The Indian Police Journal

April-June 2019 Vol. 66 No. 2

BOARD OF REVIEWERS

Editorial Board

CONTENTS

वरुण सिंधु कुल कौमुदी, भा.पु.से.
महानिदेशक

VSK Kaumudi, IPS
Director General

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
E-mail : dg@bprd.nic.in

MESSAGE

I am pleased to present the latest edition of our publication, **"Indian Police Journal"**, for the quarter April-June, 2019, on the occasion of the beginning of the Golden Jubilee Year of the Bureau of Police Research and Development. The Indian Police Journal is being published since 1954. With the creation of the Bureau of Police Research and Development on the 28th of August, 1970, the responsibility for publication of the IPJ was assigned to it. The Bureau inherited the legacy of the Indian Police Journal and it has become its flagship publication.

2.   The Indian Police Journal has created its own readership among police professionals, forensic practitioners, research scholars, academicians, management communities, civil society organizations and also in the field of Correctional Administration. It has been the continued endeavour of the Bureau to enrich our readers through well researched articles on subjects like Policing, Police Administration and Management, Correctional Administration and Prison Management, Forensics and sharing of good practices and standards among the police forces. I am sure, readers will appreciate our efforts and continue to extend their patronage.

3.   I further appeal to all our stakeholders, academicians and research scholars to help us in improving the quality and ensuring continuity and timely publication of the Indian Police Journal through their articles and feedback.

(V S K Kaumudi)

Editorial

It is my great privilege to announce that Bureau of Police Research & Development is entering into its Golden Jubilee year with celebration of this Foundation day.

A brief look at the work of Bureau of Police Research & Development indicates that it has been working for improvement in the delivery of Police services, under the overall guidance of the Ministry of Home Affairs.

In addition to its role in policy planning for smart as well as safe city projects, BPR&D has also taken the huge initiative in capacity building towards gender justice as well as containing crimes in general.

Significant projects that have had an impact on the quality of service of the police are also under progress. This includes Impact Assessment of Police Modernization Scheme, Crime Victimization Survey, Witness Protection Scheme, Highway Safety, Community Policing, and Student Police Cadet Scheme. In all its endeavours, the Bureau aims at augmenting the positive attitude towards service orientation, integrity, and professionalism among the policemen. All the authors eloquently contributed features on varied issues that need immediate addressing and make the journal one of a kind in many ways. All pieces without exception are fairly good and greatly informative one can not skip them at any cost. However, some extensively impressive ones, I believe must be talked about without prejudice. Some excellent vignettes of this collection, I pride myself on exhibiting are by Dr. Shamiulla, who in his paper very deftly explores the legal perspective of the global response to cybercrimes.

IT and computers have enhanced the scope of the police investigation to a great extent encompassing all focused areas. Dr. Mohit Kumar Garg, IPS in his write up discusses the evolution of legal provisions related to the admissibility of electronic evidence, which is vital. Besides, I cannot overlook the magnificent piece forwarded by Prasant N. Chaudhary and Jayanto N. Chaudhary that dwells at length on the need to ensure a sense of security in the North-East region and put forth their suggestions about making 'Act East' a reality.

An avid supporter of drones being used by different countries, Pankaj Kumar Singh, IPS asserts that Drone technologies are indeed a game changer and their right usage can not only cut down on time and costs but also help in optimal decision making.

In the meticulously researched article 'Child Abuse' the authors have given recommendations about the steps which could be taken to detect child abuse at an early age and save the life of a child.

Well, I find no end to it.

I express my profound gratitude to the members of this editorial team who have contributed a great deal to fostering intense and acute awareness and making the issue highly intriguing. The dedication undertaken by the writing crew is noble and unwavering beyond a shadow of a doubt. The issue displays an overwhelming response as a whole.

I hope, we will continue to get your support in the form of articles and feedback. Many thanks.

<div align="right">Editor in chief</div>

K Y C
KNOW YOUR CRIMINAL
A new initiative on Policing

Dr. Prateep V Philip, IPS*

KYC (Know Your Criminal)

1.1 Know Your Criminal or KYC acronym is a concept which has been derived from the well-known nomenclature of KYC, the widely known *'Know Your Customer[1]'* used by banks for collecting data on its clientele. Know your criminal concept can be employed by various law enforcing agencies for fast tracking different types of criminal elements - law and order, property crimes, drug offenders, traffickers, prohibition offenders, etc. As a well laid out process, it may turn out to be an effective tool of law enforcing agencies for verifying the identity of its potential criminals and updating records on repeated offenders. It would facilitate in assessing their criminal intent and activities in the public domain. The application of the concept of 'social network analysis' would make it further vibrant and effective.

