Cyber Policing and Cyber Crime Investigation in India: An overview

Nalini Venuturumilli

Doctoral Fellow, Department of Public Administration, Osmania University, Hyderabad.

Abstract

With the rise of cyber crime, the meaning of the term "space" in relation to crime has changed. We no longer confine ourselves to a geographical understanding of crimes and criminals. As opposed to many traditional crimes, a criminal in cyberspace is not bound by a specific location or physical jurisdiction. The advancements in information and communication technology (ICT) have benefited humanity in a number of ways. However, it has also presented us with enormous obstacles and created chances for crime to use cutting-edge digital tools (Muthukumaran, 2008). The same ICT tools are being used by the deviants to engage in illegal trade, recruit terrorists, commit security breaches and acts of terrorism, among other things, as well as harass, threaten, deceive, harm reputations, extort, and harass others. Due to this, society now views "Cyber Crime" as a serious problem for which governments urgently need to take swift and decisive action. Governments have responded by creating legislation and institutional frameworks to handle the issues presented by the cyber world. However, since the internet is a constantly changing environment, much more work needs to be done to combat cybercrime and investigate it. With this background, this paper discusses of various issues and challenges in the domain of cyber policing and cyber crime investigation.

Keywords: Cyber Crime, Cyber Policing, Policing in India, Information Technology Act, Investigation in India

Understanding of Cyber Policing:

The cyber world has brought about a new paradigmatic transformation in terms of the connectedness of people and places, the ease with which services can be provided, and the swiftness with which transactions may be completed. However, at the same time that opportunities are expanding, risks and vulnerabilities are also growing. These have brought challenges that are unlike any others that have been faced by the law enforcement agency. Because of this situation, the ability of the police to handle these issues, the speed with which policymakers can adjust the framework to suit the demands of the time, and the capability of multiple governments and institutions to collaborate and coordinate with one another are all called into question.

The Information Technology Act, which is the legislative underpinning for India's cyber policing, has created the general parameters for cyber policing in India through its multiple provisions. This was done in accordance with international standards. Under the condition that it adheres to the protocol defined in Section 69 of the Information Technology Act, the government has the ability to intercept, monitor, or decrypt any information that is generated, sent, received, or stored in any computer resource. According to the Information Technology (Amendment) Act of 2008, this authority may be exercised if the Central Government or the State Government, whichever is applicable at the time, determines that doing so is necessary or expedient for maintaining public order, preventing incitement to the commission of any offences related to the aforementioned that are punishable by law, or defending India's sovereignty or integrity, defence of India, security of the State, or friendly relations with other states.

In any circumstance, the method that has been specified must be followed, and any agency of the relevant government must be instructed to record the explanations for the action taken in writing. Both of these requirements must be met. The subscriber or intermediary is responsible for providing any and all facilities as well as technical support when it is required. These include the following: (i) providing users with access to or securing access to the computer resource that contains the relevant information; creating, sending, receiving, or storing the relevant information; (ii) intercepting, monitoring, or decrypting the relevant information, as appropriate; or (iii) providing users with access to the relevant information stored in the computer resource.

The failure to offer the aforementioned facilities and technical support will now result in a fine and a possible prison sentence of up to seven years' duration. The Information Technology Act (IT) was amended by the Information Technology Act of 2008 (Act). According to the newly introduced Section 69A of the material Technology Act, 2008, the Central Government or any of its personnel have the ability to direct the limitation of public access to any content through any computer resource under the same criteria as were specified before.

Section 69B addresses the issue of determining who has the authority to approve the monitoring and collecting of traffic data or information through any computer resource for the purpose of ensuring cyber security. Because of the Information Technology (Amendment) Act of 2008, the Central Government has the ability to grant any government agency the authority to monitor and collect traffic data or information that is generated, transmitted, received, or stored in any computer resource. This is done in order to improve cyber security and to identify, analyse, and prevent any intrusion or spread of computer contamination throughout the nation. When it comes to the question of how different organisations and governments might work together to combat cybercrime, the issue of cybercrime drags us into the domain of not just intra-state or inter-state but also worldwide levels of cooperation.

Benyon et al. have brought up the possibility of international coordination between law enforcement agencies that are investigating or working to prevent digital crime at one of three levels, namely macro, micro, or both. At the macro level, governments and international bodies frequently work together, particularly through the organisations Europol and Interpol. On a smaller scale, it is possible for the police departments or law enforcement bodies of multiple country states, such as the PcEU in the United Kingdom and the FBI in the United States, to work together on an investigation. According to Bryant and Stephens (2014), human encounters between researchers are a common form of collaboration at the micro level.

Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, is the first worldwide treaty to combat internet and computer crime by harmonising national laws, improving investigative methods, and encouraging international cooperation. This was accomplished through the Convention on Cybercrime, also known as the Budapest Convention on Cybercrime. On the first of July in 2004, the Convention will officially enter into force. The Convention has not yet gotten support from the international community due to the fact that India was not involved in its drafting, and other states fear that it may violate their sovereignty if it is implemented.

It is generally agreed upon that public authorities, not the government, should be in charge of maintaining order on the internet, which is primarily a function of the latter. However, academics have emphasised that in addition to publicly financed or state-supported policing, corporate and non-governmental policing can also be utilised to monitor the cyber world (Halder & Jaishankar, 2016). It is absolutely necessary, in order for cyber policing to be successful, to construct synergies between public, corporate, and non-governmental policing.

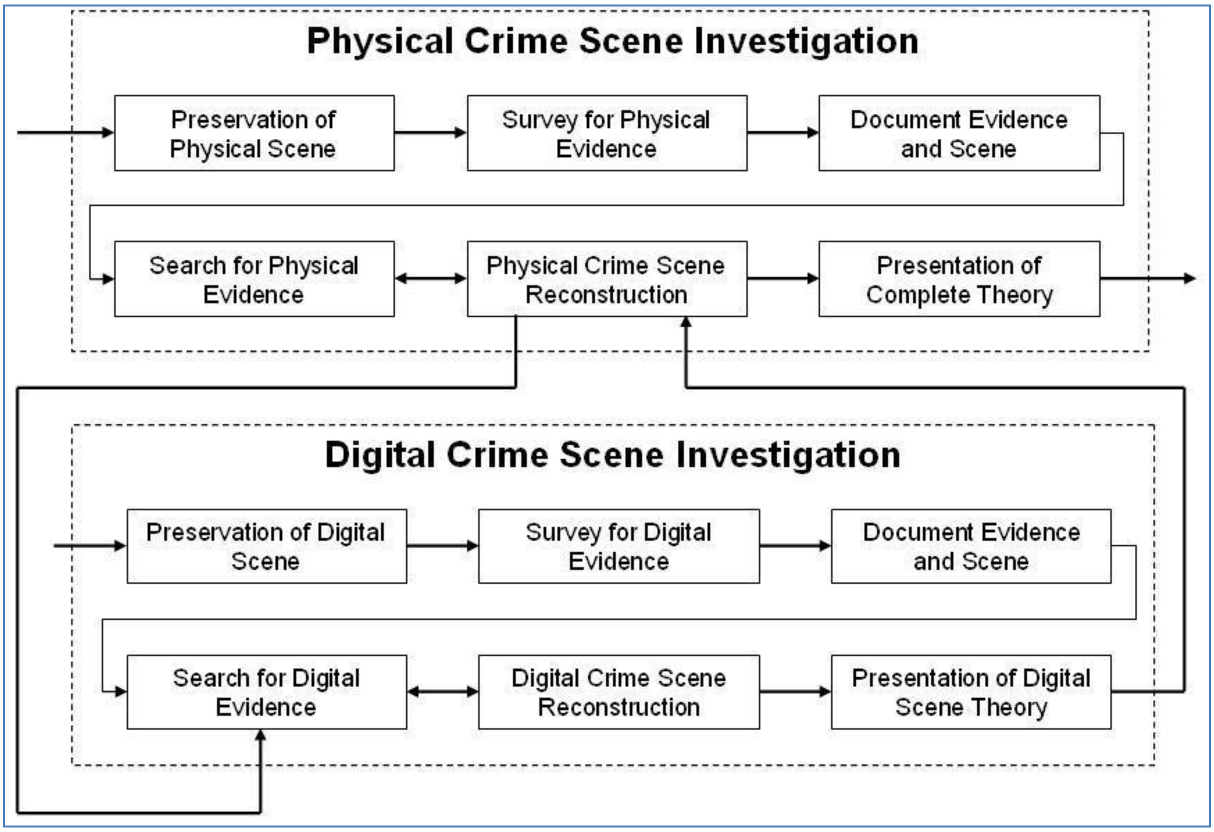
It is becoming increasingly difficult to police the internet as a result of the ease with which "offender mobility" can be achieved (Yar, 2005). In addition, despite the existence of cybercrime treaties, cross-jurisdictional cybercrimes may be difficult to investigate and prosecute when there is antagonism or a hostile relationship between two nations (Chang, 2013). The presence of the offender in many jurisdictions makes it more difficult to conduct cyber policing, and this difficulty is compounded when the offender remains anonymous.

