A Study of Need for Police Reforms in India in Cyber Crime Manner

Amritanshu Sharma\textsuperscript{1}, Dr. Depika Bhatnagar\textsuperscript{2}

Research scholar\textsuperscript{1}, Adjunct Faculty\textsuperscript{2}

Oriental School of Law\textsuperscript{1,2}

Oriental University Indore, Madhya Pradesh, India

Abstract:

As more and more of our work digitized chances of leaking of data seems improbable and the problem of law enforcement officials, individual and companies need to bear the cost of crime and loss. Digital technology and the internet are providing criminals with new opportunities to commit crime. It is now essential that police officers have the capability to deal confidently with the cyber element of crimes as it is fast becoming a dominant method in the perpetration of crime. But more than that, it is becoming a part of everything that the police have to deal with because the internet and digital are part of most people's lives now. After the advent of computer revolution started in India, most of our activity Connected with the internet and we are directly and indirectly transact with the borderless Cyber world. This paper describes the various challenges of law enforcement agencies faces in handling cyber crime, cyber crime legislative standards across jurisdictions, introduction of specialist force to combat cyber crime and finally, suggestions and conclusions are highlighted to modernize police force capacity to tackle the crime.

I. INTRODUCTION

After the number of user increased the challenges for our police force to adopt different strategies to fight crime in virtual world is need of the hour for prevention and nab the criminals involved in the cyber crime. Financial institutions do not always report crimes committed against their customers because they are concerned about customers losing their confidence in the security of the institutions' computer systems. This makes it difficult for police forces to effectively identify and understand threats, risks and harm posed by cybercrime as they do not have all of the necessary information they need. The complaint need to go specific cyber security cell police station not to all the police station for lodging the complaint, lack of awareness and distance factors results many cases being unreported. Rapid deployment team This is the newest of the national threats to require a national response by the police service. A large-scale cyber incident could be caused by either the aggregation of individual cybercrimes or the commission of a single attack. We need to classify the threat based on the level of impact.

- Large scale incident, Terrorism, Financial institution, Threat to public law disorder, attack on government online services
- Medium scale incident “Corporate level” data theft
- Small Scale Incident “fraud, child bullying, identify fraud offences The threat of a large-scale cyber incident is the newest of the national threats to require a national co-ordinate response by the police and the national law enforcement and intelligence agencies. 1. In case of large-scale cyber incident National Level Computer Emergency Response Team (CERT-In) co-ordinate with National Critical Information Infrastructure Protection Centre, rapid deployment team should be created in every state that connect locally, regionally, nationally to deploy at short notice to reduce the risk of disruption and improve the security posture. Rapid deployment team consists of computer specialists in cybercrime. In the form of high-tech crime investigators who recover evidence from computers, covert internet investigators (CII). Interagency cooperation Proper co-ordination and support between the departments is necessary for uniformed operations, internal communication should be strengthen by establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure. 2. Law enforcement powers to obtain digital evidence When dealing with cyber crime for LEAs to be able to quickly secure digital evidence, often in multiple jurisdictions, to ensure that it is retained and the forensic quality of the evidence is preserved. 3. In getting information for forensic analysis from overseas ISPs and telecommunication services is often too slow to identify an offender. Data is generally not received in time to be submitted to court. Inconsistent legislation or a lack of cyber crime offences can also mean that individuals based overseas escape extradition and prosecution for cyber offences because there is no similar offence in the country of origin. If international cooperation is done on a police to police basis tedious process will be changed which make it easy to obtain evidence to identify offenders fast enough to enable a prosecution. 4. For example, inconsistent telecommunications intercept data retention laws can mean that evidence that would be complexities of securing electronic evidence (e-evidence) of any type of crime or economic offence. The National Cyber Security Policy of 2013 refers to effective law-enforcement capabilities for investigation and prosecution of cybercrime, but not to the broader issue of electronic evidence. Securing e-evidence is an increasingly complex undertaking. The sheer volume of cases involving e-evidence, the number of devices, users and victims involved, and technical complications such as encryption present major challenges. The transnational nature of e-evidence, it may be stored in foreign jurisdictions even in cases that are otherwise fully domestic, combined with the transversal scope of e-evidence, in that any crime may entail such evidence, has implications on international cooperation in criminal matters. Most mutual legal assistance (MLA) requests for e-evidence are

