ज्ञान-विज्ञान विमुक्तये

athshala पाठशाला

MHRD Govt. of India

athshala पाठशाला

A Gateway to all Post Graduate Courses

MHRD Govt. of India

An MHRD Project under its National Mission on Education through ICT (NME-ICT)

Subject: CRIMINOLOGY

Production of Courseware

- Content for Post Graduate Courses

Paper : CYBER CRIMINOLOGY & CYBER FORENSICS

Module : Cyber Policing and Cyber Crime Investigation

ज्ञान-विज्ञान विमुक्तये

MODULE 32 : CYBER POLICING AND CYBER CRIME INVESTIGATION

Component - I - Personal Details

Role	Name	Affiliation
Principal Investigator	Prof(Dr) G S Bajpai	Registrar National Law University Delhi
Paper Coordinator	Prof(Dr) K. Jaishankar	Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat
Content Writer/Author(s)	Dr. Akshat Mehta	Associate Professor and Head, Department of Police Administration, Raksha Shakti University, Ahmedabad, Gujarat
Content Reviewer	Prof(Dr) K. Jaishankar	Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat

Component - I (B) Description of Module

	Description of Module
Subject Name	Criminology
Paper Name	**Cyber Criminology and Cyber Forensics**
Module No.	32
Module Name/Title	**Cyber Policing and Cyber Crime Investigation**
Pre-requisites	• Meaning, Nature and Characteristics of Crime • Difference Between Other Crimes and Cyber Crimes • Different Types of Crimes • Information Technology Act • Policing in India • Crime Investigation in India
Objectives	• To understand Cyber Policing and the challenges of doing so. • To comprehend the Cyber Crime Investigation including a theoretically grounded model for it. • To discuss the various issues and challenges in the domain of cyber policing and cyber crime investigation.
Keywords	Information Technology Act, Cyber Policing, Policing in India, Cyber Crime Investigation in India.

Table of Contents

Learning Outcomes

After the completion of this module, you will be able to:

1. To understand Cyber Policing and the challenges of doing so.
2. To comprehend the Cyber Crime Investigation including a theoretically grounded model for it.
3. To discuss the various issues and challenges in the domain of cyber policing and cyber crime investigation.

Cyber Policing and Cyber Crime Investigation

1. Introduction

The interpretation of the term 'space' vis-à-vis crime has undergone transformation with the advent of cyber crime. We are no more restricting ourselves to the geographical comprehension of the crimes as well as criminals. A criminal in the cyber space is not confined to a geographical/physical jurisdiction, as was the case with many of the conventional crimes.

The developments in the world of Information and Communication Technology (ICT) have paid dividends to the humanity in various ways. Yet at the same time, it has thrown before us huge challenges and present opportunities for crime using new and highly sophisticated technology tools (Muthukumaran, 2008). The same ICT tools are being used by the deviants to harass, threaten, dupe, damage the reputation, extort, indulge in illicit trade, recruit terrorists, and carry out security breaches and acts of terror, etc. This has resulted in society looking at 'Cyber Crime' as a significant challenge and dire need for governments to act speedily and strongly. The governments have responded by formulating laws and establishing institutional mechanism for addressing the challenges of cyber world. However, considering that the cyber world is a dynamic world, much more needs to be done for cyber policing and cyber crime investigation. In this module, issues of cyber policing and cyber crime investigation will be discussed.

2. Cyber Policing

The cyber world has brought a new paradigmatic shift in terms of connectivity, ease of providing services and speed in transactions. Yet at the same time there are growing threats and vulnerabilities. These have posed challenges for the law enforcement machinery like never before. This scenario raises questions relating to preparedness of Police to address these challenges, the quickness of policy makers to adapt/amend the framework as per the needs of the time and the ability of different governments and institutions to cooperate and coordinate with one another.

The legislative framework in the form of Information Technology Act through its various sections has laid down the broad contours for cyber policing in India. Section 69 of the Information Technology Act empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down there. This

power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence [The Information Technology (Amendment) Act, 2008].

In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so. These include (i) providing access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or (ii) intercepting or monitoring or decrypting the information, as the case may be; or (iii) providing information stored in computer resource.

The failure to extend the above-mentioned facilities and technical assistance has been made punishable with an imprisonment for a term which may extend to seven years and shall also be liable to fine [The Information Technology (Amendment) Act, 2008] Section 69A inserted in the Information Technology Act, 2008 vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above.

