

ISSUES OF POLICING THE CYBERSPACE

Dr. Pradnya Saravade, Dy. Commissioner of Police,
Enforcement, Crime Branch, C.I.D., Mumbai

Cyberspace is fast emerging as an alternate way of living for the growing generation today. Civilization has seen the development of many technologies in the past but the emergence of cyberspace is the most revolutionary since it has enabled an explosion in social communications between ordinary people across geographical and political boundaries. Youngsters are chatting with friends and strangers, doing their shopping, opening businesses, discussing issues close to their heart with people across the globe, all on the Net. Obviously then, the cyberspace is also attracting the social deviants to commit trespasses on acceptable social behavior on the Net. The typical cyber criminal today is a youth, who spends most of his time on the Net, who is technologically savvy and who either believes that he is invisible to law enforcement and the victim or who likes to play the game of 'Catch me if you can' with the law enforcement. Such a deviant is capable of doing immense damage to societies, nations and economies through his capabilities on the Net. What then are the issues of policing in cyberspace?

These issues can be conceived as three fold –

- a) Educative and preventive policing in cyberspace,
- b) Intelligence gathering for trends in hackers' and terrorists' methodologies and

- c) Crime Investigative policing.

To my mind, there is a serious gap in police capabilities and understanding on all the three issues in India. However, we have an advantage in policing the cyberspace as compared to policing in the physical world. We have the opportunity to create better systems and traditions of policing in the cyberspace, for the future. Can we, therefore, take the initiative?

In today's situation in India, there is a large generation gap between cyberspace users and non-users. At the family level, the parents are usually in the 'non-user' category whereas, the children are the 'users'. There are, therefore, no 'morals' in cyber usage. Supervision over Internet usage by youngsters is missing while at the same time 'work at the computer-table' by children is encouraged in homes and parents feel proud of the technological capabilities of their children. In a scenario of this nature, there is a felt need for law enforcement agencies to team up with the IT industry and propagate the 'do's' and 'don'ts' of cyberspace usage by school and college-going youngsters. It would be our job to create a groundswell of understanding on the part of all stakeholders in cyberspace, on the issue of cyber safety and cyber security. As part of preventive policing on the Net, it is important for law enforcement to reach out to the students,

parents, IT businesses and the average Net users to make them aware of legal boundaries while using the Net and also the pitfalls that they could fall into and become unsuspecting victims for criminals prowling in cyberspace.

In Mumbai Police, we had a successful beginning in educative policing of the cyberspace, when we launched the 'Cyber Safety Week' in 2003, August. We repeated the awareness raising exercise in August 2004 and received a tremendous response in terms of audience and speaker participation at various fora that were part of the Week-Long campaign. It is estimated that we could touch one lac stakeholders at the least during the 2004 Week.

The educative campaign for stakeholders, started by Mumbai Police, has crystallized in the formation of various formal meeting groups with e-business associations like NASSCOM and WIRC - ICAI (Institute of Chartered Accountants of India). We have also formed 'E-Security Clubs' in 17 colleges in Mumbai, wherein the education in e-security and e-safety will be a round-the-year process and done with the initiative of the college students themselves.

As part of our endeavor to enhance our own capability in investigation of cyber crime, we have started short (one week) training courses for the officers of Mumbai Police, wherein they are given inputs in the Information Technology Act-2000, procedures and protocols to be followed while seizing electronic evidence and the basic tools of cyber crime investigation.

So far, 178 officers of the city police has been put through this training at the Mumbai Cyber Lab, which is an infrastructure set up with the help of NASSCOM for enhancing police-public co-operation initiatives in cyberspace. Our experience with these training courses has shown that police officers shed their fears and inhibitions regarding cyber crime investigation after participating in the training. It is obviously very important that simultaneously while undertaking public awareness campaigns on cyber safety and raising expectations of people on the capabilities of the police to handle their grievances on Net usage, the police officers at both-the police station level and the Crime Branch level – are given the necessary wherewithal to handle such complaints. Therefore, 'Educative and Preventive Policing' should go hand in hand with developing capacity on 'Crime Investigative Policing'.

In order to earn public faith in the capacity of Law enforcement to secure the lives of citizens from terrorist attack, we need to develop expertise on tools to develop intelligence on the Net. Obviously, such capacity would be restricted to a core and elite team within the State Police – but develop and reinforce such a core team of IT sleuths we must and is the need of the times. Use of IT speeds and secrecy for interpersonal communication has been known to be regularly used by international terrorist organizations to wreak havoc on humanity. As law enforcement agencies, we require to evolve ways to co-operate internationally

to share information and prevent such serious crimes. As part of the Cyber Safety Week – 2004, we held a video-conference with a U.S. Law Enforcement cyber crimes specialist, to discuss how issues in cyber crime management are tackled there. The NASSCOM and Mumbai Police participated in this video – conference session. In order to reinforce interstate sharing of thoughts and to further co-operation on tackling cyber crime in India, we repeated a session called 'Sharing of Thoughts' in Cyber Safety Week – 2004. This session was first held in the 2003 Cyber Safety Week.

We invited and held discussions with senior, policy level police officers from many States like Rajasthan, New Delhi, Uttaranchal, Gujrat and Central Police organizations like the National Police Academy.

Along with our efforts to make the stakeholders think and focus on preventing cyber crime, it is felt that such efforts need to be replicated in places all over the country. It will not only set the trend for safe cyber usage within our own country, but also project the Indian Police as a leader in such initiatives world wide.



Never interrupt your enemy when he is making a mistake.

- **Napoleon Bonaparte** (1769-1821)

better to remain silent and be thought a fool than to speak out and remove all doubt.

- **Abraham Lincoln** (1809-1865)

Yes, the Cyber Cafe is almost ready for use, but wait for another 3 yrs, so that this Cyber Cafe gets electricity connection...