http://ijesc.org/
not related to cybercrime but to fraud and financial crimes followed by violent and serious crimes. Given the volatility of e-evidence, the mutual legal assistance process is rather inefficient. Response times of 6 to 24 months to MLA requests appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the obligation of governments to protect society and individuals against cybercrime and other crime. Securing e-evidence for criminal justice purposes is particularly challenging in the context of cloud computing where data is distributed over different services, providers, locations and often jurisdictions, and where mutual legal assistance is often not feasible. It risks failure of governments in their obligation to protect the rights of individuals and society against crimes and loss of faith in the rule of law. Cloud computing further complicates the matter. MLA requests are about cooperation between competent authorities. But if evidence is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions, it is difficult to identify to which authorities to send a request. Furthermore, law-enforcement powers are tied to the principle of territoriality, meaning that a criminal justice authority can only enforce its laws, such as ordering a service provider to produce data, or searching and seizing a computer system, on its own territory. The Indian Ministry of Home Affairs, which serves as the nodal agency for MLA 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 cybercrimes. This realization has caused the US and UK, for instance, to negotiate a direct data sharing agreement that would allow UK to demand data directly from intermediaries holding data in the US. Ainsa quan non for this agreement is a written assessment that UK laws have both substantial and procedural protections for user privacy and that the government has displayed adequate respect for human rights. 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. Investigative powers Electronic communication data is essential to the successful investigation and prosecution of serious crimes (including cybercrime) to effectively prosecute online criminal activity. A broader issue relating to cyber crime is police powers, such as access powers. By allowing a warrant to be obtained for remote access, law enforcement is more likely to be able to decipher encrypted data by conducting surveillance at a point between the user and the encryption interface. This would involve remotely accessing (or hacking into a computer via the internet to obtain transmissions of product passing over that computer at a point at which it is unencrypted. While the FBI is only recently starting toes the boundaries of Rule 41s amended language Rule 41(6) (a) (b) of the Federal Rules of Criminal Procedure and Clarifying Lawful Overseas Use of Data) Act (CLOUD) Bill with respect to criminal bonnet investigations, because criminal suspects would often conceal the location of their computers using anonymous proxy servers and other obfuscating technology. India’s data protection bill should have clause based on the Bill to use on critical situation. The bill would allow U.S. law enforcement to access data stored abroad by increasing the reach of the law that federal law enforcement uses to access data, without the cooperation of foreign governments. Law enforcement could order companies to provide data regardless of the location of the data or data subject. This would mean that U.S. courts would claim global authority. The bill would enable agreements between the U.S. and other governments whose law enforcement would be permitted to directly request data from U.S. companies without adequate protections for user privacy. Cyber security policy-2013, Criminal Procedure Code, Police act 1861 and data protection Bill is silent, hence this would require legislative amendments in Police act 1861, Criminal Procedure Code and data protection Bill by introducing new rule based on the US Rule and Bill will grant the government, Judicial and law enforcement officials greatly expanded search powers and for prosecution of online offenders. The probability of getting arrested or going to jail is low. Not one of the perpetrators of the biggest headline-grabbing breaches has been prosecuted. Law enforcement agencies are stepping up their efforts, but many cybercriminals operate outside of their jurisdictions. Furthermore, efforts have to be made to equip them with: sets Infrastructure for cybercrime investigation unit Infrastructure for cyber forensic units (to aid investigation, which would be in addition to the forensic labs to give expert opinion for evidentiary purposes) Appropriate standard operating procedures (SOPs) 10. Training The police forces capacity and contribution to the response against the national cyber threat is currently limited to the deployment of a relatively small number of specialists, who can be used to investigate cybercrime. Cybercrimes introduce unanticipated risks and effects, creating greater urgency to equip investigators with new skill sets. One such area is the establishment of a cloud computing training platform that comprises a networked and nodal nature, parallel to that of cyber security. This platform can be pivotal to increase shared knowledge and skills for investigators and connect LEAs and stakeholders. This cloud-based training system could encompass functions depicted in the diagram. Traditional modes of training through books, boards, PowerPoint / PDF-based approach are not very suitable for trainings to combat cybercrime. There is need for more practical training, something based on simulated environments. However, given the need of volumes, the proposed methodology should be scalable. The challenges of cybercrime trainings can be summarised as: Traditional PowerPoint/ PDF-based approach not very suitable Number of officers to be trained (volume) Inaccurate assessments of needs of LEAs Standardized curriculum A centralized learning platform provides users from different professions about common objectives to address cybercrimes. Standardized courses enable frontline officers, prosecutors and data analysts with varying levels of cyber knowledge to acquire a consistent overview of investigations such as digital evidence handling, intelligence development and legal procedures. 