1.2 The KYC concept developed by the Civil Supplies CID, Tamil Nadu is a much wider concept utilizing tools like Friends of Police, social network analysis, and statistics among others. The concept of KYC is linked to the *'80/20 Rule[2]'*. The domain of Business and Economics are familiar within the power of Pareto Principle. The 1848 born Italian philosopher and economist, through his various observations and investigations postulated a generalization that 80% of the things or results of action could be attributed to 20% of action.

i) The postulation about the imbalance of inputs and outputs is what became known as Pareto principle or the 80/20 rule. While it doesn't always come to be an exact 80/20 ratio, this imbalance is often seen in various walks of life.

ii) In the crime domain too, there are some notorious repeat offenders or *'recidivists[3]'* who commit a large number of offences.

iii) The ideal is to focus on these repeat offenders who are active and continuously commit offences

2.1   Evolution of KYC: The concept of history sheet has been a well established record in Police Department and is well laid down in PSO. The Civil Supplies CID, Tamil Nadu also maintains History Sheets on renowned criminals and smugglers. There are several columns maintained in history sheet which according to those times were apt and sufficient. But, these filled in details were often sketchy and irrelevant. Also, all details were not gathered and entered at all times. Hence, no quick inference could be drawn. Except by going through individual records. The history sheets have more or less been a reference document rather than a ready reckoner for actionable enforcement. KYC as a concept has been enunciated by Civil Supplies CID, Tamil Nadu to improve upon the actionable

Author Intro:

1   AAddl. Director General of Police Civil Supplies CID, Chennai

aspect and make it an effective tool. Experience tells that at supervisory levels one misses to monitor these criminals. Most importantly the potential perpetrators who are habituated to committing serious crimes easily evade our focus. Hence most of our efforts go in fire-fighting rather than doing pro-active policing. KYC uses much wider information gathering concepts including use of Friends of Civil Supplies CID and 'Social Network Analysis[4]' besides the use of statistics.

2.2   Key Elements of KYC: KYC policies incorporate the following five key elements:

•   Criminal identification procedures;

•   Criminal information management policy;

•   Social Network Analysis;

•   Monitoring activities; and

•   Legal follow up.

Key Elements of KYC
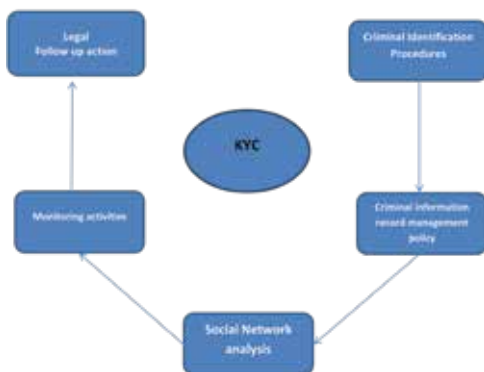
2.3   Premises of KYC: Relevant information about "clientele" is premium.

1.   Information is available in records.

2.   Information can be collate and compared from field verifications including FOPs.

3.   Information from alternate sources viz., Friends of CSCID is valuable.

4.   Information can be analyzed by use of statistical means, social network, etc.

5.   Valuable inferences can be drawn from the available information

6.   The information must be followed up.

7.   Clientele's records must be standardized and must not be knee jerk and ad hoc.

8.   Records must be maintained and updated well

9.   Intelligence collection must be timely and systematic.

10.   KYC is existential.

2.4   Benefits of KYC: The KYC approach helps us to tackle this issue effectively.

1.   It focuses on the top notch criminals.

2.   To arrive on the KYC, data of the past few years is required to be reviewed and based on it, the top criminals can be assessed.

3.   Some criteria depending on the type of criminals being profiled, to be defined so that the KYC filtering can be done from the existing data on crimes.

    a)   Detentions

    b)   Cases registered

    c)   gravity of case

    d)   Quantum of Property seized or recovered

    e)   Area of operations

    f)   No. of associates or gang members, among others.

4.   After doing a qualitative analysis of the given criteria the KYC can be arrived at. This would be a terse number which may be directly monitored by the supervisory officer. Hence it makes policing proactive as the top most criminals are well known to the senior level officers and they can monitor whether those criminals are active / dormant / in waiting.

5.   Once the KYC list is ready then next comes the follow up. The follow-up in KYC requires not only the close monitoring of the criminals but also includes the social network analysis. It is also an enabling tool for predictive policing.

KYC in Use With Social Network Analysis
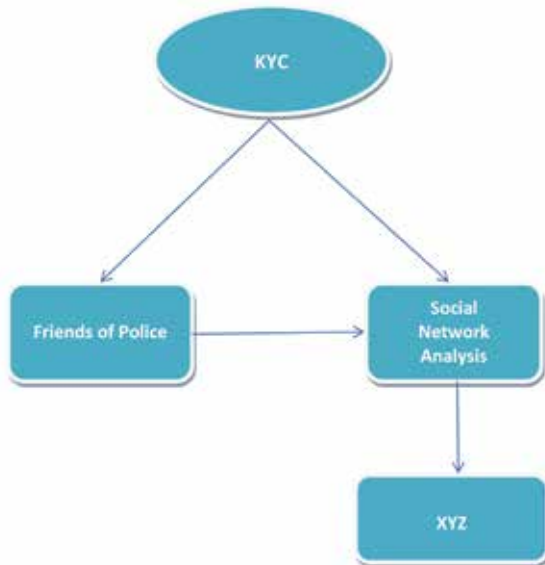
3.1   Methodology for KYC :

1. **Friends of Civil Supplies CID:** It's a novel concept introduced by Tamil Nadu Civil Supplies CID. It entails regular organizing of stakeholders meeting and enrolling of friends of CSCID or FOPs (used interchangeably). FOP is an important feedback mechanism and field verification tool for KYC for keeping tabs on top notch criminals.

2. **Stakeholders Meetings:** The Stakeholders comprise citizens from all walks of life. Like the general public who are ration card holders, Transport drivers, Transport contractors, godown staff, loadmen, civil supplies staff etc. The meetings become a platform where awareness is generated regarding a plethora of issues pertaining to public distribution system. It is also a way to get to know the PDS issues ailing the grassroot level. The grievances expressed by public are taken up for redressal. Around hundred such issues were taken up and were resolved.

