Challenge of India's Digital Sovereignty

Mains: *GS-III- Science & Technology*

Why in News?

India's digital sovereignty is under serious strain, with recent breaches and sanctions showing how dependence on foreign-owned platforms threatens national security, commerce, and governance.

What are the recent incidents that concerns India's digital and technological sovereignty?

- **Recent Security Breaches** – In April 2026, Indian Indian closed-circuit television (CCTV) networks were hacked through the Chinese software platform EseeCloud, exposing strategic defence information.
- In July 2025, Nayara Energy was abruptly denied access to its corporate email, collaboration tools, and cloud data when Microsoft's unilateral enforcement of EU sanctions due to Russian energy giant Rosneft's stake in the company.
- **Core Problem** – These incidents have exposed an uncomfortable reality –
  - India's critical digital infrastructures such as authentication systems, productivity suites, and cloud platforms operate on technology platforms owned and operated by foreign technology giants.
  - Even if data is physically stored in India, global data governance rules allow foreign cloud technology companies to be compelled by their home governments to share it.
- **Consequence for Sovereignty** – As a result, effective control over digital infrastructure shifts away from Indian entities to overseas corporations and foreign governments.
- In times of crisis, this dependence could undermine commerce, governance, and national security.

What about India's unique situation compared with the global context?

- **Vulnerability of Indian Systems** – Indian businesses and critical government services rely heavily on foreign technology platforms becomes vulnerable to decisions made by external sovereigns.
- This dependence means that if foreign governments issue directives, India could face
  - Suspension of government operations
  - Collapse of trade and commerce
  - Halted manufacturing, and

    - Weakened defence capabilities
- **Software-Defined Warfare Risks** – Modern warfare is driven by software.
- The intelligence that powers fighter aircraft, missile systems, and advanced radar installations lies in code, not hardware.
- This code is controlled by manufacturers who are accountable to foreign governments, creating a serious vulnerability for India's defence systems.
- In conflict scenarios, these manufacturers could possibly
    - Degrade targeting accuracy,
    - Reduce operational range, or worse,
    - Redirect battlefield intelligence to adversaries due to instructions from external sovereigns, all through software configuration changes.
- **Example** – During the 1999 Kargil conflict, India's access to precise GPS support was restricted, limiting navigation and targeting in mountainous terrain were operationally decisive.
- **Global Push for Digital Sovereignty** – By recognising risk & vulnerability on foreign dependence, countries worldwide are reducing dependence on foreign technology.
    - **France** – Plans to shift government departments from Microsoft Teams and Zoom to a sovereign video-conferencing platform by 2027.
    - **Netherlands, Denmark & Germany** – Exploring domestic alternatives to critical U.S. software and cloud services such as Microsoft Word, Excel, Outlook, and Teams.
    - **EU** – Seeking to reduce its dependence on American technology through independent European cloud and IT infrastructure.
    - **Türkiye** – Actively cutting its reliance on foreign technologies.

What are the challenges India faces?

- **India's Unique Vulnerability** – Unlike other nations, India's situation is uniquely precarious when contextualised within the framework of Power Transition Theory.
    - **Power Transition Theory** – When a rising nation seeks to preserve its strategic autonomy and begins to approach the level of an established hegemon, the dominant power will almost always act to restrict or contain its growth.
    - **Historical Pattern** – Rising competitors are often either contained (blocked from advancing) or co-opted (absorbed into the hegemon's system).
    - **Current Example** – The U.S. is actively trying to limit China's rise.
- **Reliance on Foreign Cloud & Software** – The heavy dependence on foreign platforms makes India vulnerable to external directives and sanctions.
- **Defence Technology Dependence** – The critical military systems rely on foreign-controlled code, creating risks in conflict scenarios.
- **Low R&D Investment** – India's gross expenditure on R&D averaged just 0.74% of GDP between 2000 and 2020 against a global average of 2.07%, limiting innovation capacity.
- **Risk Of Strategic Isolation** – Without indigenous infrastructure and stronger partnerships, India could face isolation in a fragmented global order.

What is key strategy to address the challenges?

- **Building & Strengthening Indigenous System** – The denial of GPS access during the Kargil conflict spurred India to develop its own satellite navigation system.
- Recent efforts show India's growing commitment to digital sovereignty
    - Expanding domestic semiconductor ecosystem and
    - Migrating government email systems to the homegrown Zoho platform.
- **Payments Success Story** – India's indigenous payments infrastructure through UPI and RuPay has shown that vulnerabilities arising from foreign-controlled systems can be overcome.
- This model can be extended to cloud infrastructure, e-commerce platforms, authentication systems, and defence technologies.
- **Defence Technology Self-Reliance** – India has long recognised the importance of self-reliance in defence manufacturing, its heavy reliance on the public sector has delivered the slowing progress.
- **Example** – No indigenous modern fighter aircraft despite efforts since the 1980s.
- **The U.S. model** – Defence platforms are largely developed by private corporations, with the government providing research funding and assured procurement, creating a virtuous cycle of innovation aligned with national interests.
- India is now inviting private-sector participation, such as in the Advanced Medium Combat Aircraft project under a competitive framework.
- **Partnerships for Sovereignty** – By collaborating with other nations, reduce risks of unilateral actions to denial of technology.
- **Example** – The BrahMos missile programme jointly developed with Russia.
- **Advantage** – It enables India to build technological capabilities without risking international isolation, unlike China which allowed only indigenous companies to develop critical technologies.
- **Recent developments**
    - Micron's semiconductor ATMP facility in Gujarat via India-U.S. cooperation.
    - India joining Pax Silica, a U.S.-led AI and supply-chain security initiative.
- **Raising R&D Investment** – India must urgently raise its research and development (R&D) spending to levels comparable with global leaders.
- **India's Critical Task** – With an accelerating growth trajectory, India has been inching towards this critical zone while facing a daunting task -
    - Building its economic fortune on a technology infrastructure independent of foreign influence.
    - Ensure strategic autonomy while competing globally.

What lies ahead?

- For a country of India's demographic scale and economic ambitions, seeking to approach parity with established powers, the question is not whether it can afford comprehensive technological sovereignty, but whether it can afford to forgo it.
- The extent to which India succeeds in mitigating the risks to its technological sovereignty will determine its economic competitiveness and strategic autonomy in an increasingly fragmented international order.

To take mains test, click here

Reference

[The Hindu | The challenge of India’s digital sovereignty]