INDIA GETS READY TO SET UP CYBER SNOOPING AGENCY

March 2014

India will soon be setting up a federal internet scanning agency called NCCC to spy all internet accounts and online data. NCCC is to monitor cyber security threats and inform concerned law enforcement agencies for proactive action to prevent crime. NCCC will collect and integrate internet traffic data from different gateway routers of major ISPs at a centralized location for analysis. NCCC would be set up at a cost of INR 10 billion and all top government spy and technical agencies including Department of Telecommunication, Intelligence Bureau, Research and Analysis Wing, Indian Computer Emergency Response Team, Army, Navy, Air force, National Security Council Secretariat, Defence Research and Development Organization will play an active role in the functioning of NCCC.

PSA view – In the present internet era, cyber attacks are on an increase and pose as a huge threat to the safety and security of the nation. Recently, Central Bureau of Investigation's website had been defaced by hackers and in another case attempts were made to break into Indian Railway Website. Therefore, NCCC is need of the hour and a step in the right direction to address the shortcoming in the cyber security.

100% FDI allowed in telecom sector

In a meeting of the Department of Policy and Promotion chaired by Prime Minister on July 16, 2013, it was announced that FDI limit in the telecom sector has been increased to 100%. The earlier limit was 74%. As per latest announcements, investment up to 49% is allowed to come in through the automatic route and investment above 49% is required to be brought in through the government route i.e. approval of the Foreign Investment Promotion Board.

PSA view – The announcement is seen as a welcome change. However, the policy and implementation of these announcement is what is most awaited. The increased limits are set to bring in billions of investments in this sector. Fresh foreign investments would help catalyze growth and the process of proliferation in the telecom sector across the country.

India set to frame new testing norms for telecom equipment

The Department of Telecommunications with the Department of Electronics & IT and National Technical Research Organization are all set to frame new testing standards for telecom gear to shield networks from potential cyber attacks. The Common Criteria Recognition Arrangement ("CCRA") clearance will no longer be enough to certify global telecom gear used in India, announced the National Security Council Secretariat, the apex agency looking into India's political, economic and energy and strategic security concerns.

PSA view – CCRA was created ten years back by UK, US, Canada, France, Germany and the Netherlands, Australia and New Zealand, to define a common process to evaluate security-sensitive IT & telecom products and an objective to motivate global telecom vendors to find common processes to reduce equipment certification costs worldwide. But now India has started creating country-specific telecom gear testing standards and adopting several measures: (i) mobile phone companies have been mandated to use equipment deemed "safe" by an authorized testing lab in India from November 1, 2013; (ii) India is preparing a cyber security framework and a cyber security policy; (iii) India is setting up a National Cyber Coordination Centre to monitor metadata on cyber traffic flows; (iv) Establish a pilot lab and a full-fledged certification center and development system; and (v) To adopt global approaches to its procurement policies, India is reviewing its Preferential Market Access policy designed to compel foreign companies to manufacture electronic products in India if they want to sell in India.

Two telecom security bodies for shielding telephone networks

Telecom Security Directorate ("TSD") and the National Telecom Network Security Coordination Board ("NTNSCB") will frame standards and procedures for testing network gear and monitoring implementation of the telecom security policy. While TSD will primarily coordinate work relating to security policy and project execution, NTNSCB will suggest ways to address telecom security issues in future and also monitor implementation of the new standards. India is also readying a cyber security framework, a cyber security policy and a National Cyber Coordination Centre that will monitor metadata on cyber traffic flows. In addition, Department of Telecommunications ("DoT") is working with other concerned departments to establish testing standards and procedures for telecom gear and has even sought approval of the National Information Board on the draft telecom security policy.

PSA view – Pursuant to the concerns raised regarding Chinese vendors, this step seems to be a logical step also because India is the largest market for network gears and should have proper policies to ensure the quality of products. Earlier the DoT had issued directive to mobile phone companies mandating them to use equipment deemed safe by an authorized lab in India from November 1, 2013.