3. **Stakeholders Committees:** At the Zonal and Subdivision level, the supervisory officers have formed a Stakeholders Committee. These Committees consist of the jurisdiction SP, DSP, TNCSC officers, Vigilance Officer of TNCSC, Civil Supplies serving or retired staff.

4. **Statistical Analysis:** Any records available to us can be analyzed by use of statistics to gain useful information for further implementation. The main aim here is to establish identity of top notch criminals and using Pareto's principle go for the top 20 % criminals to get 80 % results. The top notch criminals can be identified by frequency of repetition in any of important variables including BM detentions, High value Seizure cases, Four wheeler cases, no of associates involved, area of operation among others.

5. **Social Network Analysis:** Social Network Analysis (SNA) is the process of investigating social structures through the use of networks and graph theory. In law enforcement it characterizes analysis of kinship, social and commercial structures along with their backward and forward linkages to establish and decimate the structures. Social Network characterizes networked structures in terms of nodes (individual actors, people, or things within the network) and the ties, edges, or links (relationships or interactions) that connect them. Examples of social structures commonly visualized through social network analysis include social media networks, memes spread, friendship and acquaintance networks, collaboration graphs, kinship, disease transmission, and sexual relationships. These networks are often visualized through sociograms in which nodes are represented as points and ties are represented as lines.

Social network analysis is a term used in sociology now interpolated in many fields including policing pertains to our analysis of transactional aspects of social systems wherein social interaction be it kinship, family or friendship ties are used for transactions of an organized crime. Many families have been found to be involved in such crime. A careful study of Sociogram of transaction gives a useful insight into the interactions which can lead to drawing out details of other accomplices. These can further be treated mathematically to arrive at deeper inferences mostly used to analyze international terrorism and narcotics.

In policing parlance it means the analysis of the larger network which exists around the criminal. It includes:

a.   Phone numbers used by the criminal and his family.

b.   Place of residence/ hideouts.

c.   Accomplices and gang members and their contacts too.

d.   Vehicles used by criminal/ accomplice.

e.   Extrapolating all such information which may facilitate in close tracking of his activities.

f.   Maintaining a record and updating it from time to time.

g.   The Social Network Analysis is a peace time exercise which is to be initiated as soon as the KYC gets listed.

Concept of a Social Network

Social Network Analysis Through Stakeholders

An initiative has been taken to make Community Policing as a part of an effective operation for Civil Supplies CID. Community Policing aspect has enabled in intelligence collection, giving important inputs and suggestions for the improvement of the PDS system. Even the Stakeholders are fundamental from enforcement point of view. Their inputs can be utilized in the Social Network Analysis for improving the intelligence base and strengthening the enforcement as well as preventive policing.

3 Levels of Social Network Analysis
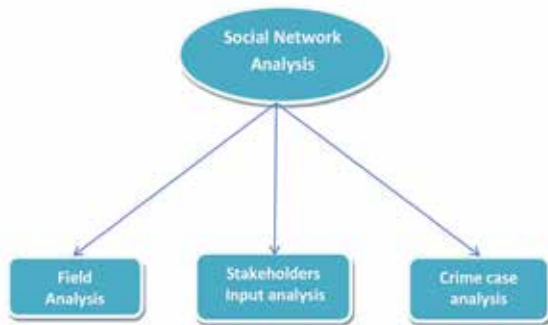
Case study 1: KYC and Social Network Analysis with XYZ: Pattani Case, Tuticorin.

Tuticorin conducted several Stakeholders Meetings and enrolled about 28 Friends of CSCID. They have maintained the KYC details for the unit. During their weekly stakeholders meetings the KYC accused were also discussed. On 16.04.2018 Inspector of Police, CSCID, Thoothukudi got information from FOP regarding smuggling and hoarding of rice near SSRBS Bus company, Kalughumalai to Sakarankovil Road, Thoothukudi. The team intercepted the Lorry bearing Regn no. TN-09-Y-6696 and seized 106 Plastic Bags of PDS rice (5300 KGS) hidden under bags of oil cake, Coriander, Urad dhall and Tarmat and arrested accused Mohaideen Pattani, Janarthanan and Muppiliraj. On Social Network Analysis it came to light that Pattani was the organiser, Raj @ Periyasamy of Paruthivillai and Kaliraj of Malaiyadikurichi were local aggregators of PDS rice who collected rice from households. Mohaideen Pattani hoarded rice bags in a hired place in Melasokkanpatti. He transported rice through Janarthanan, owner of Balachandira vinayagar lorry set from Virdhunagar to Kerala and sold it to Abdul Majid, owner of Oachira Trading Company, Chullimanoor, Nedumankadu Post, Kerala state. He bought the Horse brand empty bags from K.P. Murugan Store of Keezhla

Pavoor and weighed it 50 Kgs through weighing machine and stitched the bags through stitching machine. Mariappan of Puliyangudi who owned Mahindra Maximo load Auto bearing Regn No. TN-76-U-4635 carried rice from hoarding place to transport office at Virudhnagar. In this regard, a case was registered in CSCID Cr. No. 57/18 u/s 6(4) of TNSC (RDCS) order 1982 r/w 7(1) a (ii) of EC Act 1955.

