# Need for an Overhaul in Investigation and Prosecution of Cyber Crimes in India

Barun Kumar Sahu[1]


## ABSTRACT

*ICT is used not only by ordinary people, but also by criminals and terrorists to commit crimes. Under NeGP, we have not given due emphasis on computer forensics, and on investigation and prosecution in cyber crimes. However, a situation has come when we can no longer ignore it. Computer forensic laboratories must be strengthened with adequate skilled manpower, latest equipments and software. There is a crying need of training the public prosecutors to be able to present electronic evidences with ease. Without this foundation, e-commerce, e-governance and IT sector in the country will face a serious stumbling block.*


***Keywords*:** Computer forensics, criminal justice system, cyber crime, forensic laboratory, National e-Governance Plan

## 1. Computer Forensics and E-governance

Recent years have witnessed exponential growth in the popularity of computers, smartphones, PDAs, electronic devices, communication equipments and the Internet. Information and communication technology (ICT) tools are now cheap, and affordable even to the ordinary people. Devices as diverse as refrigerators and door-locks are now getting connected to the network, and computer devices are ubiquitous. However, ICT is being used not only by ordinary people in managing the complexities of the modern life, but is also being used by hardened criminals and terrorists to commit crimes. Committing crime has now become a lot easier. ICT is being used not only to conduct lawful businesses, but also to indulge in illegal and criminal activities, and even in terrorist activities. In the cyberspace, often there is a thin dividing line between ingenious creativity and heinous crime. Perhaps because of apparent anonymity in the Internet, people commit things in the cyberspace that they would avoid in the real world. Amongst the cyber crimes registered with the police in India, most are on forgery, fraud, criminal breach of trust, obscenity, hacking, tempering with systems, breach of confidentiality, intellectual property rights, piracy, spreading hatred, identity theft, wardriving etc.

National e-Governance Plan (NeGP) is the overall framework for e-governance initiatives in India. While NeGP does lay emphasis on computerization of various sectors in governance through Mission Mode Projects (MMPs), there is lack of emphasis on computer forensics, and adjudication in torts and civil disputes over electronic records. As various MMPs and other e-governance initiatives mature, the need for looking into disputes over and use of electronic evidences will come to the fore. This will be for both civil

[1] D-II/16, Shahjahan Road, New Delhi 110003, India (E-mail : barun_sahu@yahoo.com, Telephone: +91-11-23387313)

and criminal cases. Criminal justice system is the most important sovereign function of the government, and the government can ill afford to ignore it. The Mission Mode Projects on e-Police and e-Court has a missing link in the form of computer forensics. For healthy development of the IT sector and the IT industry, it is essential that there is proper policing of the cyberspace, and the police have adequate capability to handle electronic evidences in both cyber crimes and traditional crimes. Of course, unnecessary restrictions should not be imposed on the use of ICT tools by the people, and the people should not be inconvenienced in the name of security.

## 2. Cyber Crime

In cyber crime, ICT devices are either the target or the means of the crime, or are incidental to it. Most cyber crimes are not new crimes *per se*. Often the only difference is that the evidences are in electronic form or that the tools used to commit the crimes are ICT tools. Indeed most of the crimes committed today involve some amount of evidence in the electronic form such as phone calls, messages, emails, electronic files etc. Most cyber crime cases are booked in India under the provisions of the Indian Penal Code (IPC) and laws on economic offenses, and only very few under the Information Technology Act 2000. However, the Information Technology Act 2000 has enabling provisions for admissibility of electronic evidences in the courts of law.

Unlike traditional crime, cyber crime is not restricted by geographical boundaries. Indeed, often cyber criminals operate from other countries, as in the case of the infamous "Nigerian scam." In view of use of cyberspace by terrorists and international criminals, cyber crime also has implications on the national defense. Information warfare is now a recognized national threat. Indeed, "IT disaster" is among is the newest additions to the man-made disasters. This brings out the need of strong international cooperation on real-time basis to tackle cyber crimes. Also the legal system must recognize the computer forensic examinations done by foreign countries.

Many companies do not report to authorities about attacks on their networks out of fear of adverse publicity and losing the confidence of the clients. Companies also fear that authorities may seize their servers, and that the servers will remain with government functionaries for long time, which will cause them serious financial loss. However, such sweeping of the problem under the carpet will only make the criminals more and more emboldened.

## 3. Computer Forensics

The increasing use of ICT by the criminals, insurgents and terrorists has necessitated a re-look at the criminal justice system to tackle the impact of the new technology on the society and the crime patterns. Many evidences against even ordinary crimes are in electronic form, and this has led to the development of the new discipline of computer forensics, also called digital forensics or cyber forensics. Computer forensics involves examination of computer devices, networks, routers, volatile memories, digital cards, telephone call details, geographic information etc for the purpose of collecting evidence against crime or civil breach, and adducing the same before the courts of law. Examination of both live data (such as Internet Messaging taking place, or volatile memory in RAM) and recorded data (such as files in hard disk) are done. Some of the utilities of computer forensics are speaker identification (to identify the speaker in wiretapping etc), video authentication (to ascertain morphing etc), e-mail tracing, search of deleted files in laptops etc, cracking of passwords, steganography (to ascertain hidden messages) etc. Nowadays, the servers have memories running into terabytes; and, imaging of the entire memory of the server may not always be practicable. The log files of the servers and routers are very much required in the computer forensic examination. Indeed, digital forensic examinations depend very much on the cooperation of the server and network administrators, who may be located in the same country or in different countries.

