Cyber Crime and the Police: Insinuations to the Police Commissionerate of Bhubaneswar and Cuttack

Dr. Arpita Mitra

Information and Communication Technologies (ICTs) are progressively being adopted in Police work with the aim of nurturing greater accountability and a contrivance to check cyber crime. The knowhow about cybercrime is also inadequate among a significant section of the officers. The training programmes on cyber crime and its detection is only made available to a selected few, while the rest remain in darkness. As the number of victims of cybercrimes is increasing day by day, the policemen (even at the root level) must be aware and conscious of the nuances of cybercrime so that they can capably guide the people and counter the menace. In this regard the present paper seeks to address the predicament of cyber crime and provide suggestions to the Police Commissionerate of Bhubaneswar and Cuttack to check the peril.

Keywords: ICTs, cybercrime, information society, ecrimes.

Introduction

Today's Police is expected to provide multi-dimensional service to the people in a proactive way. This entails that they are to be equipped in the best possible way to establish them as a people friendly police force. To provide the best of services it has been found that the police force has failed to come out of its cocoon and most of the officers remain unpragmatic and uneasy towards the recent developments. ICTs are providing multifaceted array of tasks not only to the masses but also to the police. In addition to this, the abuses of ICTs have also challenged the police to a newer form of crime – cyber crime. The paper is an attempt to delve into the infrastructure and technical skills that the Police of Bhubaneswar and Cuttack should offer to the people to combat cyber crime.

Information and Communication Technologies, Cyber Crime and the Police

In recent decades, countries like the United States, Japan and most European nations have become information societies, where information workers are more numerous than such occupational categories as farmers, industrial workers and service hands. Information workers are those individuals whose main job responsibilities are to gather process or to distribute information or to produce information technologies like telecommunication equipments that are used by other information workers. India has more information workers than Japan, and about the same number as United States. These millions of information workers are mostly urban and educated, living a lifestyle similar to information workers in Silicon Valley, Tokyo or London (Singhal and Rogers 2001:17). New communication technologies such as satellites, cable television, wireless telephony, the internet and computers are bringing about noticeable changes in the Indian society. Information and Communication Technologies (ICTs) include hardware equipment, organizational structures and social values by which individuals collect, process and exchange information. (ibid: 30). Information Technologies can be used to plan, coordinate, and execute operations. Using the Internet for communication can increase speed of mobilization and allow more dialogue between members, which enhances the organizations flexibility since tactics can be adjusted more frequently. Individuals with a common agenda and goals can form subgroups, meet at a target location, conduct terrorist operations, and then readily terminate their relationships and redisperse (Zanini & Edwards 2001:36).

On the one hand, the introduction of ICTs has generally facilitated services in public administration, urban and rural administration, and urban and rural development transport sectors and has benefited the quality of life for citizens especially in medicine and health, education, environment, and agriculture (Rao 1998:171-215). As the population of this virtual community expands there is a considerable rise in the incidents of cybercrime and abuses of computer technology (Marstrand 1984: 9-12; Moore 1995:1-9). To quote Castells: "Crime is as old as humankind. But global crime, the networking of powerful criminal organizations, and their associates, in shared activities throughout the planet, is a new phenomena that profoundly affects international and national economies, politics, security and ultimately societies at large" (Castells 1999:166).

The wildfire spread of cybernetics, in the form of satellites, videocassettes, narrow casting, niche identification, cluster targeting, extra intelligent networks, simulation have become the facets of this civilization. Along with its overwhelming advantages it has entailed a major area of challenge for the law enforcement agencies in the 21st century- cyber crime variously known as computer crimes, ecrimes etc. "Cyber crimes-harmful acts committed from against a computer network – differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require less resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it and they are often not clearly illegal" (Grabosky, 1998).

Classification of cyber crimes

Cyber crimes can be of the following nine types: (a) Theft of telecommunications services, (b) Communications in furtherance of criminal conspiracies, (c) Telecommunications piracy, (d) Dissemination of offensive materials, (e) Electronic money laundering and tax evasion, (f) Electronic vandalism, terrorism and extortion, (g) Sales and investment fraud, (h) Illegal interception of telecommunications and (i) Electronic funds transfer fraud (See http://www.crime.hku.hk/cybercrime.htm visited on 12.8.2012). Furthermore, they can also be classified as the following:

(1) **Denial of service attacks:** It is an attack on a web server with false requests for pages. The server spends so much time trying to process these requests that it cannot respond to legitimate requests and may crash.

(2) Viruses, worms, trojans and other forms of malicious code: Malicious code is a general term for programs that, when executed, would cause undesirable results on a system; Computer viruses are computer programs that can replicate themselves and harm the computer systems on a network without the knowledge of the system users. Viruses spread to other computers through network file system, through the network, Internet or by the means of removable devices like USB drives and CDs. Computer viruses are after all, forms of malicious codes written with an aim to harm a computer system and destroy information. Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

(3) **Unauthorised Entry** : The activity of breaking into a computer system to gain an unauthorized access is known as hacking. The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

(4) **Information Tampering:** Intruding into and damaging information stored in different storage devices of the computer.