Further, based on FOP information Mariappan, Raj @ Periyasamy and Kaliraj were arrested. Accused Muhaideen Pattani was taken from Judicial Custody to Police Custody and enquired. He gave the PDS rice to Oachira Trading Company, Chullimanoor, Nedumankadu Post, Kerala state. Then a team went to Oachira Trading Company, Oachira complex, Sullimanoor Post, Nedumankadu, Trivandram, Kerala State along with accused Pattani and enquired one Abdul Qasim, who is a brother of Abdul Majid, and searched the premises.

Lots of efforts were taken to unearth the network and KYC concept was utilized along with use of FOPs and SNA and XYZ circle was established.

Case Study 2: KYC and Network Analysis: Ahamed Ali @ Bhavanibhai

Ahamed Ali @ Bhavanibhai,a notorious PDS rice smuggler, native of Keelakkarai, Ramnad came to Bhavani, Erode about three decades back. He is involved in PDS rice smuggling since 1996.

He has been involved in 36 PDS rice hoarding and smuggling cases under EC Act and facing trial. His family members are not involved in any EC Act offences so far. He is an active and habitual smuggler of PDS rice. He procures rice from card holders and sends it to Karnataka. His name also finds a place on the list of KYC for Erode, CSCID unit. While conducting Stakeholders meeting among the members of the Stakeholders, the details of Ahamed Ali @ Bhavanibhai and his

activities were shared and the Stakeholders were requested to convey his present whereabouts. He had been absconding since his latest case in Erodes CS CID Cr.No.131/17. Inspector of Police, CS CID, Erodeverified the cell phone call list of Bhavanibhai's social network and relatives and located his hideout and arrested him at Chennai, Periyamedu, near the Srisai park lodge on 01.03.2018. He has been detained under BM Act and Advisory Board also confirmed the BM order. At present he has been lodged in the Central Prison at Coimbatore since 01.03.2018.

With the use of KYC in stakeholders meetings and use Social Network Analysis and FOPs, a notorious offender was secured.

Case study 3: KYC and FOP: J. Christopher

J. Christopher is the one of the most notorious PDS rice smugglers in the state. He is a history sheeted Black marketer in Chennai unit (HS No.01/2014). He is a native of Naganai village, Santhakulam Taluk, Tuticorin and now resides in Ambattur along with his wife Prema and his son Hentry, daughters Soniya and Rose. He is involved in several cases of procuring PDS rice from the public and the brokers, hoarding and transporting the same to neighboring states like Andhra and Karnataka. He operates in Vellore, Kancheepuram and Thiruvallur Districts. In this connection totally 18 cases have been registered against him, 6 cases in Kancheepuram unit, 3 cases in Thiruvallur unit, 4 cases in Vellore unit and 5 cases in Chennai unit. He has been detained six times. His activities are constantly under watch by the CSCID with the help of FOPs. As a result, on 10.12.2017 his 10 associates were arrested for smuggling 4000kgs of PDS rice through a 407 van bearing no.TN-07-E-5266 after registering a case in Chennai unit crime no.287/2017 U/s 6(4) of TNSC (RDCS) order 1982 r/w 7(i) a(ii) of EC Act 1955. Further, on

17.12.2017 the accused Christopher and his associates Pathrasanan and Karthiksmuggled 2000kgs of PDS rice through the TATA 407 van bearing No.TN-29-E-7843. In this connection a case was registered in Chennai unit Crime no.295/2017 U/s 6(4) of TNSC (RDCS) order 1982 r/w 7(i) a(ii) of EC Act 1955. The accused Christopher absconded in the above two cases. The unit made continuous and tireless efforts, and with help of FOP assistance, the excellent guidance given by ADGP, in segregating the noted accused under the novel scheme of KYC, the team arrested him on 10.03.2018 and detained under PBM EC Act. Till now he is in Puzhal Central Prison.

Case Study 4: Thiruvallur Seashore Case.

Regular stakeholder meetings were conducted in Thiruvallur to prevent the smuggling Activities of PDS Rice and 22 FOPs were enrolled all over Thiruvallur Dist. One of the FOPs from Gummudipoondi area gave fruitful information that PDS Rice was stocked illegally in several seashore villages around Gummudipoondi and was being collected by a Tarrus lorry registration Number AP-27 X-1886 once a month at midnight. Some of the villagers were also party to these activities. Hence, it was not possible to secure the lorry inside the villages and also there were several routes from that area to Andhra Pradesh. Upon receiving the information on 15.06.2018 midnight that Tarrus lorry entered the village area, immediately Thiruvallur CSCID Inspector and the party conducted a vehicle check before the Sullurpet check post and secured the lorry and seized 317 bags of PDS rice (13,000 kgs).In this connection, a case was registered.

Fruitful information from FOP and purposeful stakeholders meetings resulted in such a good catch.

Case study 5: KYC and Social Network Analysis in Smuggling as family business: P Dhanapal case.

P. Dhanapal s/o Pallipattan, Mottur Village, Vellore resides with his wife named Geetha, elder son Suresh, younger son Murali and daughter Usha. During his early days he sold Karee leaves in Vellore Bus-stand and later he bought an auto and used the same for rice smuggling to Andhra. Subsequently from 2011 onwards, he himself collected ration rice from card-holders directly and smuggled the same. On 11.01.2018, upon getting information from FOP the Krishnagiri CSCID unit seizeda lorry Regn. No. TN- 23-1857 with 16,200 kgs of PDS rice at Toll plaza but the driver Rajesh of Kancheepuram escaped. In this connection, a case in Krishnagiri CS CID Cr.No.4/2018 u/s 6(4) of TNSC (RDCS) order 1982 r/w 7(1) (a) was registered and is being investigated.

