



# ANDHRA PRADESH POLICE

## CID Journal

Issue : October, 2004  
Quarter : July - September, 2004

Copyright  
Additional DGP, CID, AP  
Hyderabad.

The Opinions in the articles contributed to this journal belong to the authors and do not purport to be official policy. The authors are also responsible for complying with the copyright laws.

**It is requested to e-mail articles to [spcyber@cidap.gov.in](mailto:spcyber@cidap.gov.in)**

### **For Departmental Circulation only**

Printed, Published and owned by  
**P.V. Naidu** IPS, Addl DG CID, Andhra Pradesh.  
Printed and Published at Hyderabad.

Printed at :

**Avighna Graphics (P) Ltd.**  
#6-2-14/1, Beside Curewell Hospital,  
Lakdi-ka-pool, Hyderabad - 4.  
Tel : 55502000, Telefax : 23315067

Edited by : **C.V. Anand**, IPS.,  
SP CID, Andhra Pradesh, Hyderabad.  
on behalf of  
Addl. DG, CID, Andhra Pradesh

# CONTENTS

---

S. No.	CONTENTS	PAGE No.
--------	----------	----------

---

## A : CYBER CRIME

1.	<b>CYBER CRIMES AND THE REAL WORLD SOCIETY</b> - Lalitha Sridhar	5
2.	<b>CYBER CRIME-A NEW CHALLENGE FOR THE POLICE</b> - Balwinder Singh, Addl. Sec, Central Vigilance Commission, GOI.	8
3.	<b>ISSUES OF POLICING THE CYBERSPACE</b> - Dr. Pradnya Saravade, D.C.P Enforcement, Crime Branch, CID, Mumbai.	13
4.	<b>INFORMATION TECHNOLOGY ACT 2000-A CRITIQUE</b> - M. Sivananda Reddy, S.P. Cyber Crimes	11
5.	<b>COMPUTER RELATED CRIMES</b> - Ramnish, Dy. S.P./CCIC/CBI	20
6.	<b>INVESTIGATION OF OBSCENE MAIL IN CYBER SPACE - A CASE STUDY</b> - P. Ravi Kiran and C.V. Anand, SI, Cyber Crimes PS and S.P. CID	30
7.	<b>SEARCH AND SEIZURE OF COMPUTERS</b> - U. Rama Mohan, Computer Crime Analysis Expert APFSL, Hyderabad.	32
8.	<b>TIPS FOR AVOIDING COMPUTER CRIME</b> - Cyber Crime Cell, CID, AP.	35

## B : GENERAL

9.	<b>FIRST INFORMATION REPORT</b> - E. Ramulu, F.M. Law, APPA	45
10.	<b>THE HIGHWAY MAN</b> - Abhilasha Bisht, Comdt, CPL, Battalion	50
11.	<b>CONSPIRACY</b> - BBC Online	53
12.	<b>HUMAN RIGHTS DURING ARREST AND DETENTION</b> - T. Murali Krishna, S.P., ACB	54
13.	<b>BEWARE OF THY NEIGHBOURS</b> - C.V. Anand, S.P. CID	59
14.	<b>A BRIEF HISTORY OF FINGERPRINTING</b> - (courtesy : google.com)	61
15.	<b>PRACTICAL STEPS TO IMPROVE COURT WORK</b> -Sri Papa Rao, D.S.P. CID	63
16.	<b>OLIVE GREEN PAGIDEE (TURBAN) NUMBER 6879077</b> - G. Jayaprasad Rao, D.S.P. CID	65

Bringing out an in-house, professional journal on time is not an easy task, many officers were contacted for articles but only a few responded-we hope for more cooperation in future!

It was thought that we should go in for 'Thematic' journals i.e. to lay stress upon a certain type of crime so that the journal becomes a reference point for investigators and other keen readers. The theme this time is CYBER CRIME. Experts in the field have tried to tell us the what - why - how of Cyber Crime and we are very grateful to them. There is another section on general subjects too so that it does not become too monotonous.

The next issue of this journal to be brought out in January, 2005 will have the theme "Frauds by Banks, NBFC and Financial Institutions". It is requested to kindly contribute by reducing your knowledge of a good investigation done to an article on that matter, and send it by e-mail to [spcyber@cidap.gov.in](mailto:spcyber@cidap.gov.in) or [cvanand99@yahoo.com](mailto:cvanand99@yahoo.com) or post it to

C.V. Anand, IPS  
SP, CID, New CID Building,  
Adj. to PTI Building, AC Guards,  
Lakdi-ka-pool,  
Hyderabad - 500 004.  
Tel : 040-23316754, Mobile : 9440627694.

We also solicit articles on other general topics / issues too for the remaining 50% of the journal.

The Addl. DG, CID has decided to not only appreciate your contributions through letters of appreciation but also pay some honorarium for each article contributed by you, beginning with this issue.

Editor

# CYBER CRIMES AND THE REAL WORLD SOCIETY

- by **Lalitha Sridhar,**  
Womens Feature Service

Our understanding of the virtual world is woefully slim; and of cyber crimes, even less. But, as law enforcers are finding out, their effect on the real world is devastating; preventing and detecting cyber crimes is now being given priority. Economic offences which dog the \$1.2 trillion electronic commerce industry worldwide include credit card schemes, property cheating, systems corruption, corporate and political espionage, mafia and drug cartels, multi-site gambling offences and Internet frauds committed mainly in the course of legitimate business.

At times, these assume the character of organized crime, involving accounting, management, administrative and political establishments. Even as law enforcers struggle to cope, other - and newer - violations loom large, the victims falling into an anonymous abyss. The Internet can, and often has, become the space for predators seeking women and children.