(5) **Cyber stalking**: The use of communication technology, mainly the Internet, to torture other individuals is known as cyberstalking. False accusations, transmission of threats and damage to data and equipment fall under the class of cyberstalking activities. Cyberstalkers often target the users by means of chat rooms, online forums and social networking websites to gather user information and harass the users on the basis of the information gathered. Obscene emails, abusive phone calls and other such serious effects of cyberstalking have made it a type of computer crime.

(6) **Spamming** : Sending unsolicited bulk email.

(7) **Mouse-trapping** : Clicking the browser's back button with the mouse does not lead out of the unwanted site but only to the viewing of further unwanted pages eg. pornography. To escape the user may need to close the browser or even restart the operating system.

(8**) Phreaking** : Breaking into the telephone network illegally to tap phone lines;

(9) **Computer Damage**: Injuring the hardware of the computer.

(10) **Phishing**: The act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

(11) **Identity Theft:** This is one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity. It is the act of pretending to be someone else by using someone else's identity as one's own. Financial identity theft involves the use of a false identity to obtain goods and services and a commercial identity theft is the using of someone else's business name or credit card details for commercial purposes. Identity cloning is the use of another user's information to pose as a false user. Illegal migration, terrorism and blackmail are often made possible by means of identity theft.(See B.Etter,"Critical Issues in High-Tech Crime", available at http://www.acpr.gov.au/pdf/Presentations/apmedec02.pdf visited on 14.4.2010 and http://www.buzzle.com/articles/types-of-computer-crimes.html visited on 13.8.2012.)

Cyber Crime and Law Enforcement

The development of new technology invites the establishment of new institutions to supervise policing, and value driven design may enable new legal procedures that are better equipped to hold policing accountable. The new policing aims to prevent and pre-empt crime rather than to prosecute it. By predicting when, how, and by whom a crime will be committed, it aims to enable efficient intervention. Law enforcement has recognized in virtual space a toolkit of restraints on criminal behavior. These restraints include law, technological features, network typology, and the social construction of particular uses of computers. Again, the line between private and public law enforcement is blurring as private parties monitor the public flow of information and secure essential information junctions. The third parties including conduits, service providers, information gatekeepers, traffic routers, tool suppliers, and payment systems play on the digital crime scene and heavily regulate them (Kozlovski 2007: 108-114).

Today in its brawl against cyber crime the law enforcement agencies face a number of challenges: First, procedural resistance hinder law enforcements's ability to find and indict criminals operating online. Second, laws defining computer offences and the legal apparatus needed to probe criminals using the internet, cannot match up with the fast scientific and societal developments. Finally, there is a dearth of well trained, well equipped investigators and prosecutors to detect high tech crime. To counteract these emergent cyber threats, the role of the police in India should be redefined and the force should be professionalized to perform its tasks in cyber space through various organizational and structural changes in order to re-institutionalise the existing occupational culture, which is the main impediment of the force in combating cybercrimes (Thomas 2002:999). However the police alone cannot maintain their domain or jurisdiction over cyberspace nor can they fully exercise cybercrime patrolling. The success of fighting cybercrimes depends on the support that it gets from the legal systems and the cooperation of community and the users of new technologies in cyberspace.

Some Insinuations to the Police Commissionerate of Bhubaneswar and Cuttack

1. A Cyber Crime Cell/Police Station should be developed to handle cases dealing with computer offences.
2. A Cyber Forensic Laboratory with all updated technologies should be endorsed to detect computer crimes.
3. A team of specially trained officers expert in detecting cybercrimes should be reared in the model of 'Cybercops' of Andhra Pradesh Police. A special group of officers must be skilled in collection, storage, and, retrieval of digital evidence. Laboratory and skill development to maintain digital evidence is a need of the time.
4. The Police Commissionerate should take initiatives to have information about the recent new police technologies that are being used by police in Bangalore, Mumbai, Delhi, Chennai and Kolkata with special emphasis to cyber crimes. They should also take note of police organizations in developed countries. This will help them to keep pace with new challenges of policing and establish itself as a high tech police force.
5. The local police stations (20 police districts each for Bhubaneswar and Cuttack) should keep a vigil on the cyber cafes of their respective localities. It should be ensured that

no one will be allowed to use the cyber café without valid proof of identity. The time limit for surfing in the cyber cafes should also be restricted. Recently the State Government of Odisha has made cyber café registration mandatory. The order ensures that apart from asking for valid identity proof, the cyber cafes will maintain a record of the visitors and also prohibit surfing of websites containing pornography, obscenity, terrorism and other objectionable materials.(*'Cyber café Registration Mandatory'*, The Sunday Express, 19th August, 2012, p.4)

6. The website of the Police Commissionerate of Bhubaneswar and Cuttack should provide information to the city dwellers about the precautionary measures that should be taken to check cyber crimes. Awareness among the public about rising e crimes should be made by the city police through the website, advertisements and sensitization programmes in educational institutions.

