Combating Cybercrime in India

Dr. Karnika Seth

Introduction

In the past few decades, the contribution of information technology at the national and global forefront has been phenomenal and unprecedented. However, this unique and dynamic medium of communication has also brought techno-legal challenges. Particularly, its inherent features of anonymity and borderless expanse have lured cybercriminals leading to a rise in cyber threats, attacks & crimes.

According to a recent *Symantec survey*, India ranked 3rd in the list of countries where the highest number of cyber threats were detected in 2017. The report revealed that India ranked 4th globally with 8% of global detections of ransomware (A *Ransomware* locks the computer and demands money to unlock the system). With the increase in the value of cryptocurrency, cyber-attacks from new cyber miners have been detected wherein cybercriminal steals computer processing power usage from consumer and entities to mine digital currencies. The said Symantec report found that the detection of coin miners on endpoint computers increased by 8500% in 2017. India also ranked 2nd after the U.S in term of the highest number of malware for mobile phones.

The term '*cybercrime*' has not been defined under the IT Act 2000, which is a special enactment of Indian law governing activities carried out using the internet or linked communication devices. The term '*cybercrime*' in general, encompasses all crimes which are committed using a computer or computer network or where such computer or network is used as a medium to commit a crime or is a target of crime such as in case of causing damage to system and data. Cybercrimes may be crimes committed against the government such as cyber terrorism, crime against a person such as cyberstalking or cyberbullying, crime against property such as hacking and damage to the computer system or data thefts. Cybercrimes are of diverse kinds including phishing, wherein a gullible person is cheated by an imposter using a stolen identity compelling victim to share his financial data in order to make unauthorised debits from his account. The Information Technology Act prescribes punishment for various offences such as unauthorisedly accessing of computer or copying of data is punishable under Section 66 of IT Act, 2000 with up to 3 years of imprisonment. For cyber terrorism, Section 66 F of IT Act, 2000 provides punishment up to life imprisonment. Crimes which are punishable with imprisonment up to 3 years and fine are cognizable but bailable such as publishing or transmitting obscene material (Section 67). The crimes which are punishable with imprisonment of more than 3 years and fine such as child pornography (Section 67B) are cognizable but non-bailable.

Organisations Combating Cybercrime in India

Cybercrime poses a great threat to the national security of the country and may lead to great loss in financial stability too. Also, India's major role in the IT global market is one of the important reasons to provide a secure computing environment and the

creation of a secure legal framework to enforce the same. As per the NCRB cybercrime statistics, crimes in India reported in 2016 were *12,317* and there were only 201 convictions.

The **National Information Board** (NIB) is the highest decision-making body for information and cyber operations. It has members from all ministries, security agencies and the armed forces. The National Security Council Secretariat (NSCS) coordinates and oversees cybersecurity issues, including Cyber Diplomacy.

The National Cybersecurity Coordinator (NCSC) has been entrusted to coordinate and synergise cybersecurity efforts.

The National Security Adviser (NSA) chairs the National Intelligence Bureau (NIB) while the NCSC is the secretariat of the NIB.

CERT-IN (Indian Computer emergency response team, Department of Electronics and Information Technology, Ministry of Communication and Information Technology has been prescribed as a nodal agency for incident response) under Section 70B of the Information Technology Act 2000. The agency is responsible for collection, analysis and dissemination of information, forecast and alerts of cybersecurity incidents, adopting emergency measures for handling cybersecurity incidents, coordination of cyber incidents response activities, issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents, such other functions relating to cybersecurity as may be prescribed.

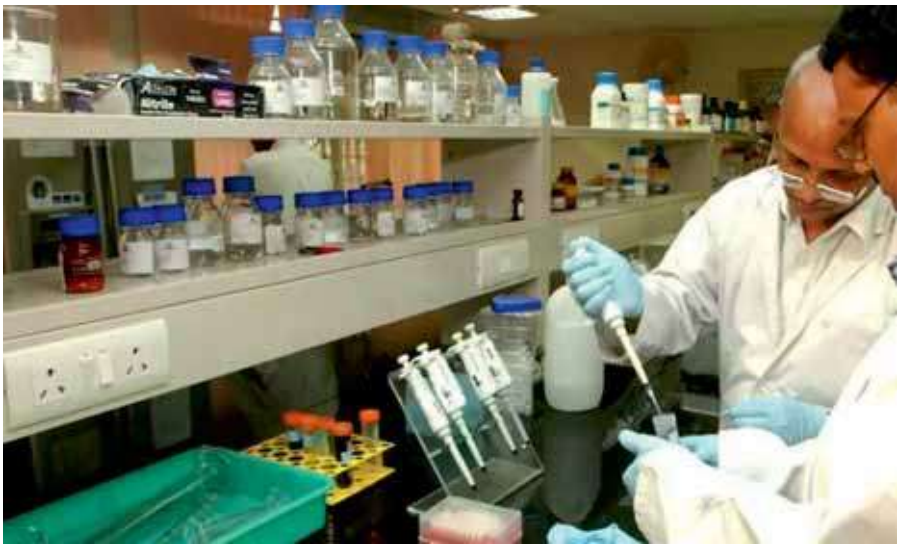
CERT-IN works with sectoral CERTs to perform incident response responsibilities. Armed CERTs closely work with National CERT to respond to cybersecurity incidents.