Section 69B discusses the power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource [The Information Technology (Amendment) Act, 2008]. As far as the question of cooperation between different institutions and governments is concerned, the issue of cyber crime takes us to the domain of not only intra-state or inter-state but inter-national levels as well.

Benyon et al. has mentioned international cooperation between law enforcement agencies engaged in countering or investigating digital crime at three levels i.e., *macro, meso or micro*. At the macro level, cooperation is typically between governments and international organisations, including through the agencies of Europol and Interpol. At the meso level, the cooperation is likely to be between police forces or law enforcement agencies located in

different nation states, for example between the PcEU in the UK and the FBI in the US. At the micro level the cooperation will often be informal and take the form of contact between individual investigators (Bryant & Stephens, 2014).

At the international level, there has been a convention also called the Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, which is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. The Convention entered into force on 1 July 2004. The Convention is yet to get approval from international community in the sense that India too has declined to adopt it as it was not involved in its drafting and some countries on the ground that it may violate their sovereignty (Wikipedia, n.d.)

The conventional thinking is that policing the cyber world is the task of public police and it is essentially a government function. However, scholars have mentioned that monitoring of cyber world can be undertaken by not just the state funded policing or public policing, but by corporate policing and non-governmental policing as well (Halder & Jaishankar, 2016). The success of cyber policing would depend upon building the synergies between public policing, corporate policing and non-governmental policing.

Policing the cyber space is becoming highly impossible due to ease of 'offender mobility' (Yar, 2005). Also in spite of the cyber crime conventions, enmity or hostile relationship between two countries may make policing cross jurisdictional cyber crimes almost impossible (Chang, 2013). The cross jurisdictional presence of the perpetrator, especially if the perpetrator is anonymous makes it all the more difficult for cyber policing.

3. Cyber Crime Investigation

Ó Ciardhuáin has argued that 'a good model of cybercrime investigations is important, because it provides an abstract reference framework, independent of any particular technology or organisational environment, for the discussion of techniques and technology for supporting the work of investigators' (Bryant & Kennedy, 2014).

One of the most theoretically-grounded models was proposed by Ó Ciardhuáin in 2004. There are 13 activities in his *'Extended Model of Cybercrime Investigations',* which are summarised below:

(i) Awareness - Recognition that an investigation is needed

(ii) Authorisation - For example, through the issuing of a warrant

(iii) Planning - Using information collected by the investigator

(iv) Notification - Informing the subject and other interested parties that an investigation is taking place

(v) Search for and identify evidence - For example locating the PC used by a suspect

(vi) Collection of evidence - Potential evidence is taken possession of

(vii) Transport of evidence - Transported to an appropriate location

(viii) Storage of evidence - Storage methods should reduce the risk of cross contamination

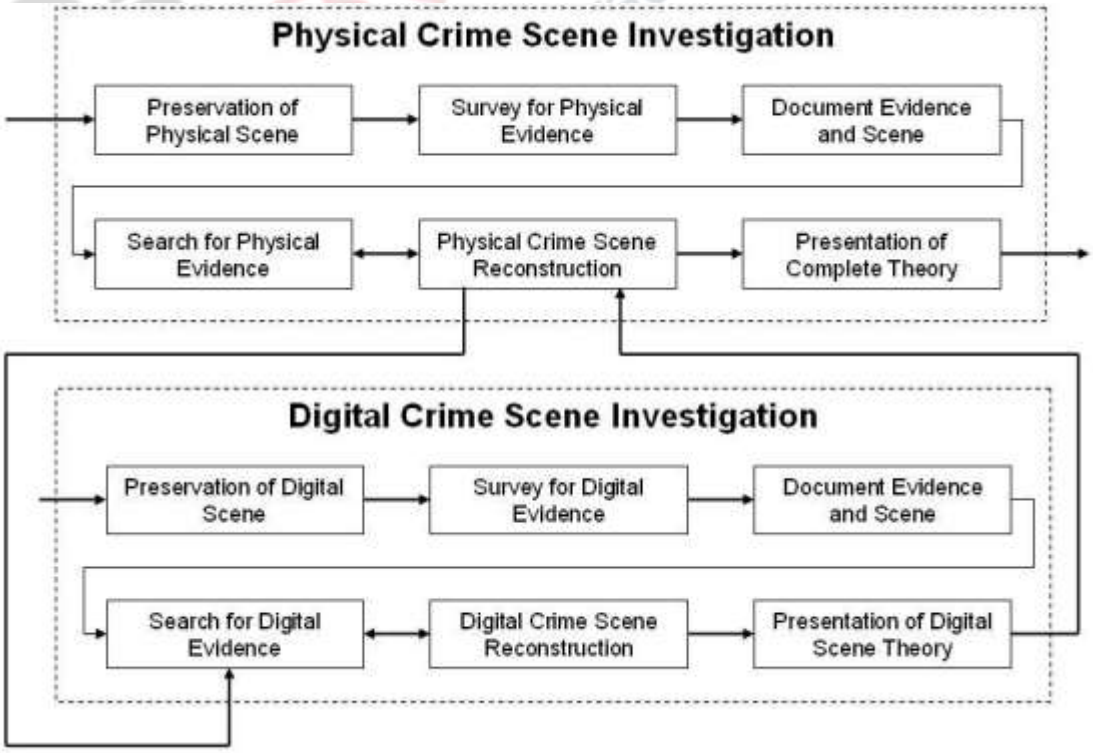
(ix) Examination of evidence - The use of specialist techniques e.g. recovery of deleted data

