

Building Law Enforcement Capacity to Tackle Cyber Threats: Lessons from Year One of Capacity Building Workshops

Bedavyasa Mohanty

Source: VMware

INTRODUCTION

In the second week of May 2017, information services across the globe were hit by a wave of ransomware attacks unlike anything that had been seen before. The now infamous WannaCry malware that targeted systems running unpatched versions of Microsoft Windows affected nearly 200,000 computers across 150 countries. When the dust settled, India along with Russia, Ukraine and Taiwan were

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions.



To know more about
ORF scan this code

identified as the countries that were worst hit by the malware.¹ Among the Indian entities, some of the most noteworthy victims were the Andhra Pradesh Police² and four state governments.³ In Gujarat, for instance, nearly 120 computers belonging to the Gujarat State Wide Area Network, which is responsible for maintaining government IT systems across 33 districts, were affected.⁴ It was also reported that multinational corporations and banks had been victims of the attack.⁵ This is hardly surprising when India has long been considered a top source of, and destination for, cyber attacks.⁶ Instances such as these affect investor confidence in the security of India's IT systems, perhaps irreparably. A recent report by Analysys Mason reported that trust in India's cyber security infrastructure is a central factor in determining the competitiveness of India's significant outsourcing sector.⁷

Despite the nascence of its cyber systems and a 23-percent internet penetration rate, India has had the second largest internet user base in the world since 2015.⁸ With the Indian government's weight behind its 'Digital India' programme, there is no indication that this pace of adoption of technology will slow down soon. However, there has been little parallel effort to strengthen the security of India's ICT infrastructure to deal with the threats brought about by digitisation. While the number of registered cases of cyber-crime in India has been steadily rising, the rate of conviction is abysmally low.⁹ A possible explanation of this failure is the deep divide between the ideation of the nation's cyber policies, and their implementation. The National Cyber Security Policy adopted in 2013 planned for the creation of a workforce of 500,000 professionals trained in cyber security by 2018. However, no serious steps have been taken in this regard to institutionalise training and capacity building efforts. Similarly, the National Cyber Crime Coordination Centre, which was meant to serve as a nodal body for cyber security and intelligence sharing, is yet to be set up despite having received the green light in 2013.¹⁰ These are only some of the obstacles that prevent India's cyber security infrastructure from maturing to desirable levels. At the heart of the matter is a lack of technical and human expertise in actively dealing with cyber threats. Recognising this dire need, the Observer Research Foundation, supported by the UK Foreign and Commonwealth Office's Cyber Capacity Building Fund, in 2016 launched a national cyber capacity building initiative to train various state and central law enforcement agencies in dealing with contemporary cyber threats.

The two-year project identifies experts from the areas of law and technology to provide contextual training to mid-career law enforcement officials (LEAs). These training sessions have covered a wide array of topics, ranging from cyber laws and internet governance to cyber espionage and security of financial systems. The sessions not only familiarise LEAs with contemporary issues in cyber security but also obtain feedback on specific areas where a lack of capacity hinders criminal investigations.

OBTAINING ELECTRONIC EVIDENCE FROM ABROAD

A common concern among the police officers that attended the four workshops conducted in 2016-17 was the lack of access to electronic evidence for criminal investigations. As India is a net data exporter, most of the electronic data generated by its citizens through social media websites, instant messaging platforms and email apps are stored outside the jurisdiction of Indian LEAs.¹¹ In these cases, law enforcement officials have to resort to formal and informal data sharing channels to access this data. It has been well recorded that these mechanisms are fraught with inefficiencies that delay investigations and often cause them to fail. Especially in cyberspace, where electronic data that is generated can be wiped out at any moment, these delays can often result in the evidence becoming permanently inaccessible. The inefficiencies in the process cannot be explained away by any single failure in the system; it is rather a result of systemic problems that exist within the Indian law enforcement agencies and bureaucracy.

The primary tool that Indian law enforcement agents rely on to obtain data stored abroad are Mutual Legal Assistance Treaties (MLATs). MLATs are bilateral arrangements (or in some cases, multilateral) that allow two countries to lend assistance to each other for purposes of investigation and prosecution of crimes. India has signed 39 such treaties with various countries.¹² Twenty-seven of these contain provisions obligating signatories to assist in collection of evidence while 25 others provide for assistance in search and seizure.¹³ However, in spite of these obligations, law enforcement officials have little confidence in successfully obtaining information through MLAT requests except in sensational and high-profile cases. The primary reason for this, as mentioned earlier, is the delay in obtaining evidence through the MLAT process – one estimate claims that the average time taken by an Indian agency to obtain evidence stored on a server in the US is three years and four months.¹⁴ The other reason, however, is a lack of expertise among Indian officials in raising these requests which results in rejection by the foreign courts. While most MLATs do not have a “dual criminality” requirement (i.e., the subject of the investigation only needs to be a crime in the requesting state), the procedural standards applicable for obtaining the evidence are that of the requested state. This means that for successfully obtaining evidence from abroad, MLAT requests need to be drafted in a form and language that would be compelling to the examining authority in the requested state. Most Indian law enforcement agencies do not receive adequate training in drafting these targeted requests.