Understanding of Cyber Crime Investigation:

According to O Ciardhuain's statements, "a good model of cybercrime investigations is important" (Bryant & Kennedy, 2014). This is due to the fact that it provides an abstract reference framework, one that is not dependent on any particular technology or organisational setting, for the discussion of methodologies and technologies that are intended to support the work of investigators.

In 2004, O Ciardhuáin presented one of the models that was considered to be the most theoretically sound. His "Extended Model of Cybercrime Investigations" is comprised of the 13 activities that are outlined in the following list:

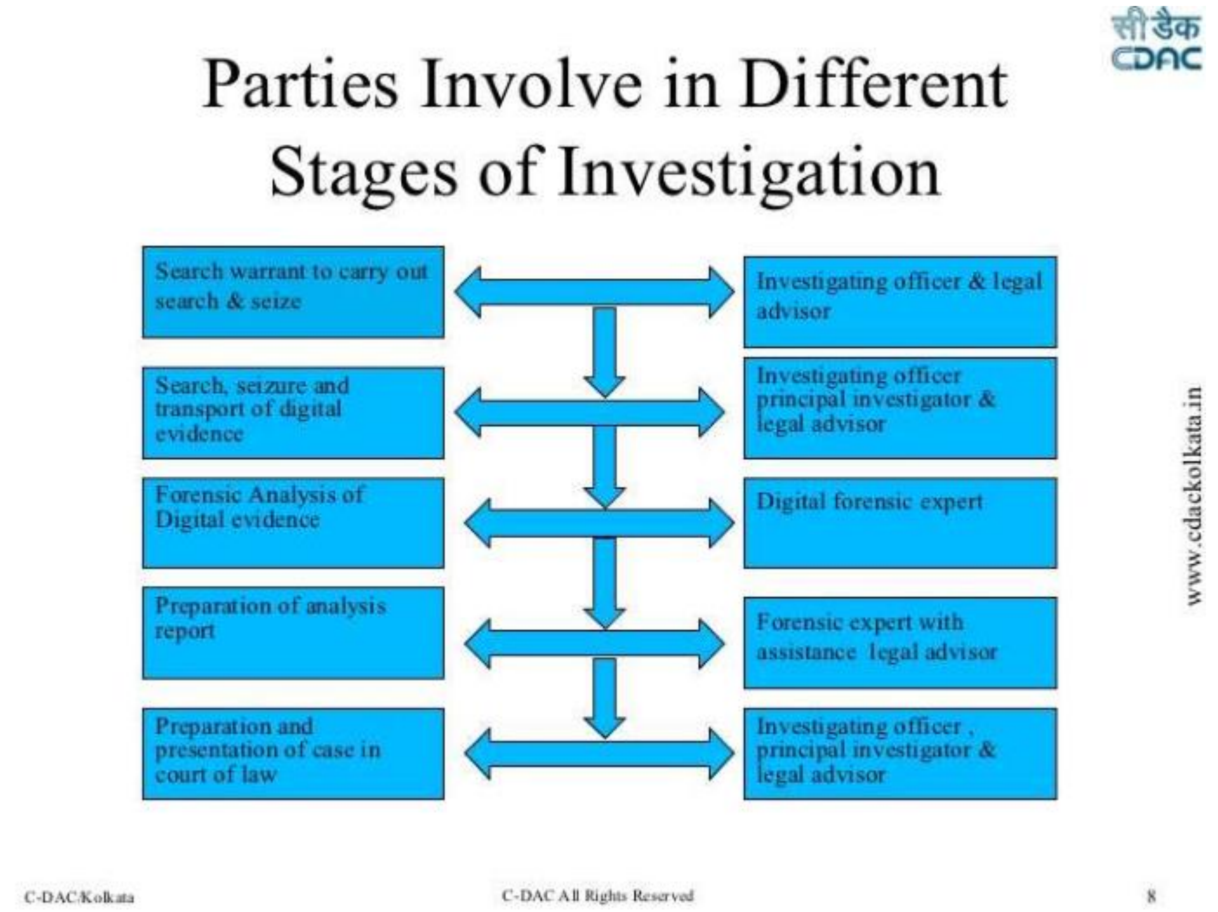
1. Awareness - Recognition that an investigation is needed
2. Authorisation - For example, through the issuing of a warrant
3. Planning - Using information collected by the investigator
4. Notification - Informing the subject and other interested parties that an investigation is taking place
5. Search for and identify evidence - For example locating the PC used by a suspect
6. Collection of evidence - Potential evidence is taken possession of
7. Transport of evidence - Transported to an appropriate location
8. Storage of evidence - Storage methods should reduce the risk of cross contamination
9. Examination of evidence - The use of specialist techniques e.g. recovery of deleted data
10. Hypothesis - A tested formulation of what may of occurred
11. Presentation of hypothesis - For example to a jury
12. Proof/defence of hypothesis - Contrary hypotheses will also be considered
13. Dissemination of information - The information may influence investigations in the future (Bryant & Kennedy, 2014).


