drishti

Cyber Security Framework In India

drishtiias.com/current-affairs-news-analysis-editorials/news-editorials/25-06-2020/print

This article is based on **“Why India needs an updated cybersecurity strategy”** which was published in The financial Express on 24/06/2020. It talks about the need for India to develop a comprehensive cybersecurity framework.

Recently, the cyber security attack on Australia’s communication system has brought the governance to a stand still. In India, too, cyber attacks have been occurring with increasing frequency. For example, leak of personal information of 3.2 million debit cards in 2016 and the Data Theft At Zomato (2017), Wannacry Ransomware (2017), PETYA Ransomware (2017) etc.

Further, Cyber security has become an integral aspect of national security. Moreover, its area of influence extends far beyond military domains to cover all aspects of a nation’s governance, economy and welfare.

Although India was one of the few countries to launch a cybersecurity policy in 2013, not much has transpired in terms of a coordinated cyber approach. Thus, there is a need for a comprehensive cyber security policy in India.

Need For Cyber Security Framework

- **National Security Imperative:** The change in military doctrines favouring the need to raise cyber commands reflects a shift in strategies, which include building deterrence in cyberspace.

    The need for a competent cyber security infrastructure as part of national security was first emphasized by the **Kargil Review Committee 1999.**
- **Increasing Importance of Digital Economy:** The digital economy today comprises 14-15% of India’s total economy, and is targeted to reach 20% by 2024.
- **Added Complexity:** With more inclusion of **artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of Things (IoT)**, cyberspace will become a complex domain, giving rise to issues of a techno-legal nature.

- **Securing Data:** Data is referred to as the currency of the 21st century and due to its bulk creation owing to India’s population, several international companies (Google, Amazon etc.) are trying to have access to it.
    - Given this there are issues related to data sovereignty, data localisation, internet governance, etc.
    - Thus, there is a need to build strong cyber security architecture.

Challenges in India's Cyber Security Approach

- **Lack of Cybersecurity WorkForce:** The Indian military, central police organizations, law enforcement agencies and others are deficient in manpower, for software and hardware aspects integral to this field.
    - Moreover, there is a growing demand for professionals in Artificial Intelligence (AI), BlockChain Technology (BCT), Internet of Things (IoT) and Machine Learning (ML).
    - According to several estimates there is a need for at least three million cybersecurity professionals today.
- **Lack of Active Cyber Defence:** India doesn’t have the ‘active cyber defence’ like the EU's **General Data Protection Regulation (GDPR)** or US’ Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Note:

Active Cyber Defence: It is far more than just the enhancement of defensive cybersecurity capabilities for the Government and the Intelligence Community.

Active Cyber Defence-defined capabilities and processes are employed to support federal, state, and local government agencies and organizations, critical infrastructure segments, and industry.

- **Overlapping Regulatory Bodies:** Unlike the US, Singapore, and the UK where there is a single umbrella organisation dealing in cybersecurity, India has several central bodies that deal with cyber issues, and each has a different reporting structure.

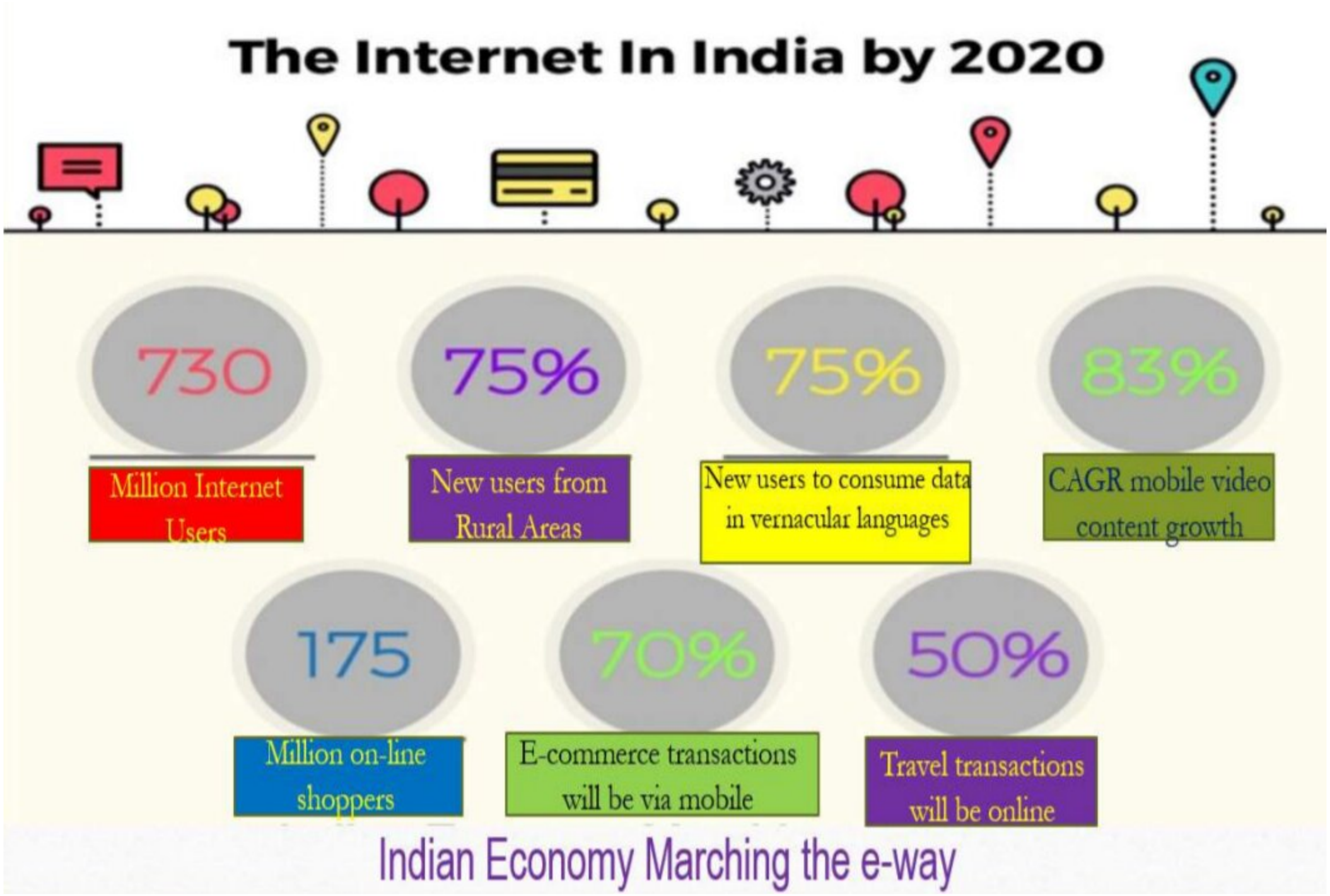
    Further, each state government has its own **Cyber emergency Response Team (CERT).**
- **Dependency on Foreign Players For Cyber Security Tools:** India lacks indigenisation in hardware as well as software cybersecurity tools.