On 05.06.2018, on FOP information, Vellore CS CID Police personnel reached the spot where Dhanapal and his sons Sureshand Murali were loading the ration rice into lorry AP 03 TB 9374. Murali was apprehended by the police party. In this connection, a case in Vellore CS Cid Unit Cr.No.108/2018 u/s 6(4) of TNSC(RDCS) order 1982 r/w 7(1)(a) has been registered against Dhanapal, Suresh and Murali.

The police team camped in the residential area of the accused and also conducted frequent stock-holders meeting from which they received information about the hide-out of the accused. Later, Dhanapal was apprehended from a farm-land where he had gone into hiding on 26.06.2018 and remanded. Further, it is submitted that action has been taken against Murali and Dhanapal to detain them under B.M. Act. The proposals are submitted to the District Collector, Vellore District and it is being followed.

Case Study 6: FOPs and Stakeholders meeting : Madurai case

Madurai unit has been conducting stakeholders 0meetings regularly and has enrolled 31 FOPs. On 05.12.17 at 1900 hrs the police party received information from friends of CSCID that TNCSC contract lorries along with PDS rice were moving inside one Sasikala modern rice mill Kalmedu, Madurai. Immediately DSP along with police party rushed and found that two TNCSC contract lorries bearing Registration No TN 67 A 3252 and TN 28 V 6162 parked inside the rice mill campus with 110 bags of PDS raw rice in the lorry TN 67 A 3252 and 86 bags of raw rice in the lorry TN 28 V 6162 with FCI godown seal slip. Soundrapandian (Manager of the mill and TNCSC contracter of the Lorry) and Sethukali (Owner of the Rice Mill) were arrested. A case was registered in Madurai CSCID Unit Cr.No. 203/17 U/s 6(2) (3)(4) of TNSC (RDCS) order 1982 r/w 7(1)(a) (ii) EC Act 1955. Later, Ravichadran (salesman of Viraganoor ration shop) and other drivers were arrested. The accused Soundrapandian was detained under BM Act.

By way of having bi-weekly stakeholders' meeting and enrolled FOPs, a big case was detected.

Utility of KYC For General Policing :

The KYC concept is an effective tool of policing as it brings into focus the 20% most notorious criminals within active supervision. Based on Pareto's principle it is these 20% who indulge in 80% of criminal activities. The concept can be useful in broader areas of policing like economic offences, cyber-crimes, crime against women, property offences, etc. In all these domains of crime, there are repeated offenders who are

frequently indulging in anti-social activities. The KYC would give a cogent frame of reference to the supervisory levels to see that the most notorious accused are monitored and their activities are curbed to prevent further damage. With an efficient follow–up system the KYC approach would result in focused monitoring, preventive policing and proactive enforcement.

References:

1. Michael Volkor,Know Your Customer ("KYC") Due Diligence Best Practices, in www.volkovlaw.com, July 9, 2015.

2. Kevin Kruse, 'The 80/20 rule and how it can change your life' in www.jorbes.com, March 7, 2016.

3. Don A.Andrews, 'Recidivism is predictable and can be influenced : using Risk Assessments to reduce recidivism', Forum on Corrections Research 1(2), Pages 11-18, 1989.

4. Scott John, 'Social Network Analysis' Sociology 22 (1), Pg 109-127, 1988 also available on www.journals.sagepub.com.

Paper Based Conventional and Digital/Electronic Forensic Documents: Emerging Trends and Changing Notions

M. C. Joshi*

Abstract

Forensic Document Science has travelled a long way through the ages and has undergone tremendous changes with the time and technological developments. Nature, pattern and tools of document frauds are changing with technological advancements, especially with the advent of digital tools and techniques. Ours is an age of tremendous growth of knowledge and effective vigilance / investigation cannot be accomplished by old fashioned hit or miss techniques. More scientific and technological discoveries have been made in the past years and they have a profound effect on the world of crime and criminals. The conventional crimes have given a way to the sophisticated **white-collar crime** committed by professional criminals armed with latest advancements in Science & Technology. Documents are mute witnesses and many a times they become vital links in a chain of evidence in serious crimes like kidnapping, arson, murder, defamation, fraud, forgery, misappropriation or criminal misconduct, embezzlement, seditious or anonymous communication etc. With the advancements and easy access to high quality plain paper copiers, digital image acquisition, processing and reproduction technologies, the fabrication of documents, security documents, Bank Notes, Passports, etc. have become easier and closer to perfection. This has led to the uncovering of new dimensions and intricacies of white-collar crimes and digital frauds on the one hand and facing of new challenges of their detection on the other. This article is aimed to present changing notions and emerging trends in forensic documents i.e. conventional and digital as well as new tools to cope with such trends and professional hazards associated with this specialised forensic domain arising out due to these trends & notions.

Keywords:

Forensic, Documents, Digital, Cyber Crimes, Counterfeit, Technology.

Historical Background

This is an age of **documents-conventional or digital/electronic** besides being an age of anxiety. Documents feature in our financial, legal, business, social and personal affairs. Hardly a day goes by without some documents playing a part in the life of every one of us.

