If the ancestors of human beings were to wake up today after their long sleep of centuries, they would be amazed to see the revolutionised and digitalised world of contemporary times. The advent of digitalisation has affected every sphere and effect of human lives to a considerable extent that it has conquered time and space. However, the use of information technology like a double-edged sword has been proven onerous for a plethora of people as there has been a colossal surge in the magnitude of threats and crimes related to cyber security. A report titled; “Global Information Security Survey (GISS)” released by Ernest Young claims that one of the highest numbers of cyber security threats have been detected in India and India ranks second in terms of targeted attacks. The need of the hour is to boost up the infrastructure potent enough to deal with potential threats related to cybersecurity as a preventive measure.

Cyber security denotes the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack and unauthorised access aimed at exploiting. In the last couple of years, India has traversed on the path of digitalising its various economic factors and has carved a niche for itself successfully. With the advent of digitalisation, paramount consumer and citizen data will be stored in digital format and transactions are likely to be carried out online which makes India a breeding ground for potential hackers and cyber-criminals.

The number of people having access to the Internet in India has been witnessing an unprecedented surge and owing to it, India has become the second-largest online market worldwide. The use of the Internet has been increasing which poses’ major threat to information-technology security issues. Various threats have emerged such as Cyber Terrorism, Cyber Warfare, digital data threat etc. Terrorists create violence premediate cyber terrorism which tends to be a politically motivated attack against information and computer systems. With an increase in online transactions, cybercriminals look for various loopholes to mine data so that intellectual property can be created. Sometimes some nation-states in order to suffice their ulterior motives tend to damage the information networks of the other nations which are termed as cyber warfare and tend to possess a great threat to the cyberinfrastructure. Due to the existence of many entities in the domain of information technology, there is a lack of coordination between them due to which infrastructure gets prone to various cyber-attacks. Cyberwars, cyber -crimes and cyber terrorism constitute the three main components of the threats related to cyber security. Coming to the cyberwar which can be referred to as the “no contact war”, poses a great threat to security concerns as this term implies to attack the Critical Information (CI) Architecture of other states. The use of cyberspace for committing identity thefts and financial fraud are very rampant and come into the category of cybercrime.

Image source: Medium

Though India lacks laws on privacy and measures to ensure the protection of data, however, there are various other proxy laws and indirect laws which provide adequate safety standards to avoid any mishap. National Informatics Centre which was established in 1976, has played a pivotal role in steering Information and Communication (ICT) Applications in government departments at the centre, states and districts facilitating improvement in the services provided by the government, ensuring greater transparency in the functioning of the government and to ensure certain improvements in the decentralised planning and management.

The Indian National Security Council which is headed by National Security Advisor plays a key role in shaping the ecosystem related to the cyber policy. Apart from this, National Information Board headed by National Security Advisor is the apex body for cross-ministry coordination on policy formulation regarded India’s cybersecurity concerns. The National Cyber Security Policy formulated in the year 2013, has been quite instrumental to build secure and resilient cyberspace in order to prevent theft of crucial information.

National Technical Research Organisation which is short for NRTO has been designed in

order to prevent national critical infrastructure and to handle cybersecurity incidents in the critical sectors of the country. NCIIPC which stands for the National Critical Information Infrastructure Protection Centre has been established under NRTO in 2014 to facilitate the protection of the critical infrastructure. The Indian **Computer Emergency Response Team (CERT-In)** has been delegated the responsibility of tracing several alerts regarding cybersecurity breaches and issues. Indian Cyber Crime Coordination Centre (I4C) has been rolled out to handle several issues regarding cybercrime in a comprehensive and coordinated manner.

"**Cyber Crime Volunteers"** is the recently launched initiative by the Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs (MHA) which has an aim to allow citizens to register themselves as "**Cyber Crime Volunteers'**. The Government has launched the online cybercrime reporting portal, cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit content. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programs and free tools to remove such programs.

Image source: Getty

However, despite several attempts to build up a concrete infrastructural set-up, there have been various loopholes such as the lack of coordination, overlapping responsibilities, lack of clear institutional boundaries and responsibility etc, certain logs emancipate which possess a great threat to the safeguard measures taken in the realm of the information technology. Apart from that, there is a need to articulate a proper doctrine that holistically covers the approach to deal with cyber conflict either for conducting offensive cyber operations or the extent and scope of countermeasures against cyber-attacks. The need for a credible cyber deterrence strategy cannot be overemphasized as the absence of the same denotes that states and non-state actors are incentivized to undertake low-scale cyber operations for a variety of purposes such as cybercrime, espionage etc.

The need of the hour is to devise a clearer strategy and ensure transparency in order to improvise upon the cybersecurity posture. Improved coordination between the various entities dealing with the threats to cybersecurity is of utmost importance. A clear public posture on cyber defence and warfare boosts citizen confidence, helps build trust among allies, and signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem. A key opportunity herein is a precise articulation of how international law applies to cyberspace, which could mould the global governance debate to further India’s strategic interests and capabilities. n particular, this should include positioning on not just non-binding norms but also legal obligations on ‘red lines’ with respect to cyberspace targets that should be considered illegitimate due to their significance for human life, such as healthcare systems, electricity grids, water supply, and financial systems. As India is moving towards more and more digitalization in all spheres, cyberspace has become a serious concern of National Security. Thus, a comprehensive policy with a skilled workforce is needed to ensure that India’s people and its infrastructure are safe, so the country can move towards development peacefully.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments