CAPACITY BUILDING AT PS LEVEL

IN CYBER CRIME INVESTIGATION

SCHEME

FOR IMPLEMENTATION

AT

STATE HEADQUARTERS

AND

POLICE DISTRICT HQRS/COMMISSIONERATES

V.S.K. Kaumudi, IPS
Inspector General of Police
National Investigation Agency
New Delhi - 110001
08th April, 2016.

I N D E X

CAPACITY BUILDING AT P.S. LEVEL IN CYBER CRIME INVESTIGATION

- Most of the states are still 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 offences in the cyber world.

- Victims face problems in reaching out to the designated police stations for giving the complaint, though, legally speaking, all the police stations should be able to register cases of cyber crime.

- Cyber Crime cases pose several challenges in their prevention, detection, investigation and successful prosecution.

- According to NCRB reports, there is considerable increase in cyber crime every year, as can be seen below:-.

Increase in Cyber Crime:

A. India:

Year		No. of Cases
2011	…	1791
2012	…	2876
2013	…	4356

B. Undivided AP :

Year		No. of Cases
2011	…	349
2012	…	429
2013	…	635

- IT Act Amendment (ITAA) of 2008 brought within its ambit several new Cyber Crimes, to deal effectively with the menace. Police capability to deal with this new challenge is grossly inadequate.

Law enforcement agencies – Present situation:

- 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.
- Sustained awareness campaign is required, using all possible means, for promoting cyber safety.
- Standard operating procedures (SOP's) for investigation and detection of cyber crime, including search and seizure as well as preservation of digital evidence, must be formulated, so that the prosecution case stands the scrutiny of courts.
- Police must also use various sections of the IT Act for effective prevention and detection of Cyber Crimes. Some of the useful provisions are Secs. 69, 69A and Cyber Café Rules.

Cyber issues involving National Security

- Only recently India has announced its National Cyber Security Policy. Indian preparedness to deal with cyber crimes, affecting the nation or to protect its cyber assets and retaliate in a cyber war needs upgradation.

- States must identity and get their critical systems notified as “protected systems” under section 70A of the IT Act. The Central Govt. must identity and notify the national Nodal Agency for protection of critical information infrastructure.

- Security technologies such as IPV6, SSL, and encryption must be used when dealing with sensitive data.

- All ISPs need to be regulated and should have a well-structured architecture with in-built security features within the hardware and the software. Cooperation from public sector and private organizations is imperative for sharing of information, data mining and retracing the digital forensic footsteps of the cyber criminals.

- Police must take lead in issues connected with cyber crime in coordination with various agencies, as it is the only agency which can investigate and prosecute a cyber criminal under the IT Act.

The **Micro Mission – 06** of BPR&D clearly informs that the Government of India is getting ready to build capacity to investigate any type of digital technology related crimes, by developing the capacity of all the investigators at the Police Station level.

As per the ITAA, 2008, Cyber Crimes can be investigated by officers of and above the rank of Inspector of Police. However, the simple and traditional crime investigation also requires a lot of digital support these days. Hence, empowering the entire Police Department in Cyber Crime investigation is a compulsion in the present day world.

Capacity building of investigators in Cyber Crime Investigation requires :-

1) **Training:**

   a) State Police should introduce Cyber Crime Investigation Module at the induction level for SIs and DSsP.

   b) Hands-on training also needs to be imparted during attachment to the PS, in Cyber Crime Investigation and Forensics.

   c) The District Police may be assisted by IT Core Teams, comprising of members with keen interest in computer, in their regular technical requirements. Members of the Core Team may be trained at different levels, including TOT.

2) **Equipment:**

   Necessary equipment must be made available with the State Forensic Science Laboratories and some basic equipment should be available at the State/Dist/Commissionerate Hqrs.

3) **Man Power:**

   Generally, very few trained and capable officers are available at the State Hqrs. New and active teams need to be developed.

4) **Infrastructure:**

   Infrastructure needs to be developed at all the State Hqrs and Police District Hqrs / Commissionarate in each state.

2. PRACTICAL PROBLEMS IN INVESTIGATION

A. Technology related problems:

- **Lack of skilled manpower**: Investigation of cyber crime requires computer skills, mainly for on-site imaging of disks and on-site analysis and tracking of leads / trail.

