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

ISAS Brief
No. 851 – 22 July 2021

India as a Muddling Cyber-Power

Karthik Nachiappan and Nishant Rajeev

Summary

A recent report by the International Institute for Strategic Studies assesses and ranks the cyber-capabilities of 15 different countries. India has been ranked as a tier three or lowest tier country. While the report notes some positives while assessing India, such as a vigilant private sector in cybersecurity matters, it highlights a siloed and fragmented government approach that dents India's cyber resilience.

State of India's Cybersecurity

A recent report by the International Institute for Strategic Studies (IISS) assessed the cyber capabilities of major states and their impact on international security, economic interdependence and military competition. Cyber capabilities were assessed based on seven components – presence of a cyber strategy and doctrine; cyber governance structures, specifically command and control; cyber-intelligence capabilities; cyber empowerment and dependence; cyber security and resilience; leadership in cyberspace cooperation; and offensive cyber capabilities. The report divided 15 states based on these assessments into three tiers. The first tier, for states that fared well across all categories, consisted of just the United States. The second tier included states that fared well in some, not all categories. And finally, the third tier consisted of states that had strengths in certain categories but weaknesses in others. India was included in the third tier. The report claims that India had made "modest progress" in developing policies and doctrine to enhance cybersecurity and that its broader approach towards reforming cyber governance has been slow and piecemeal. India, however, fared well when it came to cyber-intelligence capabilities despite "relying on partners like the United States" and pushed above its weight in cyber diplomacy despite doubts about promoting cyber norms. The report also lauded India's private sector as being more aware and vigilant concerning cybersecurity.

In terms of assessment, it is unclear whether the context around cybersecurity was accounted for when making judgments on India's cyber capabilities. Unlike other states, India exists in a difficult cyber context, constantly besieged by attacks from rivals and adversaries. It is no stranger to cyberattacks having reported 1.16 million cyberattacks in 2020 alone. Hackers have targetted India's critical infrastructure installations like its nuclear power plants and its electric grid. Cyber policymaking is not unfolding in a vacuum; instead, it involves multiple agencies and institutions, including those that have historically not dealt with cyber issues. A diffused landscape exists. The National Critical Information Infrastructure Protection Centre and the Computer Emergency Response Teams- India (CERT-In) are responsible for protecting the country against national cyberthreats. Several state level CERT-In teams have also been operationalised. The National Technical Research Organisation was created to assist in intelligence collection. The Prime Minister's Office also hosts a National Cyber Security Coordinator who is responsible for coordinating cyber

matters between various agencies. Cyber issues have also been increasingly reflected in strategy documents of the Indian armed forces. The Joint Doctrine of the Indian Armed Forces and Land Warfare Doctrine both place emphasis on developing and maintaining relevant cyber warfare capabilities to deter, defend and disrupt an opponent's cyber operations. This diffuse landscape has constrained India's cyber capabilities.

That said, India does have severe vulnerabilities on cybersecurity that require more attention. While several institutions governing cyberspace exist, their practical operation, specifically coordination, has been lacklustre. As noted in the IISS report covering India, "cyber-security powers are spread across a number of agencies, with reports of overlapping competencies and bureaucratic turf wars. The situation is further complicated by the country's federal political structure." This fragmented approach has blunted the effectiveness of the government's responses to cyberattacks, especially those that target vital systems like nuclear plants. Furthermore, India is still heavily reliant on imported equipment to build its digital ecosystems. Foreign hardware continues to form the backbone of India's digital infrastructure. Much of the country's existing telecommunication infrastructure continues to be dependent on foreign vendors like Nokia, Samsung and Huawei; the mobile handset market is also controlled by Chinese manufacturers. These imported systems may be less reliable than equipment developed domestically.

Looking Ahead

Protecting domestic infrastructures against cyberattacks is proving to be a stiff challenge for countries worldwide. Unlike most major powers, however, India has a long way to go to secure its digital landscape, a point that was underscored by this recent report. There exists some hope that India's cyber architecture will be better prepared to confront and foil threats from 2022 once the national cybersecurity strategy is finalised and the personal data protection bill is passed. Like the General Data Protection Regulation, India's data protection bill includes a provision that allows for fines to be imposed on firms and companies that do not promptly report cyberattacks. Recent cyberattacks have been increasingly sophisticated and have exploited vulnerabilities along the entire cyber-supply chain. Hence, a clear cybersecurity strategy should also clarify responsibilities of key cyber institutions. India's private sector, especially firms in the financial, telecommunication and energy sectors, have to bolster networks to fend off ransomware attacks while being prepared for related state-backed advanced persistent threats. Thus, 2022 will be a critical year for India's cybersecurity.

. . . . .

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. Mr Nishant Rajeev is a Research Analyst at the same institute. He can be contacted at isasnr@nus.edu.sg. The authors bear full responsibility for the facts cited and opinions expressed in this paper.