Â- Greater knowledge about how their roles contribute to investigations could lead to increased productivity and
efficiency
Â· Collaborative processes among investigators could be more streamlined and integrated at a global scale through this platform.
Curriculum needs to be standardized by keeping in mind different roles of different LEAs and skill sets required for each role. A tentative list of roles would include:
Â· First responder officer
Â· Frontline officer
Â· General investigator
Â· Cybercrime investigator
Â· Cybercrime intelligence analyst
Â· Digital forensics specialist
Â· Head of unit: Investigation/forensics
Â· Senior LEA manager

1.1 Cyber Range or Simulated Cybercrime Scenarios This is the key component of this model. Besides preparation of traditional modes of training through books, boards, power point/PDF-based approach, there is a strong need for more training based on simulated environments. This would mean creation of scenarios, including digital exhibits (logs, etc.) for extraction by trainees using forensic tools preloaded on the infrastructure, using appropriate procedures.

1.2 New modus operandi In cyberspace, criminals keep on adopting new modus operandi every day and therefore, simulation-based training methodology has to be contemporary. To develop new scenarios, it is important to keep abreast of new modus operandi and technology trends. This part would include:
Â· Knowledge exchange on current and emerging methods of operations (or modus operandi) of cybercriminals
Â· Within this platform, training courses could stress-test the computing skills of cybercrime experts to analyze and discern signals collected from hacker forums, internet relay chat rooms and messaging texts
Â· Attacks like phishing and tampering, advanced persistent threats, backend systems and reverse-engineering could be simulated.
Â· Combating cybercrime could take more than technical skills and require cross-disciplinary knowledge. Researchers must look at the best practices to stay ahead of hackers by understanding indicators of malware victimization, the ecology of trust and motivation among hackers, online hacker communication and interaction styles
Â· Gaining practice in such knowledge exchanges could shed light on how hacker communities interact and share information, creating actionable intelligence for cybercrime investigations
Â· Able to develop the best science to help advance cyber security training and research

1.3. Continuous redesign for training material
Â· Feedback gathered from learner usage and experience must be utilized to design new knowledge capacity and material
Â· The modules should be developed by subject-matter-experts, ensuring quality content is constantly updated
Â· Training courses should be more reflective of real-world cases and incidents
Â· Maintain engagement with users by tapping into learners interests, offering appropriate challenges and increasing motivation

1.4. LEA Certifications
Â· This platform could allow performance-based certification to demonstrate that users know what to look for and what actions to take during a cyber incident
Â· Assess if knowledge or skills have been practically transferred
Â· Automated scoring and self-assessments in different areas of cybercrime
Â· Provide critical insights into the effectiveness of training platform

1.5. Environmental scanning of new technology This platform will probe how internet-enabled technologies and wearable’s impact cyber security, policing and how crime could be conceived. A horizontal approach should involve cyber experts and technology innovators of LEAs from different countries share their cyber investigative products and threat assessments. Police agencies should perform SWOT analysis of their cyber capabilities and identify the next steps for improvement, providing insights into the different needs and stages of cyber capacity development for individual countries. Vertically, the expanse of future internet-enabled crimes could be analyzed at national, regional, and international levels

1.6. Synchronized skill levels
Â· This platform will allow new relationships with other nodes within the networks of the cyber security architecture
Â· Effective collaboration and greater harmonization provide a more accurate and comprehensive assessment of cyber criminality, ensuring responses are coordinated, effective and timely
Â· Law enforcement collaborations with the private sector to explore and design complex simulations of future communications technologies that are prone to criminal exploitation, improve cyber security skills at all levels and work with associated professions to make industry more resilient to cybercrime. In addition to training opportunities, Police force needs to seek the assistance of appropriately skilled volunteers to help them improve their skills in tackling cyber threats. Taking into account the demand for new skills to investigate crimes in cyberspace, the necessity to review policing concepts, such as the justification of a breach of public order, the applicability of techniques in policing the real world to the maintenance of order in virtual space, implementation of these instruments in a practical environment remains the highest priority. Public private partnerships are also key in enabling a more pro-active and agile approach to combating cybercrime. The shared responsibility and cooperation between police and the private sector promises to be an effective way of enhancing the effectiveness of addressing cyber-related threats and also in the fight against cybercrime. International agreements International agreement is the need of the hour to address security and the rule of law in cyber world. To overcome these challenges, India should join Council of Europe’s Cybercrime Convention Committee which gives more access and Solutions to enable criminal justice access to evidence in the cloud are a priority of the committee. The Budapest Convention provides for (i) the criminalization of conduct, ranging from illegal access, data and systems
interference to computer-related fraud and child pornography; (ii) procedural law tools to make the investigation of cybercrime and the securing of e-evidence in relation to any crime more effective; and (iii) international police and judicial cooperation on cybercrime and e-evidence. The National Cyber Security Policy of 2013 refers to effective law-enforcement capabilities for investigation and prosecution of cybercrime, but not to the broader issue of electronic evidence. Criminal justice authorities need access to data for use as evidence in criminal proceedings; without data, there will be no evidence, no justice and no rule of law. Increasingly, evidence in relation to any crime is stored in the electronic form on computer systems. This includes serious and violent crime, such as location data in cases of murder or rape, subscriber information related to ransom e-mails sent during kidnappings, data to identify and locate victims of child abuse or data on communications between terrorists. It can be assumed that this is increasingly a reality in India and that a growing proportion of the more than seven million crimes recorded entail e-evidence. The more real-world crime involves e-evidence, the greater the need for law-enforcement officers, prosecutors or judges to have the skills to deal with e-evidence. Major capacity-building within the criminal justice system is required and clear rules for access to e-evidence and its admissibility in court need to be established. The question of procedural law powers to secure e-evidence and, by extension, efficient access to evidence in a transnational and cloud context is a complicated challenge, given the limitations of the MLA process which is normally designed to protect the rights of individuals as well as the interests of states in which evidence is located. With participation in the Council of Europe Convention on Cybercrime would increase India’s ability to obtain international assistance from other parties to the convention in investigating potential cyber crime offences, particularly in relation to accessing telecommunications. This makes international cooperation critical to efforts to criminalize, detect, disrupt, prevent and ultimately to pursue effective law enforcement action.