Proposed National Telecom Security Policy

NTSP released by the DoT focuses on tightening the security related to telecommunication over the landline, cellular and broadband. The Ministry of Home Affairs ("MHA") has expressed concerns stating that the policy should allow interception of communication network by law enforcement agencies. NTSP must ensure that there is specific provision allowing law enforcement agencies to intercept telephone calls, voice-mails, e-mails and other services like BlackBerry messenger on a real time basis and also specify proper code for setting up a secure communication network. According to the MHA, NTSP should also cover issues related to priority communications over all networks. National Information Board is the authority which will finalize the proposed NTSP which will then receive concluding assent from Cabinet of Committee Security headed by the Prime Minster Manmohan Singh.

PSA view – Security over telecommunication network has always been a concern within the Government of India. Though, DoT intends to tighten the security by way of NTSP for private individuals, it is to be seen whether government will approve of the same. Use of Chinese equipments also raises concerns over

security. NTSP will ensure that all future procurements take place from Indian and trusted foreign vendors. All telecom operators will be required to regularly audit their network for bugs and security searches.

India gets the status of "authorizing member nation" from CCRA

The recently given status of "authorizing member nation" by CCRA is a morale booster for India and can help India emerge as a low cost testing hub for IT and telecom products. This status can help India emerge as a low-cost hub for testing security-sensitive IT products used in telephone and other critical infrastructure networks. CCRA is the top international agency that defines common processes to certify IT products used in infrastructure networks in telecom, power, aviation and defence sectors. This status means that India can now issue clearances to companies to set up CCRA-accredited private test labs.

PSA view – The labs in India can offer testing services at a much reasonable cost when compared to other CCRA labs. As these labs employ manual intensive process, Indian labs will have distinct cost advantages.

Telecom M&A guidelines to be in place

The Telecom Secretary MF Farooqui has announced that M&A guidelines for the telecom sector should be out within the next ten days. The Empowered Group of Ministers (EGoM), which has approved the guidelines, has sought legal opinion on whether consolidation of companies would amount to sale of equity, violating the lock-in period rule of the telecom license. As per the guidelines approved by the EGoM, the market share of a merged entity should not exceed 50%. Telecom companies that bought spectrum in auctions won't have to make additional payments to the government for radiowaves after a merger. Only companies that acquire telecom operators that had been allocated spectrum will have to pay the difference between the market rate and the old rate to the government.

PSA view – M&A will serve as another way in which spectrum can be acquired.

NATGRID Project set to initiate

NATGRID was set up by the government in the aftermath of Mumbai attacks to enable monitoring of terrorist operations through existing banking, finance and transportation networks. Various ministries and departments, called provider agencies, which hold 21 categories of citizen database like bank account details, telephone records, passport data and vehicle registration details, are supposed to be linked and shared in real-time through the NATGRID with the 11 intelligence and investigative agencies, termed as user agencies. The government will soon be issuing an executive order to give a legal framework and mandate to NATGRID.

PSA view – The government is of the opinion that it can use data from Centralized Monitoring System as well as that available via Aadhar and pass it around the various government departments through the NATGRID to stop terrorism. However, on the hindsight NATGRID can have adverse effect. It can be used as a channel to target people who might be against the government. It is to be seen how accurately this project evolves and is used by government agencies.

National Cyber Security Policy 2013 ("Policy")

The objectives of the Policy include: (a) setting up of an effective mechanism to obtain strategic information relating to cyber threats; (b) protection of Critical Information Infrastructure; (c) creation of a skilled workforce in cyber security; (d) protection of data during transit; (e) effective prevention, investigation and prosecution of cyber crimes; and (f) creation of a global understanding and cooperation on cyber security.

As per the Policy, the foremost strategy is to create a secure cyber ecosystem by providing for a nodal agency to coordinate cyber security matters, encourage companies to designate a senior member as “Chief Information Security Officer” and promote organizations to develop information security policies. Other strategies involve conformity with global best practices and certification to the various standards, strengthening of the regulatory framework and periodic review against emerging threats. The Policy talks about the operation of a national level body called the Computer Emergency Response Team (CERT-In) to coordinate all efforts relating to cyber security and work as an umbrella organization.

PSA view – The Policy will be operational by way of detailed guidelines and plans of action at various levels such as national, state, enterprise, ministry etc. It will not only help in creating awareness among organizations but also make them more conscious towards cyber security and threats. Pursuant to enforcing the Policy, the Department of Information and Technology also seeks to form a body named National Critical Information Infrastructure Protection Centre. This will seek to operate as a nodal body for protection of critical information infrastructure.

By:
Krishna Jhala
Neeraj Dubey