China's rapid improvements and development of cyber warfare capabilities in expertise, institution building, and offensive ability is remarkable. China is rapidly building its cyber capabilities to use its cyber tools in military operations. The Belfer Centre's National Cyber Power Index of 2022 has described China as the second-most comprehensive cyber power, next to the United States. The inclusion of the Strategic Support Force into the People's Liberation Army (PLA) in 2015 elevated China's dream to become a dominant cyber superpower by 2025. The Chines military views cyber warfare as a preventive measure of conventional military operations. It also uses cyber espionage techniques to recognize weaknesses in its adversary's critical infrastructures that could be manipulated in wartime. With this objective in mind, China introduced several cyber institutions to its armed forces, namely the 3rd Department of Peoples' Liberation Army (PLA), whichis accountable for Computer Network Defence (CND), Signal Intelligence (SIGINT), and Computer Network Exploitation (CNE). The 4th Department is responsible for Electronic Warfare, Integrated Network Electronic Warfare (INEW), and Computer Network Attacks (CNA). The Strategic Support Force (SSF) integrates intelligence, communications, and electronic warfare with cyber warfare to build an integrated information warfare force. China follows a"Whole of Nation" approach to building the cyber warfare and espionage ecosystem, including several patriotic hacker groups, university students as cyber warriors, and private telecommunication firms like Huawei and ZTE in conjunction with the PLA. These expanding cyber capabilities became a threat to India.

Implications for Deterring Cyber Threats

In the year 2021, Indian Computer Emergency Response Team (CERT-In) addressed 1402809 incidents. In comparison, in 2020, CERT-In reported 1158208 incidents. In India, there needs to be an effective cyber security environment, organization integration, and offensive capability. And the increase in computer and telecommunication hardware, as well as mobile phones, especially from China, has supplemented vulnerabilities to a notable degree. Keeping in mind, India needs to develop a cyber security strategy and capacity building for effective defense against cyber threats.

The sections below discuss mechanisms for effectively deterring cyber threats at the institutional level and the initiatives.

Need for a Systematic Cyber Security Strategy:

According to many experts, India requires developing a systematic cyber security strategy

to effectively deter cyber threats conventional deterrence is still regarded as a crucial component of the national system. In cyberspace, there are multiple ways to conduct warfare, malware, data theft, phishing, DoS attacks, zero-day exploits, ransomware, espionage, and disruption of a country's vital infrastructure are the typical forms of cyber-attacks. Unfortunately, it is practically challenging to defend all of them. Hence a well-defined plan must be needed to develop a national strategy to deter cyber threats. According to Lt. General Deependar Singh Hodda, the first and the most important strategy would be to identify the cyber dangers that could jeopardize national security, attacks that include damage to critical infrastructure, and compromise critical data and attempts to undermine trust in the government or creates massive public risk. Secondly, a response should focus on state-backed attacks rather than individual attackers or non-state actors like terrorist groups, given the increasing number of state-sponsored attacks these days. Thirdly, a national strategy must be developed to combat intellectual property along the boundaries of defense, high technology, and health. Like, for example the Chinese attack on two of India's vaccine manufacturers, Bharat Biotech and the Serum Institute of India (SII)19 and tried to steal the intellectual property secret of AstraZeneca and the Covishild vaccine and other vital information. Government intervention and support should be expanded to cyber-attacks on private commercial bodies. Private companies control some critical infrastructures in India and maintain most public data.

There are, however, difficulties too. The most challenging issue is identification. Nations must be clear about who is behind a cyber-attack so their countermeasures are understood or misguided. This isn't easy because, in cyberspace, spoofing locations and identities is very easy. The multidimensional nature of cyberspace also allows the launching of an attack from any geographical area. False flags could also be used to misdirect for identification of attackers. Even after identification proving that they are state-sponsored is very difficult because of the deniability factor. Another challenge to cyber deterrence is the state's secretive behaviour regarding its cyber capabilities. Nuclear and conventional deterrence worked because the capabilities and the destructive potential of each side were known. Contrary to this, cyber capabilities are yet to be explored, and nations are very secretive about their capabilities and their setups.

