Critical Infrastructure Protection

This article is based on **"Cyber attacks on critical infrastructure: Is India ready?"** which was published in The Hindustan Times on 20/05/2021. It talks about the need for securing critical infrastructure in India.

Recently, a major cyber attack crippled one of the largest pipelines in the United States (US), Colonial Pipeline, which carries about 45% of all fuel consumed on the country's East Coast. The attack disrupted fuel supplies and caused a surge in gas prices in some parts of the country.

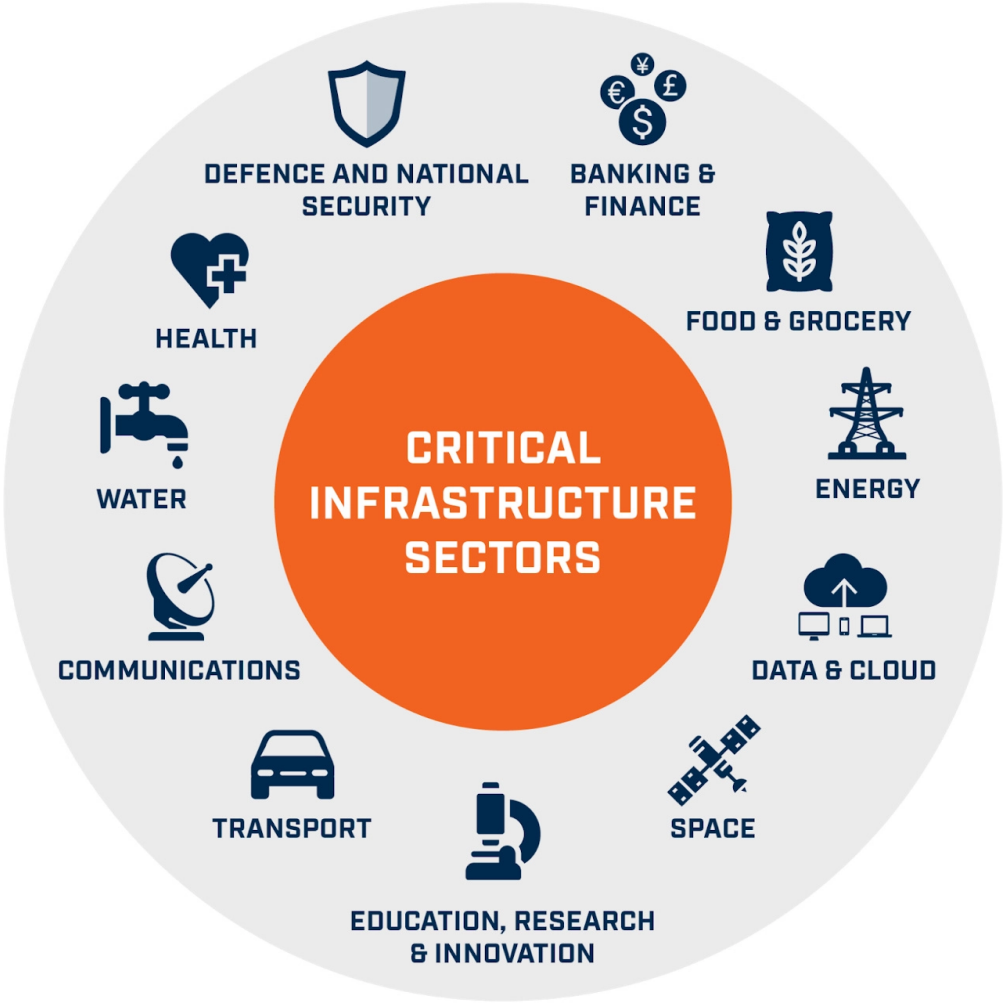
This was a case of ransomware attack, where hackers usually threaten to block the system or publish the targeted company or victim's confidential data, unless a ransom is paid.

The attack on Colonial Pipeline fits the broader trend witnessed in recent years of cyberattacks on critical infrastructure which require to be operational at all times such as traffic systems, banks, power grids, oil pipelines and nuclear reactors.

Given the increasing number of cyber attacks on critical infrastructure, it is essential for countries like India to develop a robust **cyber security architecture.**

What is Critical Infrastructure?

> Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety.



Need For A Cyber Security Framework

- **Increasing Attack on Critical Infrastructure:** In recent years, attacks targeting critical infrastructure and businesses have surged.
    - These include the 2017 WannaCry and NotPetya ransomware attacks, the 2015 attack on Ukrainian power grids and 2010 Stuxnet attack on Iranian nuclear reactor.
    - Most recently, in 2020, a China-linked hacker group RedEcho targeted India's power sector, ports and parts of the railway infrastructure.
- **Cyber Wars:** States are deploying cybersecurity attacks in order to have geo-political gains.
    - Moreover, to escape responsibility for such debilitating attacks, many States use hacking syndicates as proxies.
    - This has made critical infrastructure protection a major cybersecurity priority for India.

Associated Challenges

- **Reluctance in Sharing Information:** A significant challenge in protecting critical infrastructure is the inhibition in the private (and public) sector to share information about the vulnerability of their systems.
    - By revealing their vulnerabilities and, therefore, their proprietary information, businesses fear exposing themselves and losing a competitive edge over rivals.
    - Due to this, Indian regulators have warned that only reactive measures to cyberattacks overlooks the possibility of concerted cyber warfare by adversarial States against India.
- **Capability Asymmetry:** India lacks indigenization in hardware as well as software cybersecurity tools. This makes India's cyberspace vulnerable to cyberattacks motivated by state and non-state actors.
- **Absence of a Credible Cyber Deterrence Strategy:** Further, the absence of a credible cyber deterrence strategy means that states and non-state actors alike remain incentivized to undertake low-scale cyber operations for a variety of purposes — espionage, cybercrime, and even the disruption of critical information infrastructure.

Way Forward: Opportunities In India-Africa Relations

- **Doctrine on Cyber Conflicts:** There is a need to clearly articulate a doctrine that holistically captures its approach to cyber conflict, either for conducting offensive cyber operations or the extent and scope of countermeasures against cyber attacks.
- **Setting a Global Benchmark:** India should see the National Cyber Security Strategy as a key opportunity to articulate how international law applies to cyberspace.
    This could also mould the global governance debate to further India's strategic interests and capabilities.
- **Specifying Redlines:** National Cyber Security Strategy should include positioning on not just non-binding norms but also legal obligations on 'red lines' with respect to cyberspace-targets, such as health-care systems, electricity grids, water supply, and financial systems.
- **Promoting Indigenisation:** There is a need to create opportunities for developing software to safeguard cybersecurity and digital communications.
    - The Government of India may consider including cybersecurity architecture in its Make In India program.
    - Also, there is a need to create suitable hardware on a unique Indian pattern that can serve localized needs.
- **Public-Private Partnership:** Given the mutual distrust and vulnerability of the public and private sector, any solution involves sharing responsibility through a public-private partnership for critical infrastructure protection.
    These should focus on building an institutional framework, expanding and deepening capacity, creating security standards and strict audits and evolving a cybersecurity incident reporting framework.

Conclusion

Given the future of technology under Industrial Revolution 4.0, only an integrated, whole-of-the-ecosystem approach for securing critical infrastructure will be successful.

Drishti Mains Question

New age technologies have made critical infrastructure protection a major cybersecurity priority for India. Discuss.