Due to their widespread use in almost all walks of life, spurious documents are produced for perpetrating crime of varied nature, impact and intricacies. They are the **true** and **mute** witnesses and many a time they become vital links in a chain of evidence in serious crimes. The **white-collar crime and digital crimes of electronic**

Author Intro:

* Deputy Director & Scientist 'D', GEQD, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Govt. of India, SHIMLA

world are inextricably involved in the entire area of vigilance / crime investigation and form more than 70% of the **irrefutable physical evidence** in one or the other form.

We are living in the age of documents of both types-conventional paper based and digital/ electronic. It has been rightly pointed out by one of the eminent forensic scientists, James V P Convey in the book 'Evidential Documents' that 'Society has evolved literally into a world of Documents'. Perhaps the documents are as old as the documents themselves and are mute but true witnesses. Documents in any form are questioned or disputed because of their origin, contents or the circumstances regarding their usage/production, execution and location and which arouse serious suspicion regarding their authenticity. Like other profession, the science of questioned/forensic document examination has organisation, systems, faculties, problems and goals dedicated to its advancement & innovation with the growth of science and technology. The scientific examination of documents of any form and nature, being a scientific process basing its origin with in the legal system, rests upon the various principles, instruments, tools and software, chemicals, light arrangements and gadgets used by the forensic experts to search for the truth of immense evidentiary value in the administration of criminal justice system.

Peeping into the past, the history of handwriting analysis to assess personality, today called graphology- is an art and could be said to extend back to Confucius, who wrote: "Beware of the man whose writing sways like a reed in the wind." The first extensive work on handwriting analysis dates to 1622, when an Italian physician named Camillo Baldi published a method to recognize the nature and quality of a writer from his letters. In this book, Baldi stated the fundamental premise that continues to guide handwriting analysis today: "It is obvious that all persons write in their own peculiar way .

. . . characteristic forms . . . cannot be truly imitated by anybody else. In other words, 'like snowflakes, every person's writing is unique'. In past, Alphonse Bertillon, a French Scientist postulated 'Bertillon age' and made sincere efforts to bring the crime investigation on more scientific and analytical mode.

In context of modern Forensic Science in general and Forensic Document examination in particular, experts sharply and scientifically distinguish graphology from true handwriting examination. Graphology is a pseudoscience- a fun but not scientifically valid, although many corporations and corporate houses take it seriously enough to hire graphology experts to profile job candidates. While graphology is not regarded as forensic evidence, in past, it is used in combination with other techniques to profile criminals to aid authorities in their investigations. Authorities in the field of Scientific Examination of Questioned Documents such as- A S Osborn, Ordway Hilton, Wilson R Harrison, VP Conway, Huber R.A. & Headrick A.M. and David Ellen, etc., brought the examination of forensic documents on more scientific footings in 20th century and established the fact that it is an important tool for *corpus delicti* and declaration of any suspect document, spurious or otherwise. Professor of Criminalistics, Emeritus/ eminent Criminologist, Paul Kirk (1902-1970) has correctly observed with respect to the Handwriting examination that - *'The identification of Handwriting is most difficult of all the identifications'*.

More commonly, forensic scientists use hand writing examination for two defined purposes. One is to authenticate documents such as records, diaries, wills, and signatures. In 1983, for example, a German publisher claimed to have in its possession a collection of sixty-two notebooks that were the handwritten diaries of Nazi dictator Adolf Hitler. Handwriting analysts compared the writing in the diaries with known samples of Hitler's handwriting and concluded

that the diaries were authentic. Later analysis of the paper and ink, though, showed that Hitler could not have written them and investigation revealed that they were the work of a clever forger who was able to copy Hitler's handwriting (so successfully that one of the known samples used by the handwriting experts was itself a forgery by the same person). A similar case involved the 1991 claim by a man from Liverpool, England, that he had in his possession a sixty-three-page diary and that its author, one James Mayrick, was the notorious Jack the Ripper, who brutally murdered five London prostitutes in 1888. While analysis of the paper and ink showed that the diary was not written with modern materials, handwriting analysts concluded that it was a fake.

The second purpose for which handwriting examination is used is to link a specimen of handwriting with a crime suspect by comparing the suspect's handwriting with Questioned handwritings, for example- handwriting on a ransom note or other communication linked to a crime. The purpose is not to profile the writer but to determine if the same person produced a document known to have been written by the suspect, called an exemplar or standard, and the document in question. One of the first noteworthy cases in which handwriting analysis of this type was used was in the 1932 kidnapping and murder of Charles Lindbergh, Jr., the infant son of aviation hero Charles Lindbergh. During the investigation, Lindbergh received fourteen notes from the kidnapper. Handwriting analysis later linked these notes to Bruno Richard Hauptmann, who was convicted and executed for the crime. Even, in India Forensic Document examination has played an important role in bringing culprits to book such as Harsh ad Mehta mega-security scam, Satyam Fraud, Fodder Scam, JBT scam, CGHS frauds, Impersonation cases of recruitment institutions, Mukherjee Commission on Netaji Subash Chandra Bose, etc.

Handwriting Experts try to maintain a strict protocol with criminal suspects. They educate investigation officers not to show the suspect the questioned document and never guide the suspect how to spell or write certain words or how to use punctuation. The suspect is to use writing materials similar to those of the questioned document. The dictated text should in some respects match the content of the questioned document so that the spelling and handwriting of certain words and phrases can be compared. In either type of case—whether authenticating documents or investigating criminal suspects—handwriting analysts begin from the premise that while most people learn to write using a certain system, such as the Palmer or Zaner-Bloser system, they develop idiosyncrasies in the way they form letters and words. These idiosyncrasies and individual writing habits or specific writing impulses become fixed like dents scars and remain constant over time, even when the person is attempting to disguise his or her writing.