The Indian Ministry of Home Affairs, which serves as the nodal agency for MLAT requests and acts as a liaison between Indian LEAs and their foreign counterparts, has often been found wanting in helping harmonise these requests with the needs of the requested state. For instance, translation of supporting documents into the language of the requested state (a mandate of the MHA under MLATs) is reported to have not been followed in some instances, resulting in the

rejection of requests. In many other instances, the time taken by the MHA for review adds to an inordinate delay in the filing of these requests. Most of these problems stem from a lack of trained personnel dedicated to handling MLAT requests.

These problems, however, are not unique to India. MLATs and similar formal data sharing mechanisms are generally considered ill-suited for investigation of cyber-crimes. This realisation has caused the US and UK, for instance, to negotiate a direct data sharing agreement that would allow UK LEAs to demand data directly from intermediaries holding data in the US. A sine qua non for this agreement is a written assessment that UK's laws have both substantial and procedural protections for user privacy and that the government has displayed adequate respect for human rights.¹⁵ This agreement, which is likely to come into effect before the end of 2017, should substantially ease the process for obtaining electronic data for investigations for LEAs in the US and UK.

Indian policymakers, too, are closely studying the negotiations to explore whether such an arrangement can be replicated at the India-US level. However, steps must also be taken to ensure that the pitfalls of the MLAT mechanism are not repeated. The nodal officers in charge of making data requests must be regularly trained to draft these requests in a manner that reduces the likelihood of rejection. The review process within the Ministry of Home Affairs must also be improved so that the requests are compliant with the laws and procedures of the requested countries.

CYBER HYGIENE

The WannaCry ransomware attack highlighted the vulnerability of the cyber systems in use by Indian state agencies. Reports claim that as many as 18 computer systems in use by Andhra Pradesh Police were infected with the malware. This, however, is not circumstantial. There have been past instances where law enforcement and military personnel have been specifically targeted by Trojans and malwares in an attempt to obtain intelligence about issues such as troop deployment and strategic planning. Information on troop movements following the terrorist attack on the Pathankot Air Force base in January 2016, was allegedly obtained by Pakistan's intelligence agencies using a spyware app freely available at that time on the Google Play platform.¹⁶ These infiltrations make use of a mix of technical exploits along with social engineering to obtain access to confidential data. This was also demonstrated during one of the training workshops where some police officials divulged their account information and credentials in response to a spear phishing attempt by one of the trainers.

These instances bring to the fore the lack of a culture of cyber hygiene even among trained law enforcement personnel with access to sensitive information. Malicious actors that obtain access to this sensitive information can use it for a

range of nefarious purposes either passively (by planning further activity based on the intelligence gathered) or actively (by extorting the victim of the attack). The most notable example of the catastrophic effects of a lack of cyber hygiene is perhaps the malfunction of the Iran's Natanz nuclear power plant where the Stuxnet malware infiltration occurred through the insertion of an unauthorised USB drive in one of the plant's computers.

Cyber hygiene must therefore be a critical aspect of capacity building not only for law enforcement officials but even the administrative staff in the criminal justice system. Officials should be trained in basic cyber hygiene and security practices such as maintaining strong passwords and regularly backing up data. More sensitive data handled by these organisations should be stored and transmitted in an encrypted format to avoid compromising their integrity.

CONCLUSION


Building cyber security capacity among law enforcement agencies is a critical step towards protecting the rights of Indian citizens but it is by no means the only one. Boundaries between civilian and military; commercial and personal are often blurred in cyberspace. The networks that carry millions of terabytes of data do not discriminate between critical and non-critical systems – which is why even supposedly 'manageable' cyber threats have the potential to create catastrophic damage. A piecemeal approach towards securing cyberspace has never been viable and never will be. As a recent analysis of the state of cyber security in India by the Potomac Institute points out, the only area where India has attained relative maturity is in cyber diplomacy;¹⁷ other related domains like military cyber defence, incident response, law enforcement and research and development remain largely in the early stages of development.¹⁸

Building capacity will require more than an acknowledgement of the threats and an expression of intent to tackle them. The only way forward is for the government to institutionalise capacity building initiatives. Towards this end, the government must take the following steps to ensure that state police agencies are adequately trained to handle more common cyber crimes such as online harassment and financial fraud. There must also be capacity building initiatives aimed towards handling large-scale cyber attacks that threaten critical information infrastructure.