Image source: Cyber News

There are two particular methods of deterrence suggested by scholars. Firstly, deterrence through denial denotes reducing vulnerabilities and solidifying critical infrastructure to the extent that the adversary finds it too difficult to attack and causes little outcome. In this process indigenization is the most practical way forward. Deterrence through denial also includes proactive threat detection, frequent inspections of vital networks to check if they have been compromised, rapid threat mitigation, and better information collection. Secondly, there is deterrence through punishment aims to deter an adversary from engaging in unsuitable activity by threatening to impose severe penalties. Also, a nation should always respond the attacks which is a direct threat to its national security. This reaction should not be limited to cyberspace but involves kinetic military actions with other diplomatic, economic, and legal measures.

India must work on identification capabilities to improve the nation's cyber security. It would also be crucial to increase the amount of information-sharing and real-time threat detection among various government institutions, academia, and industries. As mentioned, one of the most significant challenges to cyber deterrence is the difficulty of identification. Thus, collective action by all specialized agencies and the developing advanced competencies in cyber forensics will be appreciable. For instance, in the case of RedEcho's power sector attack in Maharashtra, the process of identification and notification to the specialized authorities got delayed. Thus, attribution becomes Problematic. After creating a landscape of information sharing and protecting even civil users from cyber-attacks, India can relegate cyber weapons to the role of a deterrent.

Policy and Doctrine:

India still needs a comprehensive, modern, and updated cyber warfare strategy. India is in the final stages of clearing a National Cybersecurity Strategy, 2020 conceptualized by the Data Security Council of India (DSCI) and has a National Cybersecurity Policy, 2013. These, yet, do not discuss armed conflict or active espionage. According to Scholars, India only addresses cybersecurity attacks and not cyber warfare. The concern is over the importance of civil and military data rather than technology in actual combat and the need to adjust the current view of cybersecurity from a state of espionage to cyber warfare that can be used to harm in case of active war. The current cybersecurity regulations in India avoid questioning the importance of cyber warfare and the necessity of cyber weapons. India views cyber security through a civil lens in the context of financial resilience and protection. India must develop a strategy that discusses two philosophies of thought mentioned earlier, cyber strategy for offense and defense. India must combine the two in a strategy focusing on deterrence. India's current strategy adopts a reactionary "whack-a-mole" approach rather than forming deterrence. India must toughen its targets and aim primarily at state-sponsored attacks through cyberwarfare strategies. In contrast, cybersecurity strategies will continue to concentrate on non-state data breaches.

Image source: Pinterest

Government Agencies in Cyberwarfare Deterrence:

The cyber command-and-control structure in India has progressed since the early 2000s but stays decentralized, not integrated, and operates independently. Overlapping competencies, bureaucratic turf, and the federal political system complicate the situation more. For smooth coordination, a policy-making and coordinating agency needs to be established. The National Technical Research Organisation (NTRO), which is the apex Cyber agency of the nation, was set up in 2004 and modelled on the U.S. National Security Agency, it reports to the national security advisor and is tasked with technical intelligence-gathering, signals interception and influence operations. National Critical Information Infrastructure Protection Centre (NCIIPC) was founded in 2014 under the direction of the NTRO, In 2003 the government set up a national Computer Emergency Response Team (CERT-In) which functions under the Ministry of Electronics and Information Technology which played significant role tracking and monitoring cyber incidents across all the sector including government and private sectors. National Cyber Coordination Centre (NCCC), subordinate

to CERT-In, finally began operations in 2018. The NCCC is responsible for intelligence-sharing between government agencies and for coordinating government responses to cyber-attacks. In May 2021, India set up its Defence Cyber Agency (DCA). The DCA operates closely with National Technological Research Organisation, India's Research and Analysis Wing, National Security Council, and the Defence Research and Development Organisation. Further, there are a number of other agencies that deal with cyber security issues under the central government. For Example, Defence Information Assurance and Research Agency, which is now merged with the DCA, Defence Intelligence Agency, and the Defence Space Research Agency etc.