Physical Crime Scene Investigation
Preservation of Physical Scene
Survey for Physical Evidence
Document Evidence and Scene
Search for Physical Evidence
Physical Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation
Preservation of Digital Scene
Survey for Digital Evidence
Document Evidence and Scene
Search for Digital Evidence
Digital Crime Scene Reconstruction
Presentation of Digital Scene Theory

Source: http://www.dynotech.com/articles/images/crimescene.jpg

In order for us to have a complete understanding of this module, it is necessary for us to have an understanding of how investigations of cybercrime are conducted in India. According to Section 78, which stipulates that "notwithstanding anything contained in the Code of Criminal Procedure, 1973," a police officer with the rank of Inspector or higher has the ability to investigate any offence committed under this Act. This authority is shown by the fact that "notwithstanding anything contained in the Code of Criminal Procedure, 1973," In addition, Section 80 confers upon law enforcement officers and other officers the authority to enter, search, and conduct other investigative activities. Any police officer with a rank not lower than that of Inspector or any other officer of the Central Government or a State Government authorised by the Central Government in this regard may enter any public place and search without a warrant any person found there who is reasonably suspected of having committed, committing, or being about to commit any offence under this Act [regardless of anything contained in the Code of Criminal Procedure, 1973]. This provision applies to any officer of the Central Government or a State Government authorised by the Central Government in this regard.

A person who is detained in accordance with the provisions of subsection (1) by an officer who is not a police officer must, according to subsection (2) of the IT Act, as amended in 2008, be brought or sent before a magistrate who has relevant jurisdiction or the officer-in-charge of a police station without undue delay. This provision was added after the IT Act was amended in 2008.



सीडैक CDAC

Parties Involve in Different Stages of Investigation

Search warrant to carry out search & seize ⟷ Investigating officer & legal advisor

Search, seizure and transport of digital evidence ⟷ Investigating officer principal investigator & legal advisor

Forensic Analysis of Digital evidence ⟷ Digital forensic expert

Preparation of analysis report ⟷ Forensic expert with assistance legal advisor

Preparation and presentation of case in court of law ⟷ Investigating officer , principal investigator & legal advisor

www.cdackolkata.in

C-DAC/Kolkata C-DAC All Rights Reserved 8

Source: https://image.slidesharecdn.com/ cyber forensic standard operating procedures-111212225028- phpapp01/95/ cyber-forensic-standard-operating-procedures-8-728.jpg?cb=1323730615

Critical view of Cyber crime and Cyber Policing:

In the fast-paced, ever-changing world that characterises the fields of cyber policing and cyber crime investigation, there are an abundance of challenges and obstacles that need to be overcome, as was previously said. These have been discussed in the following ways:

Legal Framework

The most critical issue in cyber policing and investigation of cyber crime is the legal framework within which it operates. Before the Information Technology (IT) Act, 2000 was passed, the cyber world in the context of India was unregulated, and there was doubt among the law enforcement authorities regarding the acceptable course of action to be followed in response to criminal offences that were committed in cyber space. A legislative initiative that resulted in the creation of the IT Act, 2000 was responsible for defining cybercrime and making cyber policing and investigation a practical possibility for the first time. In addition, as a result of the dynamic nature of the Act, it was determined to be necessary to modernise a number of its provisions, which was accomplished in the year 2008. The authority to investigate cyber offences was delegated to an Inspector, as opposed to the Deputy Superintendent of Police, as was provided by the legislation that had been in place previously. This Act also covers additional types of illegal activity that might be committed online, such as cyberterrorism and child pornography. As a consequence of this, the legal framework aims to provide responses to a number of questions, one of which is the following: what kind of behaviour in cyberspace would be classified as a cyber crime? What kind of investigation will be conducted on that computer crime? What kind of consequences might someone face if they were caught committing such a cybercrime? In the context of the internet, what exactly constitutes "evidence"?