1. **Training modules:** The government must begin designing standardised and dynamic modules that can offer training to law enforcement officials from conceptual aspects of cyber security and data protection to advanced investigative technologies.¹⁹ These modules should be authored by information security practitioners and must seek to incorporate theoretical and practical aspects in equal measure.

2. **Cyber range:** The government must invest in building state-of-the-art cyber-ranges – sandbox environments where networks and hardware can be isolated and put through rigorous testing. These can be used to conduct penetration testing of IT infrastructure and software used by civilian as well as military agencies. India currently does not have government-owned cyber ranges and until such time that these can be developed, the government must make use of privately owned cyber ranges²⁰ to test the integrity of its networks. Currently, Cisco runs a cyber range in Gurugram, Haryana to train information security personnel from government and private sector, as well as to test products before deployment.
3. **Hardware security:** An important aspect of cyber security is ensuring that the tools that are used by public sector enterprises are not themselves compromised. This can hardly be ensured when India has little say in the production of electronic goods or ensuring the integrity of supply chains. In 2013-14 for instance, China alone accounted for 58 percent of all electronics imports to India. To tackle the lack of cyber hygiene described above, there must be a mandatory updating of computer systems in use by Indian LEAs including installation of high quality anti-virus software and firewalls; regular backups of stored data; and a transition to licenced enterprise software wherever required.²¹
4. **Public reporting platform:** It has been said that the number of cyber-crimes reported to LEAs is unreliable since many instances go unreported either due to a lack of awareness on the part of victims or a lack of faith in LEAs to successfully investigate cyber crimes. LEAs should develop a nationwide, open portal where instances of cyber crimes and harassment can be reported even in cases where no formal complaint is filed. This will help understand trends in cyber crimes and guide capacity building in the long run.
5. **Public-private partnerships:** Increased partnership with the private sector is a familiar refrain whenever cyber security is discussed and rightly so. The private sector which is at the forefront of technological innovation can not only bring its technological prowess to bear against cyber threats but also assist in investigations through proactive disclosures. This cooperation, however, must go beyond mere information sharing and should involve personnel exchange programmes similar to INTERPOL's Cyber Fusion Centre, where experts from the private sector actively assist in investigation of cyber crimes.
6. **Legal reform:** Many challenges to investigation of cyber crimes and electronic data gathering can be solved by reforming India's data protection laws. For instance, Section 67C under the Information Technology Act, 2000 provides for preservation of data by intermediaries that can assist in criminal investigations. This provision is scarcely used by LEAs since no rules of procedure have been drafted under the Section, rendering it almost

redundant. The government must take a closer look at the data protection laws in India and revamp them as necessary to assist investigative agencies.

7. **Open-source tools:** Law enforcement officials should be trained in the use of various open-source tools that can analyse data over the internet to gather evidence. These tools that are inexpensive and compatible across systems, can be used by LEAs to conduct cyber forensic examination of the electronic evidence gathered during their investigations.
8. **Funding and coherence in strategy:** The Indian government needs to implement recommendations articulated in the National Cyber Security Policy, 2013. This can be achieved by setting up a roadmap for achieving training and acquisition targets. There should also be demarcation of clear timelines for the completion of these projects as well as identification of a dedicated fund for achieving these objectives. The government should actively seek the cooperation of civil society organisations, the private sector, and universities, to help fill the technical expertise gap within government departments. 

ABOUT THE AUTHOR

Bedavyasa Mohanty is an Associate Fellow with ORF's Cyber Initiative.