(x) Hypothesis - A tested formulation of what may of occurred

(xi) Presentation of hypothesis - For example to a jury

(xii) Proof/defence of hypothesis - Contrary hypotheses will also be considered

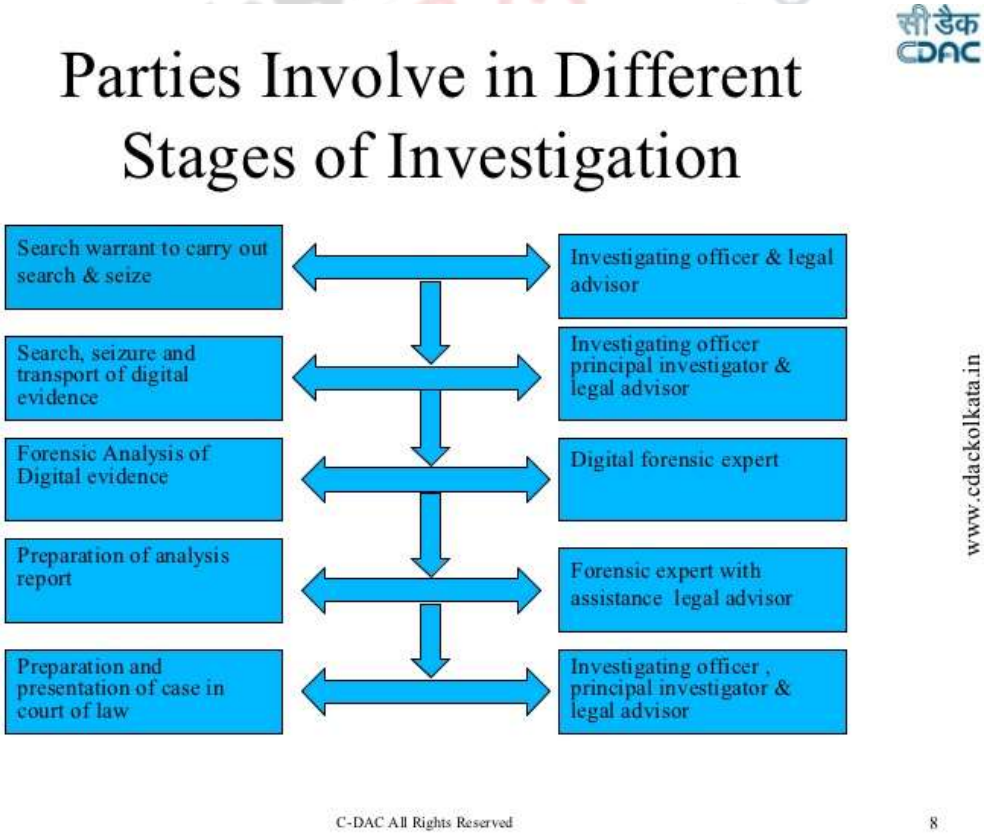
(xiii) Dissemination of information - The information may influence investigations in the future (Bryant & Kennedy, 2014).



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

The process of cyber crime investigation in India is vital to our understanding of this module. The power to investigate cyber offences has been mentioned in Section 78, which says that 'notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act'. Further, Section 80 provides for the power of police officer and other officers to enter, search, etc. It says that notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act [The Information Technology (Amendment) Act, 2008].