Nature of Cyber Policing

In light of the typology that Halder and Jaishankar (2016) have proposed, one question that immediately comes to mind is, "What exactly is the nature of cyber policing?" Should public policing take on the challenge of the growing threat posed by cybercrime on its own, and is it even capable of doing so? Or, for the best results, should non-governmental organisations (NGOs) or the private/corporate sector be involved? The interaction of all three factors will, without a doubt, result in original approaches to solving the challenges. It is also essential to keep in mind the ever-changing "cyber-threat landscape" and how it affects policing (Wall, 2007, 2010, and 2015). All of this provides strong evidence that cyber policing ought to be increased in terms of both its scope and its reach, and that additional stakeholders ought to be incorporated.

Cyber Crime Investigation

The ability to investigate cybercrimes is mentioned in Section 78 of the IT Act, and Section 80 of the Act grants police officers and other officers the right to enter, search, and other similar activities. As more serious cybercrimes are reported, one would expect to see a proportional increase in the number of people convicted of those crimes. This has not always been the case, however, as evidenced by the fact that countless investigations and prosecutions have been put on hold. According to Brown (2015), the primary reasons for this result include trans-jurisdictional barriers, dishonesty, and the incapacity of significant actors in the criminal justice systems to appreciate the fundamental aspects of technology-assisted crime.

The majority of regions only have one or a very small number of police stations that are dedicated to investigating cybercrime, which may not be enough to keep up with the exponential rise in the number of crimes that are committed online. In addition, it is difficult for victims to get in touch with specific police stations in order to submit complaints (Kaumudi, 2016).

The core challenges in cyber crime investigation are:

- There is shortage of trained cyber investigators.
- Very few cyber forensics facilities are available in Forensic Labs.
- There are delays in receiving reports due to huge backlog.
- There is lack of institutional mechanism to obtain help of cyber experts from industry.

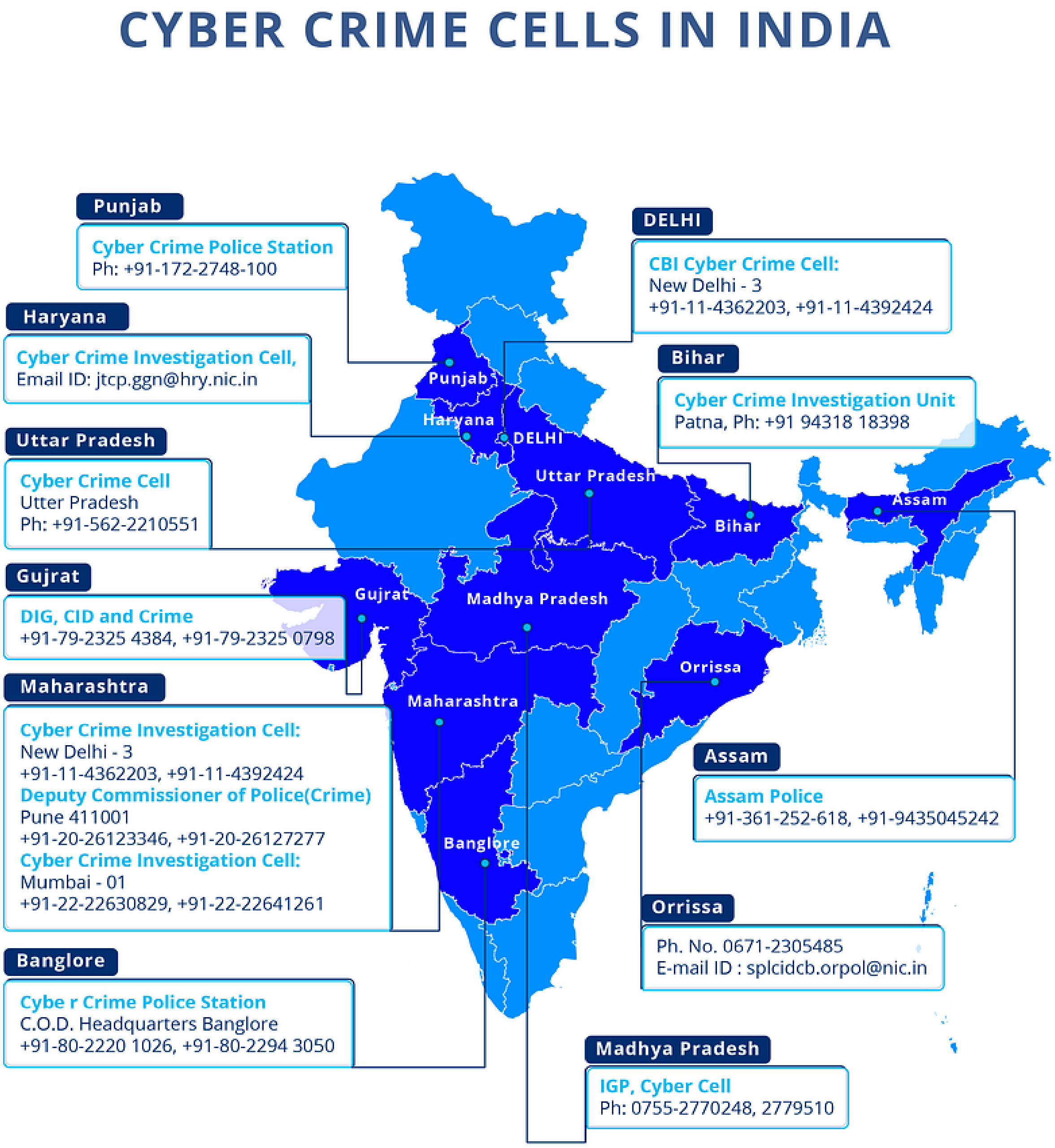
Coordination between Countries/ International Protocol – Criminal Investigation