II. RECOMMENDATIONS AND CONCLUSION

To suggest remedial measures to ensure effective prevention and control of the cyber crimes based on the study following suggestions are recommended:
# Use of Encryption Technology
# Increase number of appointment of cyber forensic consultant.
# Educating the public on cyber crimes cases
# Liberalization of Law relating to Search and Seizure
# Development of Cyber Forensics lab and Biometric Techniques
# Need to establish a Computer Crime Research and Development Centre in every state.
# Need for Universalisation of Cyber Law
# To Combat the Menace of Cyber Terrorism increase training allocation fund once in every 2 years
# Establish Special Cyber Crime Investigation Cell for Hi-Tech Crimes every state.
# Create awareness of Cyber Crimes at the High School level
# Introduce Cyber Laws in the Curriculum in graduation level
# To develop strategies to help decrease the backlog of digital evidence, develop a mechanism to track the timelines of the cyber security team response to report of cyber crime activity
# Re Establishment of Special Cyber Courts to handle Cyber Crime case in every major cities
# View FIR functionality available on Police citizen portals as per Supreme Court guidelines
# Planting of Baits in Cyberspace for Worms and Viruses
# Use of Data Analytical tool to Regulate of Social Networking Sites
# Need for Imparting Training to Officials to Investigate Cyber Crimes
# Encouragement of Cyber Crime Victims to Lodge Complaints
# Increased international law enforcement cooperation among nations and the private sector and investment in more resources for investigation, especially among developing nations
# Modernisation of current processes, such as the Mutual Legal Assistance Treaty (MLAT), which allows governments to enlist the help of other government in cybercrime investigations and evidence collection
# Better collection of aggregate data by national authorities
# Standardization of threat information and coordination of cyber security requirements to boost security in critical sectors like finance
# To implement national working group on cyber crime to maintain dedicated mechanism for the review and development of legislative responses to cyber security police lack sufficient tools to identify offenders or deploy technical capability to remove malicious software. LEAs must have the tools needed to work with international partners in a concerted effort to tackle the cyber crime problem and prosecute the members
# Legislation to support remote access to attack other machines in preventing cyber attack
# To follow Council of Europe Convention on Cybercrime policy adapting measures to our national cyber security policy along the line of the treaty

III. CONCLUSION

An oft repeated quote in the context of the internet is that of Judge Nancy Gertner in Digital Equipment Corp. v. AltaVista Technology: The internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the internet is concerned, not only is there perhaps â€œno there, there, the there is everywhere where there is internet access.17â€ This research paper attempts in pointing out urgent need of legislation and policy formulation in the field of cyber crime investigation. Problem of potential misuse of internet is increasing day by day, its important for law makers, judicial and government to ensure that law reflect updated to tackle the menace of cyber crime and it is time to gear up for law enforcement official to fight computer crime.

IV. REFERENCES


[3]. AusCERT, Submission 30, p.15


[9]. The Economic Impact of Cybercrime No Slowing Down McAfee Labs Threat Report, McAfee, December 2017


[11]. Interpol


[13]. Tatiana Tropina cyber policing the role of the police in fighting the cyber crime. European Police Science and Research Bulletin. Special Conference Issue Nr. 2
