ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

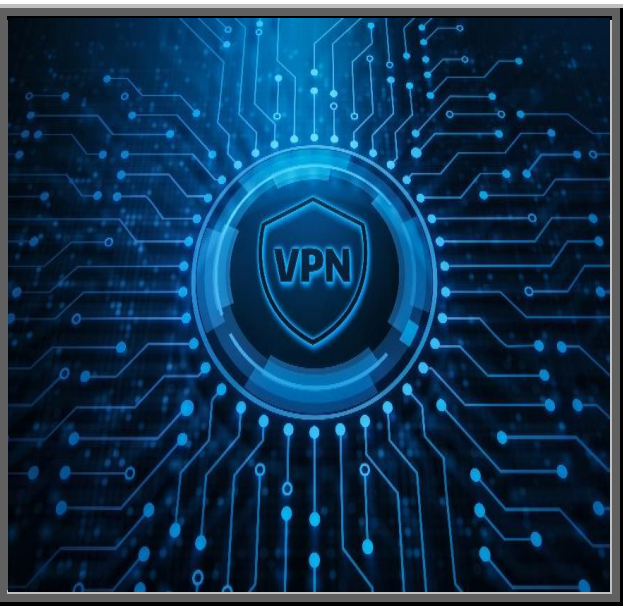
INDIA'S NEW CYBERSECURITY DIRECTIVE: TO BE OR NOT TO BE?

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Malik Qasim Mustafa

September 21, 2022

(Views expressed in the brief are those of the author, and do not represent those of ISSI)



As the extended deadline of September 25, 2022, for the implementation of India`s New Cybersecurity Directive by the CERT-In is approaching, the panic in the Indian ICT landscape has started to mount. The Indian tech industry has termed this new directive as a threat to the Digital India Vision and showed immense resistance. However, the government of India has reaffirmed its commitment to the new directive. What is CERT-In? What this new cybersecurity directive is all about? Whether the government of India would enforce this directive or pull it back due to massive resistance and fallout?

What is CERT-In?

The "Indian Computer Emergency Response Team (CERT-In) was appointed by the Central Government as a key cybersecurity agency under section 70B of the Information Technology (IT) Act, 2000.[1] Under sub-section (4) of section 70B,[2] the CERT-In is in charge of the collection, analysis and dissemination of information related to cybersecurity incidents. In addition to issuing alerts and forecasts, the CERT-In is responsible for the coordination and taking of emergency measures to handle cybersecurity incidents. It can also issue "guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and

1 Government of India, *The Information Technology Act*, 2000, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
2 Ibid., 28.

reporting of cyber incidents." Under sub-section (6) of section 70B,[3] the CERT-In is authorised to demand information and give directions to the service providers, intermediaries, data centres, body corporate and any other person to carry out its functions.

What is India's New Cybersecurity Directive?

The text of the new directive defines its objective very clearly. The Government of India has issued this directive in the interest of "the sovereignty or integrity of India, defence of India and security of the state."[4] Furthermore, the Government of India wants to maintain "friendly relations with foreign states and public order…" to prevent "incitement to the commission of any cognizable offence using computer resources or for the handling of any cyber incident." The directive contains the following six measures:

1. Synchronisation of Information and Communication Technology (ICT) System Clocks

For the synchronisation of all ICT systems clocks, it is mandatory for all government organisations, data centres, services providers, corporate bodies and other intermediaries to connect with "the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers." Furthermore, all entities that have their ICT infrastructures in numerous geographical locations across the globe must use such standards and accurate time source systems that do not deviate from the NPL and NIC.

2. Extensive List of Reportable Cyber Incidents

Annexure – I of the directive contains an extensive list of cybersecurity incidents for mandatory reporting to CERT-In. This includes traditional incidents like compromise and unauthorised access of critical systems and data, defacement of websites, spreading of viruses, attacks on servers, attack on network devices, identity theft, spoofing and phishing attacks, denial of service (DoS) and distributed denial of service (DDoS) attacks, attacks on E-Governance, E-Commerce applications and digital payment systems, data breach and leaks, attacks through malicious mobile apps, fake mobile apps, unauthorised access to social media accounts. The list also includes cybersecurity incidents related to designing, development, manufacturing and use of emerging technologies like attacks on systems/servers/software/applications related to the Internet of Things (IoT), cloud computing, big

3 Ibid., 28-29.

4 Government of India, Ministry of Electronics and Information Technology (MeitY), Indian Computer Emergency Response Team (CERT-In), *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet,* No. 20(3)/2022-CERT-In, April 28, 2022, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drone, artificial intelligence and machine learning.

3. Reduced Time for Reporting Cyber Incident

It is mandatory for all government organisations, data centres, services providers, corporate bodies and other intermediaries to report the cybersecurity incidents, mentioned in Annexure I, within six hours of first noticing such incidents.

4. Extended Access of CERT-In to Information

For appropriate emergency response and prevention of cybersecurity incidents, the CERT-In can direct/order information from all government organisations, data centres, services providers, corporate bodies and other intermediaries. They must assist and provide required information to CERT-In in the prescribed format and specified timeframe. Failure to do so will be considered non-compliance with this directive. Furthermore, all government organisations, data centres, services providers, corporate bodies and other intermediaries would designate a point of contact to interact with CERT-In for all types of communications and compliance issues.