According to Jaishankar (2008), persons who travel in virtual space have characteristics that are completely distinct from those who move in physical space. Because of the release from inhibitions, anonymity, and geographic isolation given by internet, crime and criminals now require a new interpretation. It's likely that the people who commit crimes against others online don't actually live in the same place as the people they victimise. On the other hand, it's feasible that they couldn't be more opposite of one another. In this particular scenario, the investigation process is required to take into consideration not only the laws of the nation's individual states, but also, on occasion, the laws of foreign nations. Because of this, the legal authorities of the many nations and countries need to increase their level of coordination, understanding, and collaboration with one another.

Capability of Law Enforcement Machinery

The capability of the machine is a crucial issue that needs to be addressed in the field of cyber policing and the investigation of cyber crime. When figuring out how effective a piece of equipment is, one of the most important factors to consider is the skill set of the people who work in the cyber crime investigation cells or units. The fundamental hiring standards that have been created for the nation's police force will make the problem much worse. The Indian Police Organisations need to employ and make use of the most knowledgeable individuals they can find in the realm of cyber technology in order to meet the difficulties posed by inventive but deranged brains.

In one of his earlier pieces of writing, the author made the observation that cybercrime offers new challenges because the organisations that are tasked with investigating such crimes do not have the requisite skills to carry out their tasks and because the underpaid police officers are unsure of what to do (Mehta, 2009). Because of financial fraud and mismanagement, the traditional methods of investigation need to be revised as well. The circulation of fake currency poses a significant challenge to India's national security at this time. However, this is precisely what forces that are hostile to India's ascent have been seeking to do (Mehta, 2009). The destabilisation of the Indian economy at a crucial moment in its development is the last thing we should be anticipating and the last thing we should expect to happen.



CYBER CRIME CELLS IN INDIA

Punjab
Cyber Crime Police Station
Ph: +91-172-2748-100

Haryana
Cyber Crime Investigation Cell,
Email ID: jtcp.ggn@hry.nic.in

Uttar Pradesh
Cyber Crime Cell
Utter Pradesh
Ph: +91-562-2210551

Gujrat
DIG, CID and Crime
+91-79-2325 4384, +91-79-2325 0798

Maharashtra
Cyber Crime Investigation Cell:
New Delhi - 3
+91-11-4362203, +91-11-4392424
Deputy Commissioner of Police(Crime)
Pune 411001
+91-20-26123346, +91-20-26127277
Cyber Crime Investigation Cell:
Mumbai - 01
+91-22-22630829, +91-22-22641261

Banglore
Cybe r Crime Police Station
C.O.D. Headquarters Banglore
+91-80-2220 1026, +91-80-2294 3050