Further sub-section (2) says where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station (IT Act amended, 2008).



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

4. Discussion

As mentioned earlier, the domain of cyber policing and cyber crime investigation operates in a dynamic environment and there are several issues and challenges to be addressed. These have been discussed as under:

4.1. Legal Framework

The first and foremost issue in cyber policing and cyber crime investigation is that of the legal framework under which it operates. In the Indian context, prior to the enactment of Information Technology (IT) Act, 2000, the cyber world was unregulated and there was confusion amongst the law enforcement authorities regarding action to be taken on criminal acts committed in cyber space. It was only with the legislative action resulting in IT Act, 2000 coming into being that cyber crime was defined and cyber policing and investigation became reality. Further, owing to its dynamic character, a need was felt to amend certain provisions of the Act, which was undertaken in the year 2008. In this Act additional cyber crimes like child pornography and cyber terrorism were included and an Inspector was authorized to investigate cyber offences as against the Deputy Superintendent of Police authorized in the earlier legislation. Thus, there are several questions which are sought to be addressed by the legal framework, like - Which act in cyber space would be called a Cyber Crime?; How will that Cyber Crime be investigated?; What would be the penalty for committing such Cyber Crime?; and What would be called 'evidence' in Cyber Space?, etc.

4. 2. Nature of Cyber Policing

Flowing from the typology given by Halder and Jaishankar (2016), a question which comes to the mind is that what is the nature of Cyber Policing? Should Public Policing alone tackle the menace of cyber crime or is it in a position to manage it alone. Or should Private/Corporate or NGOs be roped in for effective results? Certainly the synergy between the three is likely to present solutions to address the challenges. The changing 'cyber-threat landscape' in the words of David Wall and how it impacts the policing also needs to be kept in mind (Wall, 2007, 2010 and 2015). This all clearly points towards broadening the breadth and scope of cyber policing and involvement of multiple stakeholders.

4.3. Cyber Crime Investigation

The power to investigate cyber offences has been mentioned in Section 78 of the IT Act, and Section 80 provides for the power of police officer and other officers to enter, search, etc. With escalations in reports of serious cyber crime, one would expect to see a

corresponding increase in conviction rates. However, this has not been the case with many investigations and prosecutions failing to get off the ground. The chief causes of this outcome may be attributed to trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime (Brown, 2015).

Most of the states are performing cyber crime investigation with one or very few dedicated cyber crime police stations which may not be able to cope with the phenomenal increase in the offences in the cyber world. Victims are also facing the problems of reaching out to designated police stations for filing their 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.