ENDNOTES

1. Anirudh Regidi, "WannaCry ransomware: Despite govt denials, experts say that India is the third largest source of attacks", Firstpost, May 17, 2017, available at: <http://tech.firstpost.com/news-analysis/wannacry-ransomware-despite-govt-denials-experts-say-that-india-is-the-third-largest-source-of-attacks-376439.html>.
2. IANS, "Andhra police computers hit by cyberattack", Times of India, May 13, 2017, available at: <http://timesofindia.indiatimes.com/india/andhra-police-computers-hit-by-cyberattack/articleshow/58658853.cms>.
3. Neeta Sharma and Sneha Mary Koshy, "Monday's Ransomware Attack Fails to Dent India, Says Minister: 10 Facts", NDTV, May 15, 2017, available at: <http://www.ndtv.com/india-news/ransomware-wannacry-surfaces-in-kerala-bengal-10-facts-1693806>.
4. Tech Desk, "WannaCry ransomware attack: List of Indian states that have been affected", The Indian Express, May 17, 2017, available at <http://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-attack-list-of-indian-states-that-have-been-affected-4660449/>
5. Surabhi Agarwal and Aritra Sarkhel, "Cyber experts working round the clock to protect India from the 'biggest ransomware' attack", The Economic Times, May 15, 2017, available at <http://economictimes.indiatimes.com/tech/internet/cyber-experts-working-round-the-clock-to-protect-india-from-the-biggest-ransomware-attack/articleshow/58674741.cms?from=desktop>.
6. Symantec, "Indian Businesses Under Fire: Professionalization of Cybercrime Means Organizations Now Need To Brace Themselves For Repeated Attacks", Symantec, April 21, 2016, available at: https://www.symantec.com/en/in/about/newsroom/press-releases/2016/symantec_0421_01.
7. Analysys Mason, "How Strong Encryption Supports the Development of a Safe and Secure Internet: An Asia-Pacific Perspective", Analysys Mason, September 26, 2016, available at

- http://report.analysismason.com/strong_encryption_asia/Encryption_study_2016-09-27_FINAL.pdf
8. Broadband Commission, “The State of Broadband: Broadband catalyzing sustainable development”, Broadband Commission, September 2016, available at <http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf>
 9. Arunabh Saikia, “Why most cybercrimes in India don't end in conviction”, LiveMint, July 29, 2016, available at: <http://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html>.
 10. Saikat Datta, “India's cyber protection body pushes ahead”, Hindustan Times, January 20, 2014, available at: <http://www.hindustantimes.com/india/india-s-cyber-protection-body-pushes-ahead/story-4xa9tjaz6ycfDpVg95YqPL.html>.
 11. With 200 million monthly active users, for instance, India is the largest market for Whatsapp, the instant messaging service owned by Facebook.
 12. Central Bureau of Investigation, “MLATs”, Central Bureau of Investigation, available at: <http://cbi.nic.in/interpol/mlats.php>.
 13. Leilah Elmokadem, “Mapping of Sections in India's MLAT Agreements”, Centre for Internet and Society, December 31, 2016, available at: <http://cis-india.org/internet-governance/blog/india-mlat-agreements-sections-map-dec-2016>.
 14. Neha Alawadhi, “CBI & FBI join hands to reduce time required to fulfil requests on information and evidence”, Economic Times, December 15, 2017, available at: <http://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-hands-to-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms>.
 15. Peter J. Kazdik, “Assistant Attorney General, US Department of Justice, in Letter to Joseph R. Biden, President, United States Senate,” Department of Justice, July 15, 2016, available at: https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf.
 16. Pranay Upadhyay, “Honeytraps on Facebook, spyware: How Pakistan is snooping on Indian troops”, News18, March 15, 2016, available at <http://www.news18.com/news/india/honeytraps-on-facebook-spyware-how-pakistan-is-snooping-on-indian-troops-1216191.html>
 17. Through the Ministry of External Affairs, India has been effectively engaging in international norm building processes on cyber security. It has also identified cyber security as a tier-one foreign policy element.
 18. Melissa Hathaway, et al., “India Cyber Readiness at a Glance”, Potomac Institute for Policy Studies, December 2016, available at: http://www.potomac institute.org/images/CRI/CRI_India_Profile.pdf
 19. Madan M Oberoi, “National Capacity Strengthening to Combat Cybercrime”, Digital Policy Portal, July 21, 2016, available at: <http://www.digitalpolicy.org/national-capacity-strengthening-to-combat-cybercrime/>
 20. PTI, “Cisco launches 5th global cyber range lab in Gurugram”, The Economic Times, April 12, 2017, available at: <http://economictimes.indiatimes.com/tech/internet/cisco-launches-5th-global-cyber-range-lab-in-gurugram/articleshow/58142965.cms>
 21. Reuters, “India presses Microsoft for Windows discount in wake of cyber attacks”, CNBC, June 30, 2017, available at: <http://www.cnbcm.com/2017/06/30/india-presses-microsoft-for-windows-discount-in-wake-of-cyber-attacks.html>



Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org