7. The Contact Number of police personnel dealing in Cyber Crime should also be mentioned in the official website.

8. The new generation policemen should be trained in the application of ICTs in police work to help them to carry forward the legacy of the police organization successfully. Policemen who are new entrants must be imparted training in ICTs at the inception of training programme to enable them to understand its importance in police work. In addition to this will reduce the inhibitions in using computerized technologies. They will also be sensitized about the abuses of computer technologies.

9. All complaints of cyber crimes should be given importance. Special directions should be given to local police stations so that they can properly guide the people if they come with complaints of cyber crimes.

10. The Crime Statistics of the cities of Bhubaneswar and Cuttack does not show any data on cyber offences. This should be included as a separate category in the list and should not be merged with other traditional forms of crime. (See http://bhubaneswarcuttackpolice.gov.in/crimestatistics.php visited on 5.8.2012.)

11. Awareness programmes should be carried out to sensitize police officers about the Information Technology Act, 2000/2008.

12. Since the number of educational institutions is increasing in Bhubaneswar and Cuttack with a regular flow of students from all over India, the Police Commissionerate should be extra vigilant and sensible towards the youth. Since the offenders and victims of cyber crime are mostly the young generation the police should take a constructive and reformatory approach while dealing with them.

13. Sensitization programmes on cyber crimes should be organized by the Police Commissionerate in educational institutions to spread awareness about computer abuse among students. Students should also be updated about the provisions of the Information Technology Act, 2000/ 2008.

14. Community Policing Programmes should also be initiated to check cyber offences. The people's participation can be of great help in combating cyber crime.

15. The Police Commissionerate needs to provide access to technologies especially wireless handsets, computers, internet, and mobile telephones to all ranks of policemen to make them adept in handling ICTs.

Conclusion

The Police Commissionerate of Bhubaneswar and Cuttack has to match steps with other capital cities like Hyderabad, Bangalore, Mumbai, Delhi and Kolkata in so far as protection against cyber crime is concerned. The police of the twin cities has to initiate noteworthy measures to combat computer crimes. The abuses of ICTs is on the rise and with so many educational and industrial developments going on, it is the need of the hour to develop a more proactive safety measure to check the peril. Since the victims as well as the offenders of cyber crime are mainly the younger generation it is important that they should be adequately sensitised about the legal directions against cyber crime. With the recent regulations on cyber cafes the police officer not below the rank of an inspector has to be assigned the responsibility to check or inspect cyber cafes and computer resource or network established at any time to comply with the Technology (Guidelines for Cyber Cafes) Rules, 2011 as issued by the Ministry of Information Technology. In this regard the Police Commissionerate can play a notable role. More so, the police officers including those working at the grass root especially in the local police stations if adequately informed can be active in combating cybercrime. The insinuations to the Police Commissionerate have come with the hope that if implemented can make the police of the twin cities more high tech and agile in combating cyber crime.

References

Castells, M. 1999. 'The Information Age: Economy, Society and Culture'; *The Information Age*, Vol.III; Blackwell; Oxford

Grabosky, P.N. 1998. 'Crime and Technology in The Global Village', Paper presented at the conference: Internet Crime held in Melbourne, 16-18February1998, by the Australian Institute of Criminology.

Kozlovski, N. 2007. 'Designing Accountable Online Policing in Balkin J.M., E. Katz E. & S.Wagman. et al. *Cybercrime: Digital Cops in a Networked Environment*. New York:New York University Press; 107-134.

Marstrand, P. 1984. *New Technology and the Future of Work and Skills*. New York:Pinter.

Moore, R.H. 1995. 'Technology and Private Security, What does the Future Hold?' *Journal of Security Administration* 18(12);1-9.

Rao, P.B. 1998. *Information Network and Resource Sharing*.New Delhi:Reliance

Singhal, A. & Rogers,E.M. 2001. *India's Communication Revolution: From bullock Carts to Cyber Marts*. New Delhi: Sage Publications.

Thomas, K.V. 2002. 'Cyber Crime and Policing' in Alexander P.J. (ed). *Policing India in the New Millennium*.New Delhi:Allied; 989-1000.

Zanini, M. & J.A. Edwards. 2001. 'The Networking of Terror in the Information Age', in Arquilla J. & D. Ronfeldt. etd. *Networks and Netwars: The Future of Terror, Crime and Militancy*.Santa Monica, CA:RAND.

'Cyber café Registration Mandatory', *The Sunday Express*, 19th August, 2012; p.4.

Websites:

Etter,B."Critical Issues in High-Tech Crime", available at http://www.acpr.gov.au/pdf/Presentations/apmedec02.pdf visited on 14 April, 2010.

http://bhubaneswarcuttackpolice.gov.in/crimestatistics.php visited on 5.8.12.

http://www.crime.hku.hk/cybercrime.htm visited on 12.8.2012.

http://www.buzzle.com/articles/types-of-computer-crimes.html visited on 13.8.2012.

Dr. Arpita Mitra, Assistant Professor, School of Law, KIIT University, Bhubaneswar, Odisha-751024, Email - arpitaamitra@gmail.com.