Also, the Ministry of Information Technology is empowered to issue directions for blocking for public access to any information generated, transmitted, received, stored or hosted through any computer resource as per rules prescribed under Section 69A of IT Act, 2000. Such grounds lie whenever Central or State government is satisfied that it is necessary for the interest of sovereignty or integrity of India, defence of India, the security of State, friendly relations with foreign states or public order to block any online content.

National Cybersecurity Policy 2013 aims to create a secure cyber ecosystem in India, provide security and safety in the use of Information Technology systems and online transactions and to extend benefits of Information Technology in all sectors of the economy.

Role of Ministry of Home Affairs

Ministry of Home Affairs deals with matters relating to Cybersecurity, Cybercrime, National Information Security Policy & Guidelines (NISPG) and implementation of NISPG, NATGRID etc. The Ministry has divisions that issue advisories and drives capacity building initiatives and issues grants to states to set up cyber forensic labs to combat cybercrimes in India. MHA is responsible for Coordination with CERT-In, NCSC, National Critical Information Infrastructure Protection Centre, MEA, IB, Deity, Defence etc. MHA deals with NISPG policy and its implementation/compliance in other government organisations. It also grants permissions for interception/blocking of web traffic under Section 69 of IT Act, 2000. Whenever Central or State government is satisfied that it is necessary in the interest of sovereignty or integrity of India, defence of India, the security of State, friendly relations with foreign states or public order, it has the power to direct any agency of appropriate government to intercept, monitor or decrypt internet traffic of computer resource. The permission to make such interception is granted by Secretary, MHA as per guidelines issued under Section 69 of the IT Act,



2000. Failure to abide by the mandate is an offence punishable with up to 7 years of imprisonment and fine.

The **National Critical Information Infrastructure Protection Centre** (NCIIPC) is the National Nodal Agency for the protection of critical information infrastructure. **National Cyber Coordination Centre (NCCC)** provides real-time incident awareness and rapid response to cybersecurity incidents and exchange of information for proactive, preventive actions by individual entities. Representatives of all stakeholders, including the armed forces, are part of the NCCC. Following are the organisations represented in the NCCC:

National Security Council Secretariat- coordinates and oversees cyber security issues, including Cyber Diplomacy.

MHA – manages Cybersecurity, Cybercrime, National Information Security Policy & Guidelines (NISPG) and implementation of NISPG, NATGRID

MEA -main role in cyber diplomacy, prevention of cyber conflicts and war, international law and treaty arrangements.

MEITY/CERT-IN/NIC/STQC - To promote e-governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITeS industries, enhancing India's role in Internet Governance, promoting R&D and innovation, enhancing efficiency through digital services and ensuring secure cyberspace, promotion of information technology education and Information Technology-based education. Issuance of digital signatures are under body of CCA.

DOT- deals with Policy, Licensing and Coordination matters relating to telegraphs, telephones, wireless, data, facsimile and telematic services and other like forms of communications.

MOD/HQ IDS/Armed Forces- Defence threat intelligence platform, formulation of strategic defence policy, operations, structures to combat cyber threats

NTRO is set up for the protection of critical infrastructure for internal and external security with intelligence bureau monitoring cases of terrorism and insurgency.