- **Lack of technical and forensic equipment:** For investigation of cyber crime and securing digital evidence, special software and tools are required.

- **Lack of training:** There is need for officers in handling and application of forensic tools and techniques.

- **Lack of public awareness:** Wide publicity is needed on a sustained level, regarding modus operandi of cyber fraudsters, especially to alert them against dangers involved in responding to tempting e-mails or SMSs.

B. Internet related problems:

- Investigation related to Net to Phone activities.
- Internet using GPRS facility, where the same IP is given for many cell phones at the same time. (Natting IP / Framed IP)
- Getting information about IP addresses outside the country without Letter Rogatory is not possible. (e.g.: yahoo.com)

C. Cyber Cafes:

- Required user log is not maintained at cyber cafés.
- C'sP instructing net cafes to instal software, such as CLINK, but unregistered net cafes not installing it & some net cafes are installing

DEEPFREEZE software in the name of system security, which doesn't store any user data.

D. Banks

- Many Banks are not following the KYC norms.
- Most banks are not providing information for investigation quickly.

E. Service Providers:

- Mobile service providers not collecting proper address and identity proof of the customers.
- Identification of bulk push SMS origin is getting very difficult.

3. TYPICAL CYBER CRIMES

- **Online lottery frauds / online job frauds**

  In this type of offence, innocent people are contacted by the fraudster through both SMS and Email communication stating that they have won huge amount in lottery or got lucrative job offer. Slowly, in the name of customs, anti-terrorism, conversion, NOC, VISA processing, etc., incremental money will be asked to be deposited in bank accounts which are created with fake credentials. Mostly people from foreign origin (like Nigerians) are indulging in such offences. The money lost by the victims runs into crores of rupees. On the same analogy, people are being targeted and cheated in the name of jobs abroad.

- **Online harassment**

  Of late, there has been an increase in this type of offences and the victims are mostly female. The cyber criminal uses mobiles, emails and social networking sites to harass the victims creating fake identities, posting derogatory, obscene and private content, causing mental agony, and affecting family relations, leading to divorces and break-up of engagements.

- **Online cheating**

  Criminals are using matrimonial sites and other advertisement sites with false content to lure innocent victims, again mostly female, thereby cheating them for wrongful gain and blackmailing. In another type of offence, profile of divorced women is collected by these habitual offenders who lay a trap and convince them that they will marry them and take undue advantage of their situation through physical exploitation and cheating them financially.

- **Fake online appointments in reputed multi-national companies**

  For such offences, cyber criminals access the details of people whose resume is posted on different online job portals with their personal details. Using those details, the cyber criminals contact them and offer jobs and collect money in the name of processing fee, etc., for wrongful gain.

- **Phishing frauds:**

  In this line, cyber criminals contact netizens in the guise of popular banks, Income Tax Department, Webmail service providers, such as Gmail, Yahoo Mail, etc., and send messages asking the targets to part with their security credentials such as Username, password, account information, date of birth, etc., so that they can hack into those accounts for wrongful gain.

- **ATM, Debit and Credit card frauds:**

  These are all possible both online, by collecting the PIN numbers, CVV numbers, and offline, by cloning the card.

- **Hacking cases**

  The term Hacking has broad connotation, but in Cyber parlance it means unauthorized access. There are several ways and means used by these fraudsters to compromise computer security, bank accounts, mail accounts, websites and web servers for defamation, wrongful gain, cheating, stealing of personal data. In hacking cases, targets could be individuals, companies, nations or critical infrastructure.

- **Publishing of obscene content**

  This is also one type of online harassment, wherein victims share their intimate pictures, videos with people who manage to come very close to them and, at a later time, if some issues arise between them, the victims are targeted by publishing their personal / private videos, on the net.

- **E-Mail spoofing for cheating:**

  Import and export companies operating in the manufacturing and trading segments are receiving spoofed emails purportedly from international customers which are actually fake. The spoofed emails appear to be genuine as the contents are relevant to the business. The emails are sent to customers requesting them to transfer money to bank accounts st different locations across Asia and Europe. Unwittingly, following the instructions based on such email communications, money is being deposited in unknown accounts causing loss of several crore every year.

- **Cyber terrorism:**

  The most deadly and destructive form of cyber crime is “cyber terrorism”. The traditional concepts and methods of terrorism have acquired new dimension. In the age of information technology, terrorists have acquired expertise in producing the most deadly combination of weapons and technology, which, if not properly checked without delay, will take a heavy toll on the society. The damage, so occurred, would be almost irreversible and most catastrophic, in nature. In short, we are facing the worst form of terrorism, popularly known as “Cyber Terrorism”. The expression “cyber terrorism” includes an intentional negative and harmful use of the information technology which has both national and international ramifications on the economic, industrial and strategic fronts.

4. CAPACITY BUILDING: PHASE – WISE REQUIREMENTS

1. **Phase-I:** Cyber Crime PS, Digital Investigation Lab and Cyber Academy may be set up at the State Hqrs., in every state.

2. **Phase-II:** All the District Headquarters and Commissionerates should have, at least, one Cyber PS designated to deal with Cyber Crimes.

3. However, all the police personnel, irrespective of their place of posting, may be given hands-on training in CRIME INVESTIGATION USING DIGITAL TECHNOLOGY.

4. The Intranet facility of state police such as E-COPS is being integrated under the CCTNS Project for missing persons, unidentified dead bodies, etc., through programmes such as Child Track. On similar lines, some application to connect the data of all the cyber offenders committing crimes online, irrespective of the place where they stay, needs to be developed.

5. Tools such as Call data analysis and crime mapping should be kept for usage by any investigator online in the main server of the state.

6. There should be a **CYBER BULLETIN** within the CCTNS structure, wherein Police from different states could share the details of online offenders who are apprehended and are wanted. This data may be used by the entire police force in the Country. In the same bulletin, SOPs, Judgments, MOs and other related information may be shared among the investigators, as Cyber Crime is global in nature and criminals may operate from anywhere in the world.

5. DUTIES AND RESPONSIBILITIES OF CYBER CRIME PS AND DIGITAL INVESTIGATION LABS

- Registration of Cyber Crime cases whenever cognizable cyber crime is reported under the Information Technology Act.
- Investigation of cases registered at Cyber Crime PS and also those cyber crimes cases transferred to it from other units.
- Securing witnesses and recording their evidence.
- Collection of Oral, Electronic, Documentary and Circumstantial evidence from the victims / servers / computers, online servers, etc., to connect the offender to the offence
- Collection of evidence / information from Internet Service Providers, Mobile Service Providers, Banks, Financial Institutions, Payment Gateways, Online commercial websites, Email Service Providers, Social media service providers, etc.
- Preparation of Letter Rogatory, Look Out Circular, Red Corner Notices and Extradition proposals.
- Collection of appropriate certificates U/s. 65 (B) I.E. Act.
- Supervising and monitoring of pending trail cases
- Presenting evidence during the trial of cases.
- Collection of Intelligence regarding cyber crime
- Petition enquiries.

Certificate courses for the staff:

Training: The entire 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.

Basic training modules for two weeks are given below. Apart from this, some staff needs to be trained in Android, Java, C, C++, Pearl programming languages, etc., for high end investigation.

Why Digital Investigation Lab in Cyber Crime PS?

During the traditional crime investigation, forensic process comes at a later stage in the course of investigation whereas in case of Cyber Crimes / Cyber related crimes, investigation starts with the forensic process, such as Network Forensics, Onsite Forensics, Disk Forensics and Video Forensics. In these circumstances, there is imminent need for Digital Investigation Lab for identifying the criminal, based on technical clues.

Why Experts?

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.