Although the current government has made some organisational changes, there are no task forces focused on the conduct of Offensive Cyber Operations (OCOs). It is rumoured that the DCA, which falls under the Integrated Defence Staff (IDS), is capable of hacking into networks, mounting surveillance operations, and laying honey traps. But cannot pursue integrated OCO-related missions because of the existence of too many organisation, and it does not have any independent command authority. Nor does it perform the same functions as United States USCYBERCOM, whose main motto is to direct, synchronize, coordinate and plan cyber operations in cyberspace. The DCA is primarily a tri-service agency geared to extending training support and technical advice to each individual service. Thus, all the agencies need to be converged under a single unified service and command organisation comparable to United States Cyber Command (USCYBERCOM) or the Chinese People's Liberation Army Strategic Support Force (PLASSF). Although service-specific cyber capabilities should exist, an integrated and unified organisation will allow better coordination and execution of offensive cyber operations.


Image source: Asia Military Review

Need for Trained Personnel:

India, especially the military does not retain an adequate number of well-trained personnel for the conduct of offensive cyber operations. Skilled cyber security expert is the backbone of a country's cyber strength. The total strength of cyber security experts deployed in different government agencies of the government is a sheer 550 compared to more than 100'000 in China, 91,000 in the USA, and 7000 in Russia. According to many scholars, thus recruiting experts from the civilian domain is essential. If the armed services were to recruit from the civilian sphere, these experts must imbibe some of the military demands for launching a specific objective and mission. The benefit of having civilian experts is their technical expertise. They also give the Indian state cover in the form of deniability and anonymity. They can prepare and launch offensive operations based on operational needs and develop malicious code or malware, which can infiltrate networks of adversaries.

Leveraging the Strength of India's IT Ecosystem:

India has substantial strength in the field of computer software and Information Technology (IT), but its reservoir of human and technical capital in this sector remains untapped. It is concentrated heavily in the private and civilian sectors. Since India's offensive capabilities

are generally weak against China. Thus, leveraging private sector expertise is imperative. India has that potential, India is one of the biggest I.T. powerhouses, and as per the National Association of Software and Services Companies, NASSCOM IT industry revenue is estimated to grow 15.5 percent in the financial year 2021-22, 227 billion U.S. dollars from 196 billion dollars in 2020-21. Indian I.T. industry is estimated to directly employ nearly 51 lakh people with an additional 4 lakh 45 thousand people during the 2021-22 financial year.

Technological Advancement and Indigenisation:

Technological advancement is also an essential aspect of deterrence. Leaders of China understand the importance of technology in their rivalry for global power and dominance. The Chinese "Made in China (MIC) 2025" aims to convert China into a leading manufacturing power by indigenously developing key high-tech industries like semiconductors, quantum computing, 5G, aerospace technology, and AI etc.This MIC strategy plays an important role in China's ambition to develop the PLA into a "world-class military" by 2049. There is a tremendous first-mover advantage that can set international standards and alter the geopolitical balance. For example, Chinese companies like Huawei, ZTE have already grabbed the lead in 5G technology, with 460 million 5G customers in 2021, accounting for 70% of worldwide users. In addition, China is getting a lot of attention in the fields of A.I. and quantum computing. Stanford University's AI Index ranks China among the top three countries for global AI vibrancy. In economic investment, China accounted for about one-fifth of global private investment allowance in 2021, attracting $17 billion for AI start-ups. China is the primary supplier of semiconductors to all manufacturers worldwide, including American and European brands. China surpassed Taiwan as the world's largest maker of micro conductors.