DRDO - Evolving Information Security Policy and its implementation across DRDO through various laboratories/ establishments, Increasing Information Security Policy awareness and training

Industry/TSP/ISP- Promote Internet/ Broadband for all, develop & establish a secure & robust infrastructure for internet penetration

Police, Forensic Labs

In the case of cybercrimes, an FIR is registered by the complainant at the earliest instance and such jurisdiction is made out either at the place where the offence is committed or in some cases such as cyber defamation where the complainant is defamed. Different states and units have created cybercrime police station to handle millions of growing cybercrimes. India has more than 30 cyber cells notified and 39 forensic labs (Central & State) have been notified by the government to support cybercrime investigations. In case if an investigation is to be made abroad, where an accused person has escaped from the country after committing a crime or part of the crime has been committed outside the country or the witness and other material then the investigation may be required to be made in another country. Informal information or material leads may be collected through designated intelligence agencies. The international police cooperation cell is the designated agency for routing requests for informal enquiries to be made with National Central Bureau of other countries, Interpol Headquarters as well as our Missions abroad. It may become necessary to send police from India to another country for investigation for which express consent of the country will be required and some formalities are prescribed.

In order to sensitize and train judiciary and police officers in investigating cybercrimes, several organisations such as the National Judicial Academy, National Police Academy, National Investigation Agency, CBI and BPR&D conduct various training in cyber law to train its officers on cybercrime and investigation from time to time.

Many laws enforcing agencies including Central Bureau of Investigation have created separate units or cells for handling cybercrimes.

CCTNS and National Intelligence Grid are India's two largest databases for information related to international crime and criminals.

Courts

There are no separate criminal courts set up under the IT Act, 2000. However, for claiming compensation, secretary (IT) of all states have been empowered to grant compensation for unauthorised access, copying of data or other grounds set out in Sec 43, 43A of the IT Act,2000. Appeals against orders of this Authority are filed before the Telecom Dispute Settlement and Appellate Tribunal.

In order to conduct formal investigation and collection of evidence under Section 166-A of CRPC, 1973 through a competent court a letter rogatory is prepared within the ambit of Mutual Legal Assistance Treaty (MLAT), MOU b/w India and requested country or on the basis of reciprocity in case no such Treaty and MOU exists. India has signed MLATs with approx. 39 countries to date.

At times provision of an International Convention to provide such cooperation may be used where both India and requested country are a signatory. No request for issue of Letter Rogatory (LR) can be brought before a court by an investigating agency without prior permission of Central authority which is Ministry of Home Affairs. Before making a proposal to MHA an investigating agency needs to examine the matter whether it is necessary to get investigation conducted abroad and study the MLAT provisions for applicable principles such as dual criminality. Where no such bilateral or multi-lateral arrangement exists, LR can be made on the basis of assurance reciprocity. India has not signed any Cybercrime Convention so far to evince effective cooperation from international agencies/member countries and is unable to effectively deal with trans-border cybercrime such as cyber-attacks, pornographic rackets involving multiple jurisdictions.

Incoming LR in India

All incoming LR are received by Under Secretary (Legal), Internal Security Division, Ministry of Home Affairs, Lok Nayak Bhawan, New Delhi 110003 and are entrusted to an Investigation Agency (State Police/CBI) in consultation with Joint Director (Policy) in CBI. Where LR needs to be executed through the State Police, it will be sent to IPCC, CBI for getting it executed by the State Police concerned. The agency entrusted with the task of execution of LR would execute it in terms of the provisions of the MLAT, MoU and Arrangement etc., if it exists with the requesting country otherwise the evidence shall be gathered under the provisions of Indian laws, as applicable.

Handling of extradition requests

Extradition is either done under the Extradition Treaty or other Extradition Arrangement or Assurance of Reciprocity with the requesting country. Extradition request can be generally made only after a charge-sheet has been filed in the court and the court has taken cognizance of the case. If the accused available in other country is to be arrested and produced in the court in India, the requisite action to bring such accused to India is through Extradition Process. The principle of dual criminality is invariably followed for extradition requests. An accused extradited for a particular offence can be tried only for that offence by the receiving

country. The State investigating agency sends extradition requests to the IPCC, CBI, New Delhi through the State Home Department who would, in turn, send the same to MEA for further necessary action.

Ministry of Finance regulates laws governing banks, financial services and is empowered to issue policy measures to prevent and combat cybercrimes. It allocates budgets for R&D including in the domain of increasing cybersecurity capacities and connected R&D.

Industry bodies: At the industry front, NASSCOM and DSCI have emerged as major players in creating standards for securing data and privacy of consumers and enterprises. DSCI also establishes a national skills registry for background checks and verification of IT professionals employed by the industry and cyber labs programmes to train law enforcement. Both NASSCOM and DSCI have setup cyber labs across different states of India. DSCI has issued standard operating procedures for the investigation of cybercrimes (Cybercrime investigation Manual 2011).