5. Maintaining System Logs within India

It is mandatory for all government organisations, data centres, services providers, corporate bodies and other intermediaries to ensure secure enabling and maintenance of logs of their all ICT systems within the jurisdiction of the Indian government for the rolling period of 180 days. This log information must be provided to CERT-In on order/direction as well as while reporting a cybersecurity incident.

6. Maintenance of Information by VPN Service Providers

It is mandatory for data centres, virtual private server (VPS) providers, cloud service providers and Virtual Private Network (VPN) service providers to maintain the information about all the registrations for an extended period of five years even after cancellation and withdrawal. The directive also includes the list of information required for registration as well as record keeping. It includes validated names of customers, purpose and time period of hiring (including dates), ownership pattern, allocated IP addresses with time stamps, email address, verified address and contact numbers.

7. Maintaining Information about Financial Transactions

It is mandatory for virtual asset service providers, virtual asset exchange providers and custodian wallet providers to main all records of financial transactions and information collected under Know Your Customer (KYC) for the time period of five years. The directive includes the list of identification information to be maintained as well. This includes but is not limited to ID, nature, date and amount of transaction along with IP addresses, time zones and time stamps. As per the directive, the objective of these measures is to ensure cybersecurity for the citizens in the realm of financial transactions. These measures, in any way, will not affect the protection of their data, fundamental rights and economic freedom of the Indian citizens.

Response to New Directive

In the last few years, India`s effort to imitate Western rules and regulations is becoming more and more visible. Foreign experts believe that these regulations might appear to be democratic and westernised but there is an authoritarian Indian twist in the backdrop. Under the tag of enhancing cybersecurity and protecting data privacy, the current Indian government is pursuing a dictatorial plan without any proper public accountability and transparency mechanisms in place. Unlike the EU`s GDPR, there are no checks and balances in the Indian government for handling such a huge amount of sensitive data. The issues of enforcement and compliance would further add fuel to the fire. Despite tall claims, the existing CERT-In neither has sophisticated technology nor financial resources to ensure enforcement and compliance for such an extensive directive at such a huge level. In the absence of capacity and resources, to what extent the political will of CERT-In would aid the enforcement? Is it practically possible for CERT-In to send millions of people to prison on the charges of non-compliance?[5]

Another major concern for the tech industry is the damage this directive would inflict on Indian standing in the global tech industry. Many Indian experts believe that this harsh directive would force well-established international companies to pull their businesses out of India. Instead of compliance, they would prefer to relocate their businesses to other countries. Various VPN companies in India have already expressed their concerns regarding the ambiguity and harshness of this new directive. "The new Indian VPN regulations are an assault on privacy and threaten to put

5 Claudia Glover, "Will India's controversial new cybersecurity rules be enforced?" *Tech Monitor*, May 19, 2022, https://techmonitor.ai/technology/cybersecurity/india-cybersecurity-data-breach.

citizens under a microscope of surveillance," said Proton VPN in their official tweet.[6] Express VPN said that it is "fully committed to protect the privacy of its users." Furthermore, many VPN companies e.g. Nord VPN are considering pulling out their services from India.[7] To ensure secure maintenance of the log record and personal data of customers for an extensive period of five years, international as well as national companies would have no other option than to invest in new infrastructure, which would increase the cost of doing tech business in India. Increasing costs along with the compliance hassle would not only discourage the new local tech start-ups but also create massive honeypots of data readily available to be misused by hackers. Similarly, the synchronisation of ICT system clocks with government-approved servers is against the established best practices. This could create a single vulnerability point and failure of this point could result in a massive fallout for the entire national ICT infrastructure. Instead of strict centralisation, Indian experts are suggesting decentralisation of networks to avoid a single big chokepoint.[8]

Despite massive criticism from the tech industry, the signs of compromise and flexibility from the Indian government are nowhere to be seen. "If these rules are not for you, then this place is not for your business," said Mr Rajeev Chandrashekhar, Indian Minister for IT.[9] To conclude, even if the government of India decides to implement this directive, the fallout would be so huge that it would become extremely difficult for the Indian government to continue working for a longer period. As of now, the recourse at one`s disposal is to wait and watch.

6 Newley Purnell, "Global VPN Providers Pull India Servers Over New Cybersecurity Rules," *The Wall Street Journal*, September 1, 2022, https://www.wsj.com/articles/global-vpn-providers-pull-india-servers-over-new-cybersecurity-rules-11662024603.

7 Naina Bhardwaj, "Why Are Industry Players Unhappy with India's New Cybersecurity Directives?" *India Briefing*, July 1, 2022, https://www.india-briefing.com/news/indias-new-cybersecurity-directives-what-are-they-and-why-are-industry-players-unhappy-25006.html/; Claudia Glover, "Will India's Controversial new Cybersecurity Rules be Enforced?" *Tech Monitor*, May 19, 2022, https://techmonitor.ai/technology/cybersecurity/india-cybersecurity-data-breach.

8 Neeti Biyani, "India's future is digital. But new cybersecurity rules are getting in the way," *Times of India*, August 9, 2022, https://timesofindia.indiatimes.com/blogs/voices/indias-future-is-digital-but-new-cybersecurity-rules-are-getting-in-the-way/.

9 Julian Bingley, "India Reaffirms Commitment to new Cybersecurity Rules," *ZDNET,* https://www.zdnet.com/article/india-reaffirms-commitment-to-new-cybersecurity-rules/.