Electronic devices are the backbone of our world, and semiconductors or microchips are the brains inside I.T. devices, from mobile phones to vehicles to energy grids. However, these critical devices cannot run properly unless the chips are free of weaknesses and security vulnerabilities. And that is becoming an increasingly precarious situation. It is unthinkable to rule out the possibility of unwanted changes in these integrated circuits. Most of our Critical Infrastructures like Power, telecommunications, Transport Infrastructure, Dams, Railway, and government and private institutions is flooded with Chines hardware.

According to the IEEMA database, India's import of electrical equipment has expanded significantly in the last decade, and to make power distribution networks more efficient, several cities in India have granted contracts to Chinese enterprises that represent a threat to the power infrastructure. Similarly, other essential infrastructures such as telecommunications, trains, and irrigation are under severe threat since they rely on

Chinese telecommunications And I.T. hardware. India introduced the Atmanirbhar Bharat initiative for self-reliance in 2020, and while it has had some results, a far stronger push is needed. India's future strategy should emphasize the use of advanced technologies. India is attempting to lessen its reliance on China in terms of technology, especially due to security concerns. Although there are some welcoming measures taken, Power Minister R.K. Singh declared in July 2020 that Indian enterprises would need government clearance to import Chinese power supply equipment and components. In May 2021, the Indian government followed the U.S. position, thereby excluding Chinese businesses such as Huawei and ZTE from participating in 5G trials while preferring foreign companies like Nokia, Samsung, Ericsson, Mavenir, and Cisco including only two Indian companies. Technology reliance has a direct impact on India's ambition for strategic autonomy and greater engagement in global affairs. India is also making steady development in the field of artificial intelligence. A.I. start-ups in the nation attracted a total investment of $1,108 million in 2021, 32.5% growth compared to $836.3 million in 2020.

