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

ISAS Brief
No. 1200 – 27 January 2025

India's Cyber Statecraft: Managing and Neutralising Threats

Karthik Nachiappan

Summary

India needs to practice cyber statecraft to manage, deter and neutralise prevailing and rising digital threats.

Cybersecurity is critical to India's economic future, especially given the strength and position of its digital economy. The bulk of India's economy is services, different kinds of information technology and computing services. In effect, India has a thriving services economy that is internally organised through various digital applications and services which allow Indian citizens to communicate, transact and receive subsidies, including other services. And this massive and growing digital economy and digital ecosystem relies on cybersecurity. Are India's cyber defences robust enough to protect this system from cyber risks and threats? And how should India diplomatically defend its digital economy given cyber challenges?

India's cyberspace is increasingly becoming an arena of security competition with specific adversaries, specifically China and Pakistan becoming sources of cyber-attacks with support from other kinds of non-state actors – these actors see India's vast digital apparatus as a surface and layer to target and destabilise to advance geopolitical objectives. Both China and Pakistan have rivalries with India which is increasingly acquiring a digital character. Also, India's cybersecurity policies (and related areas like data and artificial intelligence) are being taken with an eye on these security concerns, particularly threats emanating from hotspots like China. So cyber issues are now highly securitised in India, which will have implications for policies and diplomacy.

What threats dominate India's cyberspace? India faces several dynamic threats online. A range of different internal and external security threats have now been mapped onto the cyber area. India is amongst states that receive the most cyberattacks, especially state-sponsored cyber-attacks which have increased. According to the 2023 India Threat Landscape Report, India is the most targeted country globally, facing 13.7 per cent of all cyber-attacks. Microsoft claims that India ranks within the top five in terms of the number of cyberattacks received.

Most of these attacks target state and government agencies that have gone up substantially since 2021, and most of these attacks involve malware, with nefarious actors trying to extract specific information and data (including intellectual property) out of that organisation. These attacks prove that India's digital ecosystem is not secure enough and porous, leaving itself vulnerable to different kinds of threats. In effect, India is a victim of its success – a successful state in terms of digitalisation which opens itself to new threats that are moving faster than the pace of digitalisation.

Cyber, as a result, becomes an important aspect of India's diplomacy to deal with and mitigate such digital threats. India's ties with countries like the United States (US), the European Union, Singapore, Japan and the Association of Southeast Asian Nations will feature a heavy digital and cyber component as these economies integrate with India digitally. India's digital interests make it a part of an exclusive economic club (G7, Organisation for Economic Co-operation and Development and the G20 economies) where it will have to act differently than it does through bodies like the G77. What does this mean?

India's digital trade policies and positions, cyber being a key aspect, will have to evolve and keep pace with major economies through a focus on digital rules and standards. Some coordination has occurred. To digitally converge with these economies and strategic partners, India will have to straddle different identities and divides when discussing cyber issues.

The rapid growth of India's information and communication technologies sector and the potential for threats that affect its functioning generate a dangerous situation. In this evolving digital landscape, New Delhi does not have full control over what transpires in its cyberspace. Diplomacy is and will form a key part of protecting India's digital future. India's cybersecurity policies are robust and resolute at the international level where efforts are being made to strengthen digital sovereignty and give states the power to handle and manage cyber threats. Domestically, however, India's efforts lag which is now compelling the private sector to tackle and deter the kinds of threats faced online. The impact and effects of China's cyber-attacks against India are compelling India to work with partners like the US to strengthen cyber defence.

Cyber diplomacy is necessary but not sufficient. Given the range of risks India faces online, it is critical and consequential for New Delhi to also modernise, streamline and integrate cyber efforts to deter rising cyber threats, effectively organise its cyber institutions and protect its teeming digital ecosystem. Yet, New Delhi faces difficulties – internal and external – to execute this seemingly thorny digital transition. India needs cyber statecraft: a strong sober cyber strategy with institutions and policies that reflect, advance and protect the country's digital interests.

. . . . .

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.