Computer forensics is a very new field. Unlike traditional crime investigation, there is not yet exhaustive manual or standard operating procedure (SOP) available to the investigators. Search and seizure procedures of electronic devices and evidences require skills and capabilities different from the normal crimes. Unless the electronic evidences are collected and preserved properly, there may be damage to or unintentional tempering with the evidence. Improper or unauthorized surveillance may invite action against the cyber crime investigators themselves. Since ICT is an involving and rapidly changing field, many of the tools used by the investigators are not even authenticated. That is, in preliminary examinations, cyber crime investigators sometimes also use tools whose authenticity cannot be established a formal judicial process.

Indeed, most cyber criminals are highly educated, very professional and IT-savvy, perhaps more IT-savvy than the police personnel are. They use several anti-forensic tools and methods to evade detection in computer forensic analysis. Many software use very strong encryptions and locks, and are difficult to crack. The criminals take refuge behind such securities. Government of India has not yet officially allowed the BlackBerry service in India because of security concerns.

## 4. Cyber Crime and Criminal Justice System

In criminal justice system, investigation into the crime and collection of evidence is of little consequence unless the prosecution is able to secure conviction of the accused. If the investigating agency is unable to get the accused convicted by the court, it has a damaging impact on the investigating agency and it creates suspicion about the motive and capability of the investigating agency. Securing conviction in cyber crime is not easy and straightforward. An accused may be hanged based on the printout of reports generated by the electronic devices. In some cyber crimes, all the evidences may be electronic evidence without any documentary evidence or human witness. Of course, the computer forensic examiner will be the percipient witness. The defendant is bound to question the admissibility, reliability and authenticity of the electronic evidences. The forensic examiner must be able to convince the courts about the admissibility, authenticity and reliability of the electronic evidence, and that the evidence has not been tempered with.

In India, there are computer forensic cells in the Central Forensic Laboratories (CFSLs) and General Examiners of Questioned Documents (GEQDs) at Chandigarh, Hyderabad, Kolkata and Shimla, and CFSL CBI at New Delhi. Even though most states have computer forensic units, they are very much dependent on the computer forensic cells of the central laboratories. This is a serious anomaly: while cyber crimes are to be tackled by the state governments, they do not the wherewithal to conduct proper investigation into cyber crimes. The courts in India generally accept only the reports of the central laboratories. The Code of Criminal Procedure (CrPC) recognizes only certain specified laboratories foe scientific examination. As the number of cyber crimes is going up by leaps and bounds, the workload on the central computer forensic laboratories has increased too much. In addition to submitting written reports, digital forensic examiners have to give witness before the courts, and are cross-examined. However, the capacity of handling digital forensic examination cases per examiner per year remains constant, leading to piling up of cases. Delay in forensic examination seriously hampers prosecution and obtaining the custody of the accused. Indeed, substantial expansion of the computer forensic laboratories is a crying need, because the laboratories do not have manpower and resources to meet even current level of requirements. If the expansion does not take place immediately, it will seriously hamper the prosecution of cyber crime cases in near future. Also, the laboratories need to be equipped with latest equipments, and outdated equipments should be replaced.

The central forensic laboratories cannot handle the increasing number of cyber crime cases, and it is essential that capability in state governments may be developed to handle cyber crimes. We need computer forensic cell even at the district-levels, not to talk of the state-level. The central laboratories may standardize the equipments, toolkits and software needed for digital forensic examination, and may standardize the procedure for the forensic examination. Technicians of state governments may be

periodically certified by the central laboratories. This will facilitate giving legal sanctity to the state governments to handle digital forensic examination, and present evidence before the courts. Of course, the examiners will also require legal empowerment under section 45 of Indian Evidence Act, and section 293 of Criminal Procedure Code. More officers need to be empowered under Section 80 of Information Technology Act to conduct search in cyber crimes. Moreover, since the private sector is better at absorbing new technologies, some form of public-private partnership (PPP) may be required in this field.

## 5. Concluding Remarks

The ICT revolution has not only affected our social and economic life, it has also impacted on how the criminals commit crime. Whether we like it or not, the incidence of cyber crime is bound increase. It has happened and is happening all across the world. We have to prepare our criminal justice system to deal with the emerging situation. The present level of manpower and resources in computer forensic laboratories are insufficient to meet even the current level of requirement. It calls for an overhaul of the system. Computer forensic laboratories must be strengthened with skilled manpower and latest equipments and software. In the MMPs on Courts and the Police, emphasis is on ERP solutions for the administration of the courts and the police, and not on adjudication on and investigation in cases involving electronic records and electronic evidences. Computer forensics must be central to the modernization of the police force. At the same time, the public prosecutors must be trained to present electronic evidences in a sound manner, and to argue the case in the cyber crimes. Unless we tackle the cyber crimes effectively, bring the offenders to book, and keep cyber crimes under control, the growth of the ICT in the country will be seriously hampered. It will undermine our efforts at e-commerce and e-governance.

***About the Authors***

*Barun Kumar Sahu* is an Indian Administrative Service (IAS) officer. At present, he is posted as Director (Personnel) in Ministry of Home Affairs. He did his B Tech (Hons) in Computer Science & Engineering from Indian Institute of Technology (IIT), Kharagpur. He has written a number of books in English and Hindi on bureaucracy, computer and tribal culture. His books on computer are: (1) Make Computers Speak Your Language and (2) Kampyutar Boley Apki Bhasha (Hindi). He also writes articles for magazines and newspapers.