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

ISAS Brief
No. 722 – 15 November 2019

India's New Cybersecurity Institution: Ensuring a Robust Cybersecurity Posture

Karthik Nachiappan

Summary

The recent cyber-attack on the Kudankulam nuclear power plant has compelled the Indian government to restructure institutional structures managing cybersecurity. A unified cybersecurity agency is expected to be unveiled soon to manage and deter rising cyberattacks against Indian ministries and private firms. A centralised institution focused on thwarting cyberattacks could add coherence to India's positions with respect to global cyberspace rules and norms that is diffident and vague.

A few weeks ago, the Kudankulam Nuclear Power Plant in Tamil Nadu suffered a serious cyber-attack. Reporting revealed that a malware infected personal computer breached India's largest nuclear power facility's administrative network. Additional reporting indicated that, besides Kudankulam, hackers were also targeting the Indian Space Research Organisation as it was working on its moon mission though such claims have been denied. Kudankulam, however, points to a larger problem that must be addressed in terms of India's internet governance – clarifying the institutions responsible for managing and addressing rising cyber threats which could then influence and inform India's response with respect to rules governing cyberspace that remain diffident and restrained.

India's institutional apparatus on cybersecurity is diffuse and fragmented. Several ministries and agencies manage cybersecurity. The Ministry of Electronics and Information Technology (MEITY), Ministry of Home Affairs (MHA), Ministry of Defence, the National Security Council Secretariat and the National Technical Research Organisation have their own cybersecurity units. Additional specialised units include the Computer Emergency Response Tea, the National Critical Information Infrastructure and the National Cyber Coordination Centre. Alongside these agencies, several new ones are emerging – the MHA recently launched CyCord or Cyber Cooperation Centre that serves as an inter-agency platform under the remit of the Intelligence Bureau. CyCord joins other MHA agencies like the National Cybercrime Threat Analytics Unit, the Platform for Joint Cybercrime Investigation Team, the National Cybercrime Forensic Laboratory and the Cybercrime Ecosystem Management Unit. In addition, the National Critical Information Infrastructure Protection Centre is responsible for protecting assets in sensitive sectors such as defense, finance, energy, and telecommunications. Difficulties surrounding coordination in the wake of constant barrage of cyber-attacks appears to have compelled Delhi to merge these agencies under one remit to better protect India's digital infrastructures.

Soon, India may have a unified cyberspace agency that governs defensive cyber operations. The panoply of agencies managing cyber issues, mentioned above, should fall under this new agency to deter cyber threats. Coordination and communication is a big priority with this restructuring but so is the demand to centralise individual control and reporting systems as threats accumulate. Some of these changes were introduced when New Delhi unveiled its new

cybersecurity policy in August this year which will take effect from 2020. Kudankulam has hastened the necessary institutional revamping that will require cabinet assent before implementation. Command and control has risen as a policy priority in cyberspace. With this move, India positions itself to better confront and deter cyber-attacks, given enhanced information sharing between various sectoral agencies. Yet, one potential hurdle to effective cyber governance is the role of MEITY that must cede certain powers to the newly proposed agency. Currently, MEITY is the regulator of the Information Technology Act and cyber communications. Jurisdictional concerns and constraints must be resolved.

A coherent and coordinated cybersecurity approach at home emboldens India while working to shape global rules governing cyberspace behaviour. As of now, the global cybersecurity space is in flux; fragmentation reigns. Advanced economies like the United States (US), the European Union and Japan prefer an unfettered cyberspace with limited constraints while states like China and Russia desire an interventionist approach where the state determines rules on how people and firms behave online and platforms on which they do. India could tread a narrow path to ground a third way that borrows from these approaches. Yet, India has been unwilling to stake a claim on global cybersecurity rules, largely due to domestic policy incoherence.

A fragmented institutional landscape with respect to cybersecurity has muddled India's positions on cyber governance. Till now, India has not unveiled a clear position regarding responsible state behaviour in cyberspace. The United Nations (UN) has been the forum where most states prefer to negotiate a normative framework for cyberspace which was then transferred to the Group of Governmental Experts (GGE). In 2015, the GGE identified 11 cyber norms for countries to secure cyberspace that included desisting from cyber-attacks and greater information sharing on nefarious use of cyber technologies. At GGE debates, Indian officials have highlighted the security and developmental aspects of cybersecurity that mirrored the work done on the cyber issue at the UN General Assembly. Stark differences between some UN permanent member states – the US, Russia and China – on how to regulate cyberspace have hamstrung the GGE process; discord has stymied the GGE which then broke down in 2017 amidst disputes over what principles should cyberspace rules be weaved around.

A global vacuum on cybersecurity rules does not augur well for India given discernible institutional gaps with respect to cybersecurity. Other countries could step in and fill this void. Unless India bolsters its domestic cyber-infrastructure, the global positions it takes will be anodyne, broad and not targeted at preventing rising cyber-attacks. A more robust cybersecurity posture could reveal India's strategy when it comes to both defensive and offensive cyber operations to thwart adversaries. Simply put, a new unified cybersecurity agency could better inform and reinforce India's hand vis-à-vis the global governance of cyberspace.

. . . .

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.