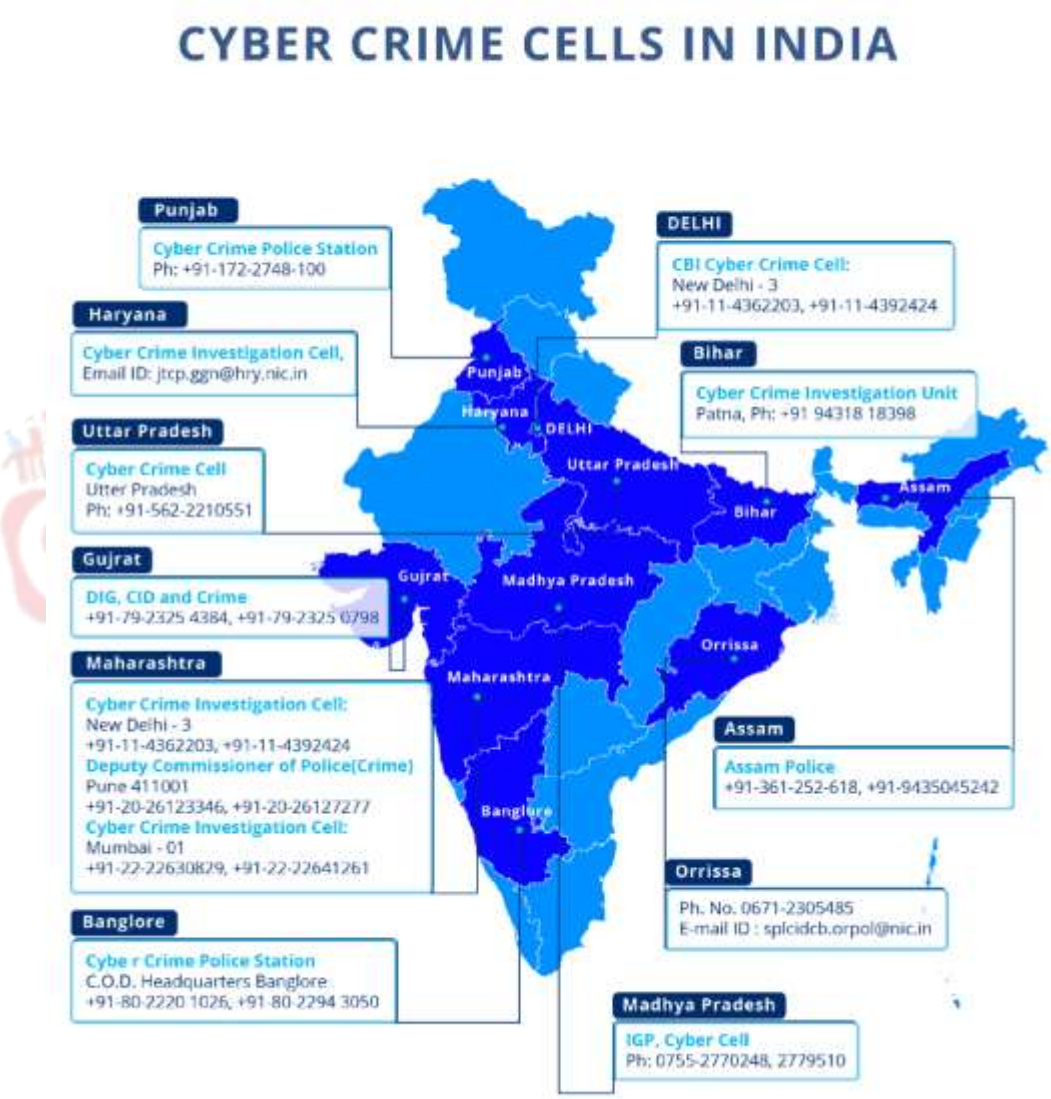
4.5. Coordination between Countries/ International Protocol – Criminal Investigation

The cyber space is altogether different space from the physical space and so are the characteristics of people travelling in it (Jaishankar, 2008). The shedding of inhibitions, blanket of anonymity and geographic insulation offered by cyber space has meant that crime and criminals are to be re-interpreted. The criminals in the cyber world and the victims in the cyber world may not be in the same physical space. Rather, there is a possibility that they are poles apart. In this scenario, the investigation process has to deal with not only the laws of the states, one nation, but across the countries as well in some cases. This requires greater amount of understanding, coordination and cooperation between the legal functionaries of different states and nations.

4.6. Capability of Law Enforcement Machinery

In the field of cyber policing and cyber crime investigation, a fundamental question is related to that of the capability of the machinery. The skill set of the people who are deployed in the cyber crime investigation cells/units is an important determinant for the effectiveness of the machinery. The general recruitment standards set for Police in the country are not going to help the matters. Indian Police Organizations require hiring and tapping the best talents in the field of cyber technology to counter the threats emerging from creative yet deviant minds.

The author in one of his previous works has mentioned that Cyber Crime poses new challenges as the agencies to investigate such crimes lack the skills to do their job and poor policeman does not know what to do (Mehta, 2009). Financial swindling and bungling also requires change in the traditional methods of investigation. Counterfeit currency has also emerged as potent threat to India's internal security. Destabilization of Indian Economy at a crucial period of its growth would be the last thing we should expect, and that is precisely what the forces inimical to India's emergence have been trying (Mehta, 2009).



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

4.7. Manpower/Personnel

The setting up of institutional framework and sanctioning adequate manpower to these institutions is also a basic requirement. The Units and Cells needs to be equipped with adequate and specialized manpower. In short, the global nature of computer crime and the digital environment, which has eclipsed the ability of any one department, state, or nation to individually manage this new paradigm change in crime, now requires more skilled and educated personnel. The provision of these new skilled and educated employees, not only for our forensic computer investigation units but also for a range of sub-disciplines within the emerging body of knowledge — sometimes referred to as computer forensics, information assurance, computer security, and software security — will have to come from our nation's universities (Johnson, 2005).

