Cyber Security Doctrine

This article is based on **"Patching the gaps in India's cybersecurity"** which was published in The Hindu on 06/03/2021. It talks about the need for India to have a cybersecurity doctrine.

Presently, all across the world, the changes in military doctrines favoring the need to raise cyber commands reflect a shift in strategies, which include building deterrence in cyberspace. Moreover, the area of influence of cybersecurity extends far beyond military domains to cover all aspects of a nation's governance, economy, and welfare.

India ranks 3rd in terms of the highest number of internet users in the world after the USA and China, but still, India's cybersecurity architecture is in a nascent approach.

This can be reflected by a report published in the New York Times that highlighted the possibility that the power outage in Mumbai, 2020, could have been the result of an attack by a Chinese state-sponsored group.

Therefore, given the criticality of cyberspace in the military, governance, and economic domain there is a need for a comprehensive cybersecurity doctrine in India.

Note:

India has been the victim of cyber attacks multiple times in the past.

- In 2009, a suspected cyber espionage network dubbed GhostNet was found to be targeting, amongst others, the Tibetan government in exile in India, and many Indian embassies.
- By pursuing the leads from that discovery, researchers found what they dubbed the Shadow Network, a vast cyber-espionage operation that extensively targeted Indian strategic entities.
- There were a number of subsequent attacks that targeted India, including Stuxnet, which had also taken down nuclear reactors in Iran.
- Suckfly, which targeted not just government but also private entities including a firm that provided tech support to the National Stock Exchange.
- Dtrack which first targeted Indian banks, and later the Kudankulam nuclear power plant (Tamil Nadu) in 2019.

Challenges in India's Cyber Security Architecture

- **False Flag Attacks:** The documents released by WikiLeaks show that groups such as the Central Intelligence Agency's UMBRAGE project have advanced capabilities of misdirecting attribution to another nation-state ("false flag attacks") by leaving behind false "fingerprints" for investigators to find.
    - This makes it difficult for India to launch a counterattack.

- **Problems With 'All of Government Approach':** While seeking to create an 'all of government' approach to countering and mitigating cybersecurity threats at the national level, has also resulted in concerns around effective coordination, overlapping responsibilities, and lack of clear institutional boundaries and accountability.
- **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.
    - India doesn't have an 'active cyber defense' like the EU's **General Data Protection Regulation (GDPR)** or the US' Clarifying Lawful Overseas Use of Data (CLOUD) Act.
- **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.

CyberSecurity Institutions

- Over the past two decades, India has made a significant effort at crafting institutional machinery focusing on cyber resilience spanning several government entities.
- The Prime Minister's Office includes within it several cyber portfolios. Among these are the National Security Council, usually chaired by the National Security Adviser (NSA), and plays a key role in shaping India's cyber policy ecosystem.
- The NSA also chairs the National Information Board, which is meant to be the apex body for cross-ministry coordination on cybersecurity policymaking.
- The National Critical Information Infrastructure Protection Centre established under the National Technical Research Organisation in January 2014 was mandated to facilitate the protection of critical information infrastructure.
- In 2015, the Prime Minister established the office of the National Cyber Security Coordinator who advises the Prime Minister on strategic cybersecurity issues.
- India's Computer Emergency Response Team (CERT-In), which is the nodal entity responding to various cybersecurity threats to non-critical infrastructure comes under the Ministry of Electronics and Information Technology (MEITY).
- The Ministry of Defence has recently upgraded the Defence Information Assurance and Research Agency to establish the Defence Cyber Agency, a tri-service command of the Indian armed forces to coordinate and control joint cyber operations and craft India's cyber doctrine.
- Finally, the Ministry of Home Affairs oversees multiple similarly-named "coordination centres" that focus on law enforcement efforts to address cybercrime, espionage and terrorism, while the Ministry of External Affairs coordinates India's cyber diplomacy push — both bilaterally with other countries, and at international fora like the United Nations.

Way Forward

National Cyber Security Policy 2013 clarified that India needs a National Cyber Security Strategy, but is yet to be released. Therefore, given the criticality of cyberspace, the new strategy should include:

- **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.
- **Multi-Stakeholder Approach:** To better detect and counter threats from both state actors and their proxies as well as online criminals, improved coordination is needed between the government and the private sector, as well as within the government itself — and at the national and State levels.
- **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.

Conclusion

A clear public posture on cyber defense and warfare boosts citizen confidence, helps build trust among allies, and clearly signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem.

Drishti Mains Question

Doctrinal clarity and institutional coherence are essential for a robust cybersecurity posture in India. Discuss.

This editorial is based on “Misplaced concern: On Supreme Court and OTT regulation” published in The Hindu on March 08th, 2020. Now watch this on our Youtube channel.