound for the US.
\n
- Faced with these dangers, countries have moved to restrict foreign products from use in critical networks.
\n
- E.g. in 2014, China banned government offices from buying Microsoft Windows
\n
- Recently, US President Trump signed a bill banning the use of Chinese Huawei and ZTE technology by the US government.
\n
- This followed a 2017 ban on the Moscow-based Kaspersky Lab.
\n

\n\n

What is the case with India?

\n\n

\n
- India seems to be largely unaware of the vulnerabilities that exist in the critical networks due to foreign hardware and software.
\n
- **BSNL** - Over 60% of software and hardware being used by BSNL is sourced from Chinese Huawei or ZTE.
\n
- This is despite Huawei being probed for hacking a BSNL network in 2014.
\n
- In 2017, BSNL signed a memorandum of understanding with ZTE for research and commercialisation of future 5G technology.
\n
- Notably, Australia has banned Huawei from supplying equipment for 5G mobile network, citing national security risks.
\n
- **AFNET** - The Air Force Network (AFNET) was launched in 2010.
\n
- Cisco (US network equipment maker) was a major supplier of equipment for AFNET.
\n
- The army's latest communication backbone, Network for Spectrum (NFS), also uses Cisco equipment.
\n
- Rather than looking at indigenous equipment, the request for proposal for NFS equipment had been manipulated to favour Cisco.
\n
- **Software** - The Indian Army mostly uses the Microsoft Windows operating system on its official computers.
\n
- Windows is an outstanding system but is a closed-source software owned by a company that is bound by US laws.
\n
- It is historically tied to the American intelligence community.
\n
- Notably, India is a prime target for American spying as India stood at the 5th place in the overall list of countries targeted by PRISM.
\n

\n\n

What is the proposal in this regard?

\n\n

\n
- In 2015, the Northern Command of the army decided to adopt the Bharat Operating System Solutions (BOSS) for all its official computers.
\n
- BOSS is an indigenously developed open-source system by the Centre for Development of Advanced Computing.
\n
- [It is an R&D organisation of the Ministry of Electronics and Information Technology.]
\n
- **Concerns** - Replicating the user-friendliness of Windows and re-training of a generation that had grown up with Windows were key challenges.
\n
- But three years later, the army is still debating the merits of BOSS.
\n
- The arguments are still centered on simplicity of usage, and not on security of networks.
\n
- There is even a push to return to Windows, instead of supporting BOSS.
\n

\n\n

What lies ahead?

\n\n

\n
- Building domestic capability for the manufacture of sophisticated weapons and equipment is indeed a major challenge.
\n
- But the same cannot be said for the hardware and software being used in the military information technology (IT) infrastructure.
\n
- Despite Indian products being available, a concerted effort to use indigenous solutions is conspicuously absent.
\n
- But with clear dangers in cyber space, India needs to move towards making changes that are essential to protect national interests.
\n
- A key task is for the Indian military to take the lead in indigenising its IT infrastructure.
\n

\n\n

\n\n

Source: Indian Express

\n