Studies have shown that about 60 per cent of all websites are sexual in content. Twenty per cent of them solicited their visitors, 13 per cent went voluntarily and the rest were pictorially lured. An estimated 100,000 pornographic websites generate revenues in the region of \$1 billion annually. The increasing popularity of chat rooms and the vulnerability of personal data to criminal access makes women and children the easiest targets for a range of culpable crimes.

The European Union has set up a Commission on Illegal and Harmful Content on the Internet. The United

States has a quasi-governmental organization called Internet Crimes Against Children Task Force. But computer sex offenders take advantage of the gullibility of their victims and the inept laws protecting them.

Children are victimized by pedophiles who are no longer lonely and hunted individuals - they are untraceable instead. Young people are exposed to pornography, hateful and violent literature, harassment, exploitation and spurious job rackets. Child molesters recruit, seduce and control the future of their victims on the Internet, capitalizing on the natural curiosity of children.

Cyber stalking happens when a person is followed and pursued online, privacy invaded, and every move watched. Cyber stalking usually occurs with women, who are stalked by men; or children, who are stalked by pedophiles. It is believed that over 75 per cent of the victims are female, in a form of harassment that can disrupt the life of the victims and leave them feeling very afraid and threatened.

Says V. Lalitha, Assistant Vice-President, Polaris Software Laboratory, Chennai: "In one landmark case in the United States, when a woman rebuffed the advances of a security guard in her office building, he posted her name, address, e-mail ID and phone number in pornographic chat rooms, with sexually explicit invitations promising her 'availability'. She was besieged by vulgar and offensive propositions, her home was stalked and her work life affected by obscene callers. She took the case to

court and the man was given a prison term of six years.”

With 19.5 per cent of online stalking translating into offline offences, cyber crimes can spill over to the real world with very real consequences.

Lalitha cautions that a common area of cyber stalking is ‘edu’ sites. In Mumbai, a 16-year-old-boy was kidnapped by a woman pedophile. Cyber crimes are very easy to commit and require very few resources in relation to the damage that can be caused. Family members have to watch out for symptoms in victims, particularly children. Cyber victims could be using inappropriate language or displaying an excessive fear of some places or things.

India is one of the few countries that has adopted the Information Technology Act, 2000. It has been lauded as a good beginning - but it is also seen as a bumpy start. The IT Act defines, among other things, what constitutes tampering with a computer source, hacking of computer document systems and publishing of obscene information.

But in what is widely acknowledged as a glaring lapse, it does not cover cyber stalking or child abuse. Unlike in a real world crime, a cyber crime is generally not preceded by a motive, the time zones can be different and a crime cannot be pinpointed to a particular hour. The crime could originate in one continent and target victims in another part of the world. Investigators find that data can be easily destroyed while clinching evidence is difficult to collect from voluminous weblogs, network and hard disk contents. Often, only strong circumstantial evidence is available.

“Finding a stalker is difficult, securing evidence even more so. The best defence is certainly prevention,” Lalitha says.

Says Sundari Nanda, Deputy Inspector General of the Indian Central Bureau of Investigation’s pioneering Cyber Crime Cell, set up in 2000: “Cyber crime is simply a normal crime facilitated by information technology. Most cutting edge law enforcement functionaries are not tuned into this yet. The minute the e-word comes in, it is the Cyber Crimes CBI Cell that is approached. Our experience has shown clearly that this cannot be a separate category for registration and investigation.”

Nanda emphasizes the need to orient legal officers and court procedures. “E-mails and computers were extensively used in the terrorist attack on the Indian Parliament. We come across cases of rape and murder with an IT component. Besides antiques and wildlife, women and children are victims of trafficking which originated in computers.” The CBI reports a spate of complaints originating from dating services and chat rooms.

There have been times when cases have had to be closed because the courtroom did not have a computer. Cyber cafes, preferred destinations for cyber criminals, remain unregulated. In one example from Pune, the court could not understand the intricacies of the case.

Problems beset law-enforcement efforts: The IT Act is ambiguous in many places; and multinational companies operating in India refuse to share information and insist they are governed by US secrecy laws.

Says Nanda, “Meaningful linkages and cooperation between agencies is vital to

cyber crime-solving. Cyberspace is an extension of the human experience. Internet users have to be made aware that there is an authority to complain to."

"Teenagers exult in an environment without strictures," continues Nanda, "They find their newly-found independence linked to a cyber identity. They find it exciting but they are extremely vulnerable."

Nanda recently went to Pondicherry to charge an 18-year-old wanted in an e-mail bombing case which held up a computer in the UK for four days. Public awareness, she says, is essential. "Women, teenagers and children have to be made wary of dating services and chat rooms for they are especially risky. No one is required to share personal profiles and information on 'public' spaces in the computer - hardly 10 to 15 per cent of the data sought is mandatory.

"Although limited Internet penetration curtails the number of possible victims,

connectivity is growing by the day in India and we must have a strong defence in place. Our greatest challenge is to make users aware of their rights. We need to evolve proactive measures to catch offenders - old ways cannot work for new problems."

It took 38 years for radio to reach 50 million people. Television reached the same number in 13 years. The Internet did it in four. By the end of 2002, there are expected to be 800 million Internet subscribers in the world. NASSCOM predicts there will be 23 million Net users in India by 2003.

Cyber crimes multiply, meanwhile, undetected and little-understood. When the victim does not even understand what his/her rights are, when the law is unclear about what precisely constitutes a crime, and when old infrastructure judges constantly changing technologies, cyber criminals can remain virtually free of both punishment and repentance.



"Policeman using a frisk engine on the internet".



"And another amazing feature of this model, it'll beep on the 27th of each month to tell you your payment's due".