6. TRAINING MODULES

a) LEVEL - 1 COURSE

Day	1000 to 1130 hrs	1130 to 1145 hrs	1145 to 1315hrs	1315 to 1415 hrs	1415 to 1530 hrs	1530 to 1545 hrs	1545 to 1645hrs
I	Welcome Address, Overview of Cyber Crime (to be handled by Police Officer / Project Manager)		Introduction to Computers (to be handled by instructor/ volunteer)		Computer Networking (to be handled by instructor/ volunteer)		Introduction to Internet browsing {some useful websites may be shown} (to be handled by Project Manager)
II	Basics of IP Address & EMAIL (to be handled by instructor/ volunteer)		Creation of Email ID for all the participants (to be handled by instructor / volunteer)		Tracing & Tracking of Email (to be handled by Project Manager)		Hands on Email tracing & tracking
III	IT Act- 2008, with amendments (to be handled by Police Officer / Legal Expert)	**TEA BREAK**	IT Act- 2008, with amendments(to be handled by Police Officer / Legal expert)	**Lunch Break**	Credit card frauds & online offences (to be handled by guest lecture (from Bank)	**TEA BREAK**	Credit card frauds & online offences - -Contd.
IV	Digital evidence: Basics(to be handled by Project Manager / Police Officer)		How to search & seize digital evidence (to be handled by Police Officer / Cyber Forensic Expert)		Basics of Mobile phone investigation (Project Manager)		Joining by all the participants - INDIACYBERCOP yahoo group (email sending / receiving)
V	Latest Modus Operandi of Cyber Criminals (Project Manager)		Revision of all the topics covered		Case Studies (Police Officer)		Issue OF certificates, feedback & valediction

b) LEVEL - II COURSE

Day	1000 to 1130 hrs	1130 to 1145 hrs	1145 to 1315hrs	1315 to 1415 hrs	1415 to 1530 hrs	1530 to 1545 hrs	1545 to 1645hrs
I	Welcome Address: Overview of Cyber Crime (to be handled by Police Officer / Project Manager)	TEA BREAK	Cyber security: Initiative of CERT, NTRO (to be handled by Project Manager)	Lunch Break	Computer Networking (to be handled by instructor / volunteer)	TEA BREAK	Introduction to virtual and cloud computing (to be handled by Project Manager)
II	Investigating Internet Crimes(to be handled by IO, Cyber Crimes)		Investigating Internet Crimes (to be handled by IO, Cyber Crimes)		IPR issues in Cyber Space (Legal Expert)		Dealing with offences committed /traced outside India (MLAT & LR Process) with sample cases(Police Officer / Project Manager)
III	Important provisions under IT ACT 2008 (to be handled by Legal Expert)		Important provisions under IT ACT 2008 (to be handled by Legal Expert)		Cyber Terrorism (to be handled by Police Officer / Project Manager)		White Collar Crimes (Lecturer from Banking industry / Police Officer)
IV	Study of Computer forensics guidelines (US-DOJ, US- Secret Service, etc.)		Volatile Data Forensics using LIVE Forensic tools (to be handled by Forensic Expert / Project Manager		CDR Analysis using software (to be handled by Project Manager)		Sample analysis of CDR by the participants
V	Study of Computer Forensic tools to acquire, recover &, analyse data.		Study of Computer Forensic tools to acquire, recover &, analyse data.		Case Studies (Police Officer)		Issue of certificates, feedback & valediction

7. ANNEXURES

ANNEXURE - I

MANPOWER REQUIRED FOR CYBER CRIME PS AT STATE HQRS

I. CYBER CRIME PS

SP / Addl. SP	1
Dy. Supdts. of Police	3
Inspectors	9
Sub-Inspectors	8
Head Constables	8
Police Constables	15
Home Guards	2
Total :-	46

(**N.B.:** Police / H.G. Personnel to have basic computer knowledge).

II. DIGITAL INVESTIGATION LAB

Inspectors	1
Sub-Inspectors	2
Head Constables	2
Police Constables	4
Private/Outsourced/Contractual experts for Mobile Tracking, Email Tracking, Disk Analysis, onsite Analysis, Imaging of disks.	9
Home Guards	2
Total	20

(**N.B.**: Police / H.G. Personnel to have basic computer knowledge).

III. TRAINING LAB

Project Manager	1
Trainer	2
Home Guards	2
Total	5

(**N.B.:** Police / H.G. Personnel to have basic computer knowledge).

EQUIPMENT REQUIRED FOR CYBER CRIME PS AT STATE HQRS.