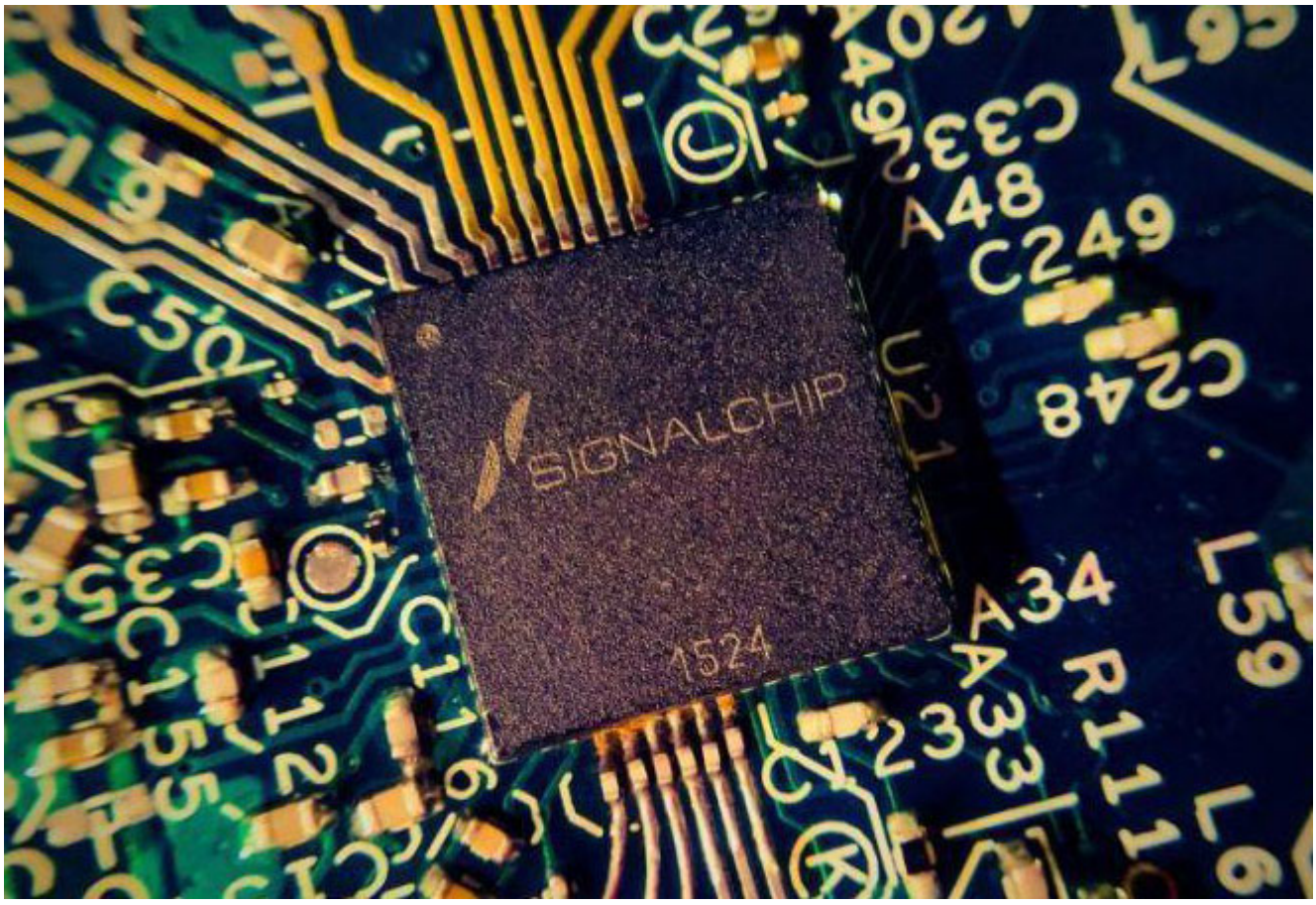

Image source: LinkedIn/ Data Bytes

In the field of semiconducting, The Ministry of Electronics and Information Technology has launched India's Semiconductor Mission, under which India is investing $10 billion to attract semiconductor manufacturers as it seeks to become a major component manufacturing hub. In 2022, the announcement of Taiwanese electronics manufacturer Foxconn and the Indian business giant TATA to set up manufacturing plants to make semiconductors boosted India's expectations, becoming India a semiconductor powerhouse. Even though China is far ahead in semiconductor manufacturing, despite this, two significant investments in India at least got a good kickstart in this area.

India needs to become self-reliant on Hitech technologies. Indigenously manufactured will provide far more security to its Critical Infrastructure and also deliver an economic boost, ultimately boosting the overall strength. If India continues to rely on foreign technologies, it is putting itself at future risk in making independent foreign policy choices.

Initiatives by the Government

Recently the Indian government has been planning to set up a unified national-level cyber security task force to focus on priority sectors concerning the growing attacks on critical infrastructure. It will operate in real-time collaboration with international partners. The task force is expected to work in conjunction with CERT-In. To strengthen India's cyber space, the National Security Council Secretariat arranged the National Cyber Security Incident Response Exercise (NCX India) for government officials and critical sector organizations. For managing financial fraud, the Ministry of Home Affairs also introduced The Citizen Financial Cyber Fraud Reporting and Management System for immediate reporting of financial frauds. Indian government also plans to establish a Computer Security Incident Response Team(CSIRT) to safeguard its power grids from cyberattacks and to counter any attempt to cripple the country's critical power infrastructure with the help of trained professionals and experts from the private sector.

Conclusion

India still needs a comprehensive, modern, and updated cyber warfare strategy and needs to adjust the current view of cybersecurity from a state of espionage to cyber warfare that can be used to harm in case of active war. Hence, it is time for India to start thinking about policies, guidelines, concepts, and doctrines to deal with this potential threat to national security. Even though India has made only modest improvements in developing cyber security capacities, crucial cyber warfare capabilities need to be upgraded to deter cyber threats effectively. India understands the vitality of the situation and is steadily moving forward to achieve those.

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