    This makes India’s cyberspace vulnerable to cyberattacks motivated by state and non-state actors.
- **External Challenges:** Challenges such as growing Chinese influence in Indian telecom space, social media is becoming a powerful tool for dissemination of “information” making it difficult to differentiate fact from fake news.

Way Forward

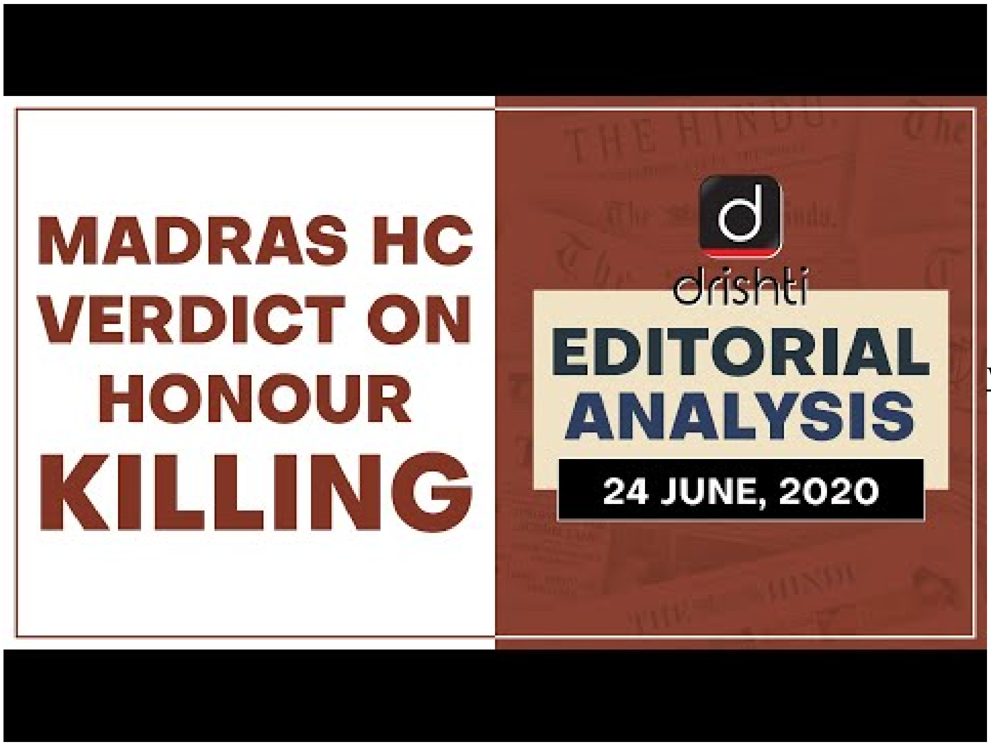
- **Creating Awareness:** With countries resorting to digital warfare and hackers targeting business organisations and government processes, India has to create awareness that not a single person or institution is immune to it.
    While the government and the corporate world are better placed perhaps to create their own programs, it is the civil society who needs to bring into this ambit.
- **Strengthening of Existing Cyber Security Framework:** National cybersecurity projects such as the **National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC)** and the Computer Emergency Response Team (CERT) need to be strengthened manifold and reviewed.
- **Bringing Cyber Security in Education:** Educational institutions including central universities, private universities, industry associations, Industrial Training Institutes (ITIs) must incorporate courses on cybersecurity.
- **Integrated Approach:** Given increasing dominance of mobile and telecommunication, both National cyber security policy and National Telecom Policy will have to effectively coalesce to make a comprehensive policy for 2030.
- **Promoting Indigenisation:** There is a need to create opportunities for developing software to safeguard cyber security and digital communications.
    - The Government of India may consider including cybersecurity architecture in its **Make In India programme.**
    - Also, there is a need to create suitable hardware on a unique Indian pattern that can serve localised needs.

Given the future of technology under Industrial Revolution 4.0, India requires a strong cybersecurity framework based on the 4D principles i.e. Deter, Detect, Destroy and Document so that it can subverse all attempts towards any cyber challenges.



Drishti Mains Question

Given the criticality of Cybersecurity in India's economy, governance and national security, there is a need for comprehensive cybersecurity policy. Discuss.



Watch Video At:

https://youtu.be/IbAT-A6iRAA

This editorial is based on **“Undesirable acquittal”** which was published in The Hindu on June 24th, 2020. Now watch on our Youtube channel.