I	**CYBER CRIME PS**	
1	15 Modular (8 GB RAM)computer work stations with one server(64GB RAM,8core) workstation for Officers	Rs.15 Lakh
2	UPS – 10 KVA	Rs.3 Lakh
3	Video Cameras – 5 Nos	Rs.2 Lakh
4	Audio recorders – 5 Nos	Rs.0.15 Lakh
5	Interrogation Room with sound proof and audio / video recording computerized system	Rs.10 Lakh
6	Air Conditioners – 2 Nos	Rs. 1 Lakh
7	Specialized training of all staff & experts	Rs. 10 Lakh
8	L.C.D. Projector	Rs. 1 Lakh
9	Printer – 3 Nos	Rs. 1 Lakh
10	Scanners – 3 Nos (Legal size)	Rs. 1 Lakh
11	Xerox machine (Heavy duty)	Rs. 4 Lakh
	Total	**Rs.48.15 Lakh**
II	**DIGITAL INVESTIGATION LAB**	
1	5 Modular computer work stations (64GB RAM and core 8 Xenon processor)	Rs.15 Lakh
2	**Encase (Ver-7)** Forensic analysis tool (This is a proprietary tool of guidance software. The advantage of this software is that it has special timeline analysis feature, which is not found in other tools)	Rs. 9 Lakh
3	Encase Portable: For onsite examination of hard disk (This is a tool for incident response at the crime scene, which has the capability to examine multiple computers at the crime scene, to identify relevant computer apart from RAM capturing facility). 2 nos	Rs.6 Lakh
4	Black Bag MAC OS imaging and analysis	Rs. 7 Lakh

5	C5 CDR Analyser	Rs. 3 Lakh
6	**Dossier Imaging Tool** with 8 TB Storage Media (This is a unique imaging tool to image one disk to two disks with 8 GB per minute speed and also has 8GB storage media.	Rs. 8 lakh
7	**Hard drive Duplicate equipment FALCON**: Is used for imaging of SATA, IDE, SCSI, USB drives with more than 8GB/minute speed.	Rs 6 lakh
8	**Write protect devices** for all storage media – Kit: Is used for preview the contents in the storage media without altering the data and maintaining the integrity of the data.	Rs.2 lakh
9	**Backbone tool:** Steganography application & detection tool: It searches files with hash matches of Registry Artefact key data base which enables any online stegno encrypted data.	Rs.2 lakh
10	**Online Social media analysis tools**	Rs. 6 Lakh
11	**FTK** – Hard Disk Forensic Tools for disk analysis	Rs.4 lakh
12	**Rainbow tables** for password cracking of several files and applications (not for emails)	Rs.6 lakh
13	**UFED** – Mobile Extraction tool for several mobile phones having phone memory.	Rs.18 lakh
14	**Cell ID** extracting tool: For identifying the available tower locations in the area in question.	Rs. 5 Lakh
15	**OCEAN Audio and Video enhancing and analysis tool.**	Rs. 30 lakh
16	Air Conditioners	Rs.2 Lakh
	Total	**Rs. 1,29.00 Lakh**

III	**CYBER ACADEMY**	
1	L.C.D. Projector	Rs. 2 Lakh
2	24 Thin Clients work stations and server for hands-on training of the participants	Rs. 18 Lakh
3	UPS – 10 KVA	Rs. 6 Lakh
4	Air Conditioners – 4 Nos.	Rs. 2 Lakh
	Total	**Rs. 28 Lakh**
GRAND TOTAL (I +II +III)		**Rs. 2,05,15,000**

ACCOMMODATION REQUIRED FOR CYBER CRIME PS AT STATE *HQRS.*

1. Police Station with work stations : 4,500 Sq.Ft.
2. DIGITAL INVESTIGATION LAB with work stations : 2,000 Sq.Ft.
3. Cyber Academy with required furniture and work stations : 2,000 Sq.Ft

ANNEXURE – II

MANPOWER REQUIRED FOR CYBER CRIME PS AT POLICE DIST HQRS/COMMISSIONERATES

I. CYBER CRIME PS

SP / Addl. SP	1
Dy. Supdts. of Police	2
Inspectors	6
Sub-Inspectors	6
Head Constables	6
Police Constables	12
Home Guards	2
Total :-	35

(**N.B.:** Police / H.G. Personnel to have basic computer knowledge).