The handwriting examination is a valid and important forensic technique to have concrete findings of immense evidentiary value. Prof. John .H. Wigmore (1863-1943), an eminent American Jurist and expert on law of evidence has stated in the introductory remark in *A S Osborn's book 'Questioned Documents', year1911 that 'A firm place has now been made for the expert witness who is emphatically scientific and not merely empiric'*. He further adds *'Each age has its crimes, with the corresponding protective measures-all alike the products of the age's conditions, and then society awakes and gradually overcomes crime by discovering new expedients'*. Therefore, it was regarded as valid and reliable evidence in court under the so-called Frye standard test, which said that judges had to accept any form of expert testimony, including that of handwriting analysts, based on techniques generally accepted by scientists. The existence

of such groups as the American Society of Questioned Document Examiners suggests that a community of scientists generally accepted the premises and techniques of handwriting analysis. Further, the U.S. Secret Service and the German law enforcement agency, the Bundes kriminalamt, maintain that their computer databases, the Forensic Information System for Handwriting (FISH), prove that among a large sample of writers, no two shares the same combination of handwriting characteristics. In 1993, Gerald R. McMenamin coined a new term 'forensic stylistics' which says- Author-specific linguistic patterns can be objectively described and often measured, making author identification possible in many cases on the basis of syntax, synthesis and colloquialism, etc.

Since 1993, though, the admissibility of handwriting analysis has come under intense scrutiny. That year, the U.S. Supreme Court, in Daubert v. Merrell Dow Pharmaceuticals, created the stricter Daubert standard, which gives federal judges under the Federal Rules of Evidence more discretion in admitting or excluding scientific testimony. Specifically, it requires judges to determine whether a theory or technique has been tested, whether it has been submitted to peer review, whether standards exist for applying the technique, and what its error rate is?

White Collar Crimes

The term "white-collar crime" was first used by an American criminologist, Edward Sutherland, in 1940, in his classic paper entitled, "White Collar Criminality". According to him, there are important sociological differences between those who commit conventional crimes, such as murder or burglary, and those who are involved in white-collar crimes. He said that the persons of respectability and social status in the course of their occupation commit white-collar crime.

In their book entitled "Crime at the Top", the Criminologists Johnson and Douglas defined it as, *"White collar-crime is an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage". "White-collar crime is primarily a non-conventional offence committed by any person with a dishonest or fraudulent intention with the motive that he may wrongfully gain or wrongfully retain money or property. It is the violation of a position of trust by someone in a formal role relationship with another person for private profit or other personal advantages".* White-collar crime is generally intended to reap monetary benefits from individuals, establishments or the State, by fraudulent means using the tools of crimes such as pen, paper, computer, mobile, etc. Its current usage includes a broad range of non-violent offenses, where cheating, dishonesty and corruption are the central elements. They are also referred to as "**commercial crime**", "**business crime**" or "**economic offences**".

Conventional crimes like rape, murder, thefts and burglaries, on which the police/investigating agencies and forensic professionals spend most of their time, will pale into insignificance, both on account of value and importance. One scam can result in the loss of millions of Rupees, amounting to more than the combined value of all the stolen property throughout the country. White-collar and corporate crimes are special challenges to the law enforcement agencies in general and forensic document scientists in particular. The forensic scientists, who are working at the sharp edge of the business, know that it is rather an undiscovered domain of crime.

The society has now leaped into the information age, which has radically changed the way in which white-collar crimes are being committed in view of easy availability of digital tools and

image processing gadgets and application software on one side and use of net-banking. Now the traces of evidences of the crime exist in both world- conventional paper based documents and in digital media. This has increased the intricacy of the white collar crimes manifold both for investigation and modalities of their scientific examination. This is a paradigm shift in the nature, pattern and basic definition of white collar crimes due to the conglomeration of conventional and digital world in the perpetration of white collar crimes. The sophisticated nature of such emerging white collar crime armed with digital tools& tricks and the fact that the offenders can usually afford best of the defence lawyers, demands a highly professional expertise, on the part of the police/ Investigation and the forensic scientists.

New Problems

Forensic Science in general and forensic Document examination and Computer/ Cybercrime forensics in particular today are going to be flagship towards the detection and investigation hence immensely assisting the administration of justice delivery system. Law has influenced the science to its growth and effectiveness and forensic science has also influenced the law both substantially and procedurally In past, right from the admissibility of opinion of experts on typewriting in the courts of law as per the verdict of Hon'ble Supreme Court of India till today's IT act and enactment of various Cybercrime laws and now commencement of thinking on the ways and means of laws for the Artificial Intelligence / Machine language driven objects are excellent examples of progressive and vibrating democratic society. New concepts like digitally or computer generated documents, transposition forgery, cloud computing, digital cloning, information highways, network forensics,

mobile forensics, SIM card forensics, etc. has emerged in today's hi-tech society for which a modalities are available which were not known a few years ago. Technological advances in the microchip technology, embedded technology, fuzzy logic, artificial Intelligence/machine language, ever expanding mobile technology, cloud computing concept and robotics, etc. on the one hand and criminalistics and other engineering areas are overwhelming on the other and have revolutionised our work. Such developments have created new problems in terms of hi-tech crimes and pressing demands to address such problems for law enforcing agencies, forensic Scientists and legal profession & courts to understand, utilize and adopt these technological capabilities for the administration of justice both civil and criminal.