For activities such as online information gathering, Network Forensics, Mobile tracking, Email tracking, Social media analysis and link analysis, regular police officers do not possess the required expertise. Hence outsourced specialists with the latest technology know-how are handy for complex investigation. The cyber staff needs to be trained in Forensic Analysis Certificate Course, Networks Security Certificate Course, Network Tracking Certificate Course, Call Tracking Training and Onsite Analysis Training, etc.

4.8. S.C. Judgment of 2006 & Model Police Act

The Supreme Court Judgment in the Prakash Singh and Ors. Vs. Union of India and Ors. dated 22nd September 2006 contained a directive, which read: "The investigating police shall be separated from the law and order police to ensure speedier investigation, better expertise and improved rapport with the people. It must, however, be ensured that there is full coordination between the two wings". The Model Police Act 2006 too has emphasized upon the same. Several of the state legislatures have also incorporated these provisions in letter. The implicit point out here is that specialized skills need to be imparted to the personnel and in today's crime scenario, cyber crime policing and investigation is not an ordinary task. The manpower needs to be exclusively recruited and trained for this task and allowed to build upon their skills on a long term basis.

4.9. Evolving Crimes

The cyber crime field has been evolving with time and bringing in more complexity. It has brought before us the challenges in the form of viruses, worms, phishing, hacking, malware, botnets, ransomware to name a few. The recent ransomware attack 'WannaCry' affecting several countries is a proof of this evolution. Clearly, it requires capabilities of

addressing these challenges. The policy framework, the institutional set up, the finances put in and manpower recruited and deployed all need to be ready to innovate and adapt to the changed threat landscape.

4.10. Support by Countries for Hacking/Hacktivists

A dangerous trend being observed is the overt or covert backing of cyber criminals by countries to damage the interests of rivals or tilt the balance of power in their favour. This has resulted in ideological battles being played between countries. Terrorists, separatists, extremists are being supported by some countries to hack the networks of opponents and damage their interests. This trend needs to be broken immediately.

4.11. How much Policing?

Several of the works which we undertake in Cyber Space are personal in nature. Hence, a 'Netizen' expects a certain amount of privacy. Yet at the same time owing to threats emanating from the cyber world, policing is also required. So, the question of 'how much policing?' should be there in the cyber space is all the more relevant. A fine balance needs to be maintained between protecting the privacy of cyber users and need for keeping adequate vigil on the activities in the cyber world. Only a couple of years back Supreme Court had struck down Section 66 A of the Information Technology Act by calling it as unconstitutional in its entirety. It was termed as draconian provision that had led to the arrests of so many people for posting contents deemed to be objectionable (Sriram, 2015).

4.12. Social Media

The policing and investigation of content on social media is another huge challenge. The law enforcement machinery is facing a huge challenge in keeping a tab over the developments on the social media. Some of the information on social media has the potential to cause huge law and order disturbances. Events in Kashmir Valley in the aftermath of the death of Burhan Wani has shown the possibility of misuse of social media for mobilizing the anti-national elements in being aggressive against Police and Armed Forces.

Source: http://media2.intoday.in/btmt/images/stories//Newstaffpics/mos1_122616124419.jpg

Summary and Conclusion

Petter Gottschalk (2010) has rightly pointed out that cyberspace presents a challenging new frontier for criminology, police science, law enforcement and policing. Since the 1990s, academics and practitioners have observed how cyberspace has emerged as a new field of criminal activity. This pace is changing the nature and scope of offending and victimization. A new discipline called Cyber Criminology (by Jaishankar in 2007) has

emerged, wherein 'the study of causation of crimes is undertaken that occur in the cyber space and its impact in the physical space' (Gottschalk, 2010).

The legislative framework is important and needs to be amended from time to time. Beyond legislative framework, even the National Cyber Security Strategy is important. In India it aims to build secure and resilient cyberspace for citizens, businesses and government. A cyber security document of a country outlines and articulates the vision, objectives, guiding principles and approach to meet cyber security goals (Rao, 2015).

The development of Cyber Crime Investigation Modules, hands on training to cyber crime investigators on Cyber Crime Investigation and Forensics, availability of necessary equipment with the State Forensic Science Laboratories and infrastructure are other important determinants in effective cyber crime policing and investigation.

In the end, it could be said that today, Cyber Policing and Cyber Crime Investigation require more professionalism, more stealth, more usage of automated technology and ability to understand the complexity of the cyber world, like never before.

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.