DELHI
CBI Cyber Crime Cell:
New Delhi - 3
+91-11-4362203, +91-11-4392424

Bihar
Cyber Crime Investigation Unit
Patna, Ph: +91 94318 18398

Assam
Assam Police
+91-361-252-618, +91-9435045242

Orrissa
Ph. No. 0671-2305485
E-mail ID : splcidcb.orpol@nic.in

Madhya Pradesh
IGP, Cyber Cell
Ph: 0755-2770248, 2779510

Source: https://cdn-images-1.medium.com/max/800/1*MJoQki-HRgEX9OTGbw7o1g.png

Manpower/ Personnel

The creation of an institutional structure and the provision of adequate resources to that framework is an additional essential precondition that must be met. It is necessary for there to be an adequate supply of trained labour accessible to the Units and Cells. Because of the global character of computer crime and the digital environment, which has exceeded the capacity of any one agency, state, or country to independently handle this new paradigm shift in crime, more knowledgeable and skilled specialists are now needed. In a nutshell, the demand for these professionals has arisen as a direct result of the global nature of computer crime and the digital environment. These newly trained and educated workers will be needed for our forensic computer investigation units as well as for a variety of sub-disciplines within the emerging body of knowledge (Johnson, 2005). This emerging body of knowledge is also known as computer forensics, information assurance, computer security, and software security. These new workers will need to be provided by the universities in our country.

The training that is required for duties such as getting information from the internet, conducting network forensics, tracking emails, tracking mobile devices, tracking social media, and conducting link analysis is not provided to regular police personnel. As a result, it is helpful to engage professionals that have the most recent technical know-how when conducting tough investigations. All of these different types of training, including forensic analysis certificate courses, network security certificate courses, network tracking certificate courses, call tracking training, onsite analysis training, and so on, need to be made available to the cyber employees.

Supreme Court Judgment of 2006 & Model Police Act

According to the judgement handed down by the Supreme Court of India on September 22, 2006 in the case of Prakash Singh and Others Vs. Union of India and Others, there was a directive that was included in the decision that stated, "The investigating police shall be separated from the law and order police to ensure faster investigation, better expertise, and improved rapport with the public." The directive stated that this separation was necessary to ensure these things. Nevertheless, full coordination between the two wings is something that needs to be accomplished. This point was further driven home in the Model Police Act of 2006, which was passed in 2006. In addition to this, a number of state legislatures have passed resolutions that are identical to these statutes.

The conclusion is that the individuals need to obtain specific training, and given the current state of the criminal environment, policing and investigating cybercrime is not a work that can be considered regular. The staff needs to be carefully selected, educated, and allowed ample time to improve their skills over the course of a longer period of time.

Evolving Crimes

The practise of cybercrime has evolved over time and gotten more complex as a result of this development. It has caused us problems in the form of viruses, worms, ransomware, phishing, hacking, malware, and botnets, to name just a few examples of these types of threats. This development was demonstrated by the recent "WannaCry" ransomware attack, which targeted a great number of countries. It should come as no surprise that this calls for the ability to deal with challenges like these. In order to innovate and adapt to the new threat environment, the institutional structure, financial investment, manpower recruited and deployed, and policy framework all need to be prepared.

Support for Hacking/Hackactivists

The tendency of states overtly or covertly supporting cybercriminals in an effort to undermine the interests of rivals or alter the balance of power in their favour is cause for concern. As a direct consequence of this, various countries are currently engaged in ideological conflict. Some countries provide financial support to terrorist organisations, separatist movements, and extreme groups in order to break into the computer networks of their adversaries and undermine their interests. It is critical to buck this trend as soon as possible.

How much Policing?

The majority of the initiatives that we are working on in cyberspace are of a more personal nature. A "Netizen" will consequently have specific expectations regarding their level of privacy. On the other hand, policing is essential because there are dangers originating in the digital sphere. As a result, the question "How much policing?" should be asked far more frequently in cyberspace. It is necessary to strike a careful balance between the requirements of keeping appropriate watch on behaviour online and the requirements of protecting the privacy of internet users. A matter of recent years have passed since the Supreme Court of the United States rendered Section 66 A of the Information Technology Act null and void, finding it to be in violation of virtually every law in existence. According to Sriram (2015), it was referred to as a severe rule that had resulted in the arrest of a large number of people for disseminating items that were regarded as undesirable.

Social Media

The monitoring and management of content on social media platforms presents yet another challenging obstacle. Monitoring what is going on in social media platforms like Facebook and Twitter may be an exceedingly challenging task for law enforcement agencies. There is content that circulates on social media that has the potential to cause severe disruptions to law and order. The events that have taken place in the Kashmir Valley since the death of Burhan Wani have shown how social media can be utilised to inspire anti-national groups to act brutally against law enforcement and the military forces.