With the increase in literacy, unemployment, globalisation and liberalisation of economic activities as well as the technological advancements, the quality, quantity, nature, modality and intricacy of problems of Forensic Documents and Cybercrime have increased manifold. There are many new problems today which were not experienced in the past by document and cybercrime experts such as-analog and digital reproduction copies, counterfeiting of credit cards and other access products, travel documents and related crimes, cryptographic and magic pen inks, colour photocopies, printing/ reproduction devices and inks/toners, MICR, high value security printing, travel and identity documents, data retrieval from damaged and spoiled or broken storage media and broken/torn SIM card, net based frauds and ….etc.

New Machines & Methods

Forensic Document Examination has made tremendous progress by the development of new techniques and methods, some of which are invented by Document Examiners while other

are adaptation of advances made in the field of science. In consonance with the scientific advancements available to everyone including the cheats, it becomes essential for the Document Experts to foresee and forecast innovative crime and to well equip themselves. Today, forensic document specialists have an array of methods and instruments at their disposal to cope with the multiplicity of white collar crimes viz. Spectral Comparators, Hyper-spectral Imaging, Comparison Microscope, Electrostatic detection techniques for decipherment of indented and secret writings, digital reproduction unit with image authentication camera, Nano-spec, UV / IR Microscopes, SEM, narrow band filters, High resolution & magnification zoom stereo Microscopes interfaced with software for dimensional measurements of graphic features, Twin Video Comparison Microscope, IPI & ICPO decipherments, anti-stokes feature finders in travel documents, etc.

In recent years, many sophisticated methods and tools such as visible light spectroscopy, non-destructive spectro-photometry and fibre optics, Electrophoresis, HPLC, HPTLC, LASER, Holography, Scanning Electron Microscopy, Kromekote lifting, Phosphorescence Marking, FTIR, ATR-FTIR, DRIFTS, DAC-FTIR, Beta-Radiography, IR Microscopy, erasure reconstruction and dating, hyper-spectral Comparison of inks, side by side comparison by spectral Comparators, chromaticity based reflectance spectra studies of ink layers, Handwriting pressure meter, computer programs / software, neutron activation techniques, X-Ray diffraction techniques etc. for the examination of conventional forensic document related problems have been introduced. The examination of counterfeit/spurious credit cards or access products involves various techniques ranging from manufacturer of plastic(polyvinyl substrate is common) to the technology of embossing and imprinting of logo and other

surface features over it. This would require IR Spectrometry, Pyrolysis GC, Thermal analytical technique, NMR technique, Mass Spectrometry and HPTLC during examination of its various constituents.

Computer Technology- A Tool for Handwriting Examination?

Computer based examination as a complementary or supplementary aid to the conventional method(s) has been tried in forensic science and some success has been achieved in the field of finger prints and other disciplines. Research is seriously being pursued for Computer based forensic examination of the handwriting. An eminent Scientist of Indian Origin Dr Sagur Srihari based at USA, working on Neural Network, Pattern recognition and image analysis /processing at centre of excellence for document Analysis and recognition (CEDAR) has come up with a proto-type of the software **(Automatic Handwriting examination system - Cedar Fox)** for examination of Handwriting. The project was financed by US department of Justice and the trial of the software is being done at FBI laboratory. Recently, we have come across a book mentioning the utility of the system, the book says:" *One of the most convincing studies supporting the scientific nature of the forensic document examination is the work on handwriting identification at the State university of the New York's center of excellence for document Analysis and recognition (CEDAR). Funded by the national institute of Justice, the CEDAR computer software program is able to recognize certain feature of the handwriting and provide possible matches from the handwriting database. Similar to the automated Finger print identification system for latent finger prints identification, Cedar assists document examiners but does not replace them. The cedar program proved that there were unique identifiable*

features to handwriting that can be objectively demonstrated. The result of these empirical studies was the general acceptance of forensic document examination as a scientific discipline in most courts". This is very encouraging and thrilling development but the feedback of US based Document experts is that 'the prototype system is too slow and yet need perfection to reasonable limit of probability of certainty of decision'. I go one step further raising inherent question- Can there be a numerical equivalent to the evidence in questioned signature/ writing area? The answer to this nascent question is probably –yes, and needs to be addressed through basic research.

Fake/Counterfeit Security Documents and Bank Notes: Past & Present

Counterfeiting of Bank notes and security documents as well as travel documents is a global menace and needs more objective & dedicated approach to cope. Counterfeiting of currency notes or legal tenders is prevalent ever since its inception by the civilized society. The volume of about 200-300 billion dollars business of counterfeiting globally inflicts governments, loss of billion dollars which speaks about the magnitude and gravity of the situation. Counterfeiting is an offence never committed by accident or by ignorance, or in the heat of passion, nor in the extreme of poverty. Its a crime expertly designed by one who possesses technical skill and lays out substantial sums for equipment. People take currency note on "face value" and because of this, many "unacceptable" notes come into public circulation affecting the psyche and confidence of the people about their own currency.

Counterfeit/fake Identity cards for press, students, airline crews, driving licenses, university degree and diplomas, etc. reasonably authentic in

appearance, are sold openly in the markets of the neighboring countries especially in the close vicinity of tourist spots of South East Asian countries. The business of fakes is so open and brisk that it has taken shape of cottage industry offering a huge variety of fake identity cards and other documents. This situation appears alarming