NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief

No. 989 – 29 December 2022

Going on the Offensive: India's Cyber Capabilities

Karthik Nachiappan

Summary

India needs to bolster its offensive cyber capabilities to deal with a barrage of state and non-state threats.

Despite clear and growing regional geopolitical instabilities and a keen awareness of the wide range of cyber threats it confronts, India has yet to develop a coherent cybersecurity strategy and doctrine. Cyber-attacks by India's adversaries, namely, China and Pakistan, have risen as strategic competition intensifies in South Asia and the Indo-Pacific. Both state and non-state actors have been targetting India's critical infrastructures like nuclear plants, energy grids, telecommunication systems, hospitals and financial institutions through cyber-attacks. There's speculation that China and Pakistan are coordinating their cyber activities to disrupt and damage India's critical sectors, most recently, during the post-Galwan crisis when Indian security agencies were on high alert.

Generally, India's approach to cyberspace has been cautious and slow, working gradually and in piecemeal – identifying cyber risks and threats, establishing institutions and policies, and using diplomacy to guard against rules that constrain its domestic powers. India's cyber agencies, especially the National Technical Research Organization and the Computer Emergency Response Team, work closely with diplomatic partners like the United States to bolster domestic cyber defence and resilience. India's cyber response is primarily governed by the 2008 Information Technology Amendment Act and cyber responsibilities that are spread across a litany of national and state agencies. This fragmentation has constrained India's cyber preparedness and stymied the growth of a partnership between the government and the private sector. As a result, the overall cyber approach has largely been defensive and domestic, focusing on fixing internal gaps before heading out to counter foreign threats.

Yet, the time to shift India's cyber approach and adopt an offensive mindset and posture may have arrived as threats proliferate. To be sure, an offensive cyber strategy does not rule out bolstering domestic preparedness; essentially, this approach allows India to proactively identify and eliminate various cyber threats before they hit Indian targets. What are offensive cyber operations? These operations are conducted by nation states using digital tools and instruments to negate and eliminate cyber threats, whether state or non-state. Often, these operations are conducted in partnership with private sector firms with better knowledge of the tools used. Offensive cyber operations vary from using software to disrupt critical physical infrastructures like power grids and ports to malware that targets dissidents or journalists or ransomware that demands payment to return data. Some cyber operations are designed to seek domestic influence or sabotage an adversary. So far, there is no available evidence that indicates India has integrated offensive cyber operations into its

arsenal but conditions do exist for India to adopt an offensive strategy to deal with cyber threats, especially from China and Pakistan.

Generally, states must have the adequate physical infrastructure to adopt an offensive cyber strategy, specifically sufficient intelligence, surveillance and reconnaissance (ISR) capabilities. These ISR capabilities must be ubiquitous, real-time, persistent and capable of executing a strike when necessary. Currently, India is in the process of transforming its ISR structure which consists of information-gathering satellites, airborne platforms and ground-based sensors that facilitate cyber operations. However, these systems and technologies must be integrated and deployed for cyber purposes. Second, states need a cyber institution or agency that manages, runs and executes cyber operations. In 2021, India established the Defense Cyber Agency, which appears to resemble a cyber command that can undertake offensive cyber operations, hack and disrupt networks and mount surveillance operations. Additionally, the office of the National Cyber Security Coordinator, launched in 2015, can help synchronise efforts among various government agencies tasked with cyber responsibilities.

Moreover, states have to work with their private sectors to develop a viable offensive cyber operations structure, given their ability to significantly influence the nature, execution and success of cyber operations. India has a robust and dynamic information technology sector that can support its cyber operations. The country also has clear strengths in the digital economy that includes a vibrant start-up culture and a large talent base whose talents can be harnessed. In addition, the private sector has moved more quickly than the government in promoting national cyber security, which gives Delhi a potential advantage.

India has the necessary institutional conditions including infrastructure, cyber agency and private sector expertise to adopt a viable offensive cyber approach. However, it lacks one fundamental aspect that could affect its ability to conduct offensive cyber operations abroad – a cybersecurity strategy. A reliable and resolute cybersecurity strategy is imperative for providing a framework that organises and executes responses to India's cyber threats. This framework safeguards India's cyber strategy, whether offensive or defensive, allocates financing to implement that strategy, including investments in areas like the ISR, and identifies pathways where the private sector can contribute, if necessary. It provides a roadmap to protect and defend your cyberspace. A strategy also allows India to adopt the requisite approach and measures to counter and deter rising digital threats. Delays in finalising this strategy effectively leave India vulnerable to an era defined by manifest cyber risks and not by pursuing them openly abroad.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.