Summary and Conclusion

As Petter Gottschalk pointed out in 2010, cyberspace presents a challenging new frontier for the fields of criminology, police science, law enforcement, and policing. Since the 1990s, academics and industry professionals have observed how criminal behaviour has expanded into a whole new field because to the proliferation of the internet. At this rate, both the nature and scope of victimisation are undergoing significant change. Cyber criminology is "the study of causation of crimes that occur in the cyber space and its impact in the physical space" (Gottschalk, 2010), and it was developed in 2007 by Jaishankar. This brand-new field of study focuses on "the study of causation of crimes that occur in the cyber space and its impact in the physical space."

Because of its significance, the legal framework must be updated on a regular basis. Even more important is the National Cyber Security Strategy, which goes beyond the statutory structure that currently exists. It is the mission of this organisation to build a safe and robust cyberspace for Indian citizens, enterprises, and the Indian government. In a nation's cyber security document, a description and expression of the nation's vision, objectives, guiding principles, and strategy for accomplishing its cyber security goals may be found (Rao, 2015).

Other important aspects of effective policing and investigation of cybercrime include the development of Cyber Crime Investigation Modules, the provision of hands-on training in Cyber Crime Investigation and Forensics for cybercrime investigators, the accessibility of necessary equipment through state forensic science laboratories, and the establishment of an adequate physical infrastructure.

In conclusion, it can be stated that cyber policing and cyber crime investigation call for a higher level of professionalism than ever before, as well as the ability to remain stealthy, make use of automated technologies, and understand the complexities of the online world.

References

Brown, C. S. D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*. 9(1), 55-119.

Bryant, R., & Kennedy, I. (2014). Investigating Digital Crime. In: R. Bryant and S. Bryant (Eds.), *Policing Digital Crime* (pp. 123-145). England: Ashgate.

Bryant, R., & Stephens, P. (2014). Policing Digital Crime: The International and Organisational Context. In R. Bryant and S. Bryant (Eds.), *Policing Digital Crime* (pp.111-121). England: Ashgate.

Chang, L.Y.C. (2013). Formal and Informal Modalities for Policing Cybercrime Across the Taiwan Strait. *Policing & Society*, 23(4), 540–555.

Gottschalk, P. (2010). *Policing Cyber Crime*. Retrieved from www.bookboon.com.

Halder, D., & Jaishankar, K. (2016). Policing Initiatives and Limitations. In: J. Navarro, S.Clevenger, and C. D. Marcum (eds.), *The Intersection between Intimate Partner Abuse, Technology, and Cybercrime: Examining the Virtual Enemy* (pp. 167 -186). Durham, North Carolina: Carolina Academic Press.

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Boca Raton: CRC Press.

Kaumudi, V. S. K. (2016). Capacity Building At PS Level In Cyber Crime Investigation Scheme for Implementation at State Headquarters and Police District, Hqrs/ Commissionerates, New Delhi, 8th April.

Mehta, A. (2009). Internal (In) Security in India: Challenges and Responses, *The Indian Police Journal*, Vol. LVI- No. 4, 26-35.

Muthukumaran (2008). Cyber Crime Scenario in India. *Criminal Investigation Department Review*, January, 17-23.

Rao, C. P. S. (2015). Analysis of the National Cyber Security Strategy of UK, USA and India for Identifying the Attributes of a Successful National Cyber Security Strategy, *The Indian Journal of Criminology & Criminalistics*, Vol. XXXIV, 2, 45-56.

Sriram, J. (2015). SC Strikes Down ‘Draconian’ Section 66 A. *The Hindu*. March 24.

Supreme Court Judgment (2006). Prakash Singh and Ors. Vs. Union of India and Ors (22nd September). Retrieved from https://indiankanoon.org/doc/1090328/.

The Information Technology (Amendment) Act, 2008. Retrieved from http://meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf.

The Information Technology Act, 2000. Retrieved from http://lawmin.nic.in/ld/P-ACT/2000/The%20Information%20Technology%20Act,%202000.pdf.

Wall, D.S. (2007/10). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised May 2010), *Police Practice & Research: An International Journal*, 8(2),183 205.

Wall, David S. (2015), The Changing Cyber-threat Landscape and the Challenge of Policing Cybercrimes in the EU. Evidence-Based Policing, 2015 *CEPOL European Police Research & Science Conference*, Lisbon, Portugal, 5th -8th October.

Yar, M. (2005). The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427.