II. DIGITAL INVESTIGATION LAB

Inspectors	1
Sub-Inspectors	2
Head Constables	2
Police Constables	4
Private/Outsourced/Contractual experts for Mobile Tracking, Email Tracking, Disk Analysis, onsite Analysis, Imaging of disks.	6
Home Guards	2
Total	17

(**N.B.**: Police / H.G. Personnel to have basic computer knowledge).

EQUIPMENT REQUIRED FOR CYBER CRIME PS AT POLICE DIST HQRS/COMMISSIONERATES

I	**CYBER CRIME PS**	
1	15 Modular (8 GB RAM)computer work stations with one server (64GB RAM,8 core Xenon processor)	Rs. 15 Lakh
2	UPS – 10 KVA	Rs. 3 Lakh
3	Video Cameras – 5 Nos	Rs. 2 Lakh
4	Audio recorders – 5 Nos	Rs. 0.15 Lakh
5	Interrogation Room with sound proof and audio / video recording computerized system	Rs.10 Lakh
6	Air Conditioners – 2 Nos	Rs. 1 Lakh
7	Specialized training of all staff & experts	Rs. 10 Lakh
8	L.C.D. Projector	Rs. 1 Lakh
9	Printer – 3 Nos	Rs. 1 Lakh
10	Scanners – 3 Nos (Legal size)	Rs. 1 Lakh
11	Xerox machine (Heavy duty)	Rs. 4 Lakh
	Total	**Rs. 48.15 Lakh**
II	**DIGITAL INVESTIGATION LAB**	
1	5 Modular computer work stations (64GB RAM 8 core Xenon processor)	Rs.15 Lakh
2	**Encase (Ver-7)** Forensic analysis tool (This is a proprietary tool of guidance software. The advantage of this software is that it has special timeline analysis feature, which is not found in other tools)	Rs. 9 Lakh
3	**Encase Portable:** For onsite examination of hard disk (This is a tool for incident response at the crime scene, which has the capability to examine multiple computers at the crime scene, to identify relevant computer apart from RAM capturing facility). 2 Nos	Rs. 6 Lakh
4	**Black bag** MAC OS imaging and analysis tool	Rs. 7 Lakh
5	C5 CDR analysis tool.	Rs. 3Lakh
6	**Dossier Imaging Tool** with 8 TB Storage Media (This is a unique imaging tool to image one disk to two disks with 8 GB per minute speed	Rs. 8 lakh

7	**Hard drive Duplicate equipment Falcon**: Is used for imaging of SATA, IDE, SCSI, USB drives with more than 8GB/minute speed.	Rs 6lakh
8	**Write protect devices** for all storage media – Kit: Is used for preview the contents in the storage media without altering the data and maintaining the integrity of the data.	Rs.2 lakh
9	**Backbone tool:** Steganography application & detection tool: It searches files with hash matches of Registry Artefact key data base which enables any online stegno encrypted data.	Rs.2 lakh
10	**Online Social media analysis tools**	Rs. 6 Lakh
11	**FTK** – Hard Disk Forensic Tools for disk analysis	Rs.4 lakh
12	**Rainbow tables** for password cracking of several files and applications (not for emails)	Rs.6 lakh
13	**UFED** – Mobile Extraction tool for several mobile phones having phone memory.	Rs.18 lakh
14	**Cell ID** extracting tool: For identifying the available tower locations in the area in question.	Rs. 5 Lakh
	TOTAL	**Rs.97,00,000**
	GRAND TOTAL (I+II)	**Rs.1,45,15,000**

ACCOMMODATION REQUIRED FOR CYBER CRIME PS AT POLICE DIST HQRS/COMMISSIONERATES

1. Police Station with work stations : 4,500 Sq.Ft.

2. DIGITAL INVESTIGATION LAB with work stations : 2,000 Sq. Ft.

ABSTRACT OF COST

1.	State Headquarters	..	**Rs.2,05,15,000**
2.	Police District Hqrs. / Commissionerate	..	**Rs.1,45,15,000**