Emerging Challenges In Combating Cybercrimes

Emerging challenges in combating cybercrimes in India include lack of homogeneity in cyberspace laws as different countries have different laws and definition and punishments for cybercrimes vary. India is not a signatory to any cybercrime convention yet but has signed MLAT with only about 39 countries in general criminal matters. The timelines of response in such MLATs is quite long and the process is quite slow as a result of which most electronic evidence is either lost or tampered. However, India has made recent efforts to foster its bilateral/multilateral cooperation with other countries and has formed agreements with Bangladesh, Brazil, Bulgaria and other countries to build its cyber diplomacy. ■

Source: Gateway House Research

1. India should consider playing a proactive role in UN Government Group of Experts level and work towards providing technological cooperation among governments and private sector to protect technical infrastructure across nations. It should incorporate principles enunciated in Tallinn Manual to emphasise the law on state responsibility, due diligence and obligations of cooperation. It is important to address issues of 'countermeasures' and 'self-defence' in cyberspace and to develop clarity on the operation of humanitarian principles in cyberspace.

2. India is a signatory to the International Covenant on Civil and Political Rights (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR), therefore it's important that India continues to work towards digitally empowering its citizens and allocate effective resources on skilling, capacity building its manpower in this domain. Of late, India has made commendable efforts through its Digital India mission, Aadhar ID Project, Bharatnet and other initiatives. Countries like Rwanda, Morocco and Sri Lanka are adopting India's Aadhar-based national identity card project and the India Stack technology infrastructure.

3. India is a member of the Global Commission on the Stability of Cyberspace (GCSC). It is a multi-stakeholder initiative of the Hague Centre for Strategic Studies and the East-West Institute that aims to create a logical set of unified norms and policies that make cyberspace safer and more stable across the member countries. From a private engagement standpoint, Tech Accords, Digital Geneva Convention and Charter of Trust are excellent private initiatives of ICT companies that bring forth collective action of private ICT companies in creating safer cyberspace. India should consider becoming a member of such industry-led initiatives too.

4. A major challenge in combating cybercrimes is that of the technology itself & insufficient extant national legal frameworks too. The law needs to catch up with the pace with changing technologies. In times of Artificial Intelligence and dark web, smart cities, big data and machine learning, new emerging threats pose a threat to our nation. It is thus imperative to constantly amend the existing laws or create new laws to combat the rise in cybercrimes. For instance, India does not have a fake news law or any policy to regulate social media or online gaming industry to date. The increase in the use of social media has generated multiple crimes some of them juxtapose with other crimes making it complex for LEAs to act such as organised transborder rackets involving simultaneous identity theft, bot attacks, extortion, cyber pornography & online grooming of children. India needs to amend the Cybersecurity policy 2013 as well as the IT Act, 2000.

5. India needs to avoid polarisation. Neither should it be overzealous on regulating the internet as in the case of China nor should it be too liberal that it has a weak framework to protect its own nation and its people. A balanced and multipronged stakeholder approach (both at the national level and from a global standpoint) will bring greater acceptability in the creation of new laws and policies and lead to greater inclusion and transparency. A positive standpoint India took recently was on the issue of Net neutrality. A multi-stakeholder PPP model has proven successful in developing new internet governance policies as well in developing R&D initiatives in the digital economy.

6. It is important to develop a robust cyber ecosystem of organisations which play an important role in combating cybercrime. Some of these organisations and their roles have been briefly outlined herein. However, the overlap needs to be removed, clear defined roles need to be spelt out and seamless coordination is needed to share real-time intelligence, and then develop strategies to prevent, operate against and combat cybercrime more effectively.

7. The Defence Cyber Agency/Cyber Formation requires to be integrated with existing national institutions and agencies are responsible for various aspects of cybersecurity. We need enabling policies, structures, processes, and information exchange to create a robust investigation ecosystem across all investigation agencies to effectively combat cybercrimes. This is aptly elucidated by the recent report issued by VIF titled Credible Cyber Deterrence in Armed Forces of India. The armed forces ought to be involved in the decision-making process, and collaborate with major stakeholders to address techno-legal challenges that continue to hinder timely intelligence, investigation and research and development in cybercrime matters.

Thus, both at the national level and internationally India needs to proactively work towards making cyberspace safer, participate in Cyber diplomacy initiatives and continue promoting the use of ICT to bolster its developing digital economy. This needs the creation of a clear set of norms, policies, organisational roles, operations, processes, robust legal framework and enhancing extant enforcement mechanisms. India needs to lead from the front, be proactive at the United Nations working group discussions concerning cyberspace, and participate in various private/industry alliances initiatives /multipronged /PPP models to further its objective of combating cybercrimes more efficiently.