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

ISAS Brief
No. 698 – 6 September 2019

India's New Cybersecurity Policy

Karthik Nachiappan

Summary

The Narendra Modi government is revamping India's cybersecurity policy in early 2020. The new policy targets growing security and economic challenges posed by the internet, particularly cyberattacks on both government and businesses. The quickening pace of digitisation across the economy covering existing and new sectors makes this announcement timely. A new policy should improve institutional functioning around cyber issues, ironing out details related to cyber coordination and accountability.

In early 2020, India's new cybersecurity policy will be unveiled. The policy will upgrade the 2013 cybersecurity policy with a cost of ₹250 billion (S$5.5 billion). The 2020 policy is largely driven by two developments – rising security and economic challenges from internet activity and a need to fortify the institutional landscape around the internet to fill existing gaps and manage new problems.

Security risks have necessitated a rethink in India's cybersecurity policy. The growing number of attacks from adversaries, state and non-state, have ratcheted concerns. According to the Data Security Council of India, India experienced the second highest number of cyberattacks worldwide from 2016 to 2018. More concerning for New Delhi is the speed with which such cyber breaches are occurring; when attacks manifest in various forms (malwares, worms, viruses, phishing, etc.), it makes them harder to defuse and thwart. Alarmingly, 35 per cent of attacks on Indian networks were allegedly attributed to China; these cross-border cyber incursions are driven by a need to access sensitive government and private sector information. Costs borne from breaches are mounting. Chinese cyberattacks have disrupted computer and communications networks through worms, malware and other phishing mechanisms. Some cyberattacks occur after major political or foreign policy announcements, for instance, cyberattacks have spiked since the Modi government revoked Article 370A which granted special status for Kashmir. Cyber experts claim India's government agencies are (and have been) particularly soft targets for hackers which calls for sustained focus to nullify attacks. The establishment of a new defence cyber agency in May 2019 could augment the Indian military's cyber capabilities, particularly shoring up cyber deterrence.

Security aside, the Indian economy's swift digitisation demands a robust responsive cyber framework to service and protect its development. Announcing the new policy, Rajesh Pant, India's National Cybersecurity Coordinator, underscored the economic potential of an updated policy framework. Enhancing cybersecurity found new importance once the Indian government introduced 'Digital India in 2015' which intends to fuel the digital delivery of services. The campaign triggered major investments into digital industries which has, unsurprisingly, unleashed a barrage of concerns around data protection. Barring a new data law, the only recourse to these queries is existing cybersecurity provisions. In addition, the rapid growth and use of digital technologies to transfer money, eased by platforms like Aadhar, has amplified cybersecurity concerns. The growth of India's digital economy coupled with the digitisation of untapped industries, like agriculture, education, energy and logistics, enables entrepreneurs and regulators to securitize operations at the outset. A digital ecosystem with effective safeguards should catalyse services, jobs and applications for Indian citizens, propelling digital interactions.

Critically, secure cyber systems and clear rules place fewer financial burdens on businesses. To limit the costs of cyberattacks, financial and operational, Indian firms in sectors like retail, banking, insurance, utilities, and telecommunications are deploying artificial intelligence (AI) tools. Two out of three large businesses in India are considering using AI to defend their digital platforms and services. Fortuitously, data harvested from Indian customers facilitates the development of AI techniques to combat cyberattacks that cannot be neutralized quickly. Deep learning techniques, pioneered through AI, facilitates the prediction, identification and prevention of cyberattacks. Sustained interactions between the government and private sector on cyber issues will empower the latter to demonstrate how technological solutions like AI can root out emergent cyber risks. AI's rapidity helps tackle a complex array of cyber threats.

Institutionally, it is time to bolster India's cyber-infrastructure. A new cyber policy could concentrate the focus, boosting coordination between various cyber regulators. Indeed, demands posed by security and economic challenges flagged above leave Indian officials with little choice. Currently, an inadequate set of statutes govern cybersecurity in India. The Indian government relies on the 2008 Information Technology (IT) Act, itself an update of the 2000 IT Act, to prevent cybercrime issues like hacking, cyberterrorism, cyber theft and disruptions to digital commerce. In 2013, then-IT Minister Kapil Sibal introduced a National Cybersecurity Policy that established a framework to manage problems emanating from the proliferation of online transactions, particularly the protection of personal information and cyberattacks. Then in June 2019, New Delhi established a cybercrime coordination unit to act as the nodal point against cybercrime. Cyber issues, necessarily, are a multi-agency affair and responsibility. A new cyber policy should enhance inter-agency coordination, establish clear accountability guidelines, set rules for public-private collaboration on cyber issues and raise cyber awareness. A diffused cyber architecture dents cybersecurity.

The new cybersecurity policy appears at a critical juncture with India's economic potential hinging on digitisation and the ability to deter emergent cyber threats. Questions concerning the security of online platforms will rise and fester if left unaddressed. The new policy should allow some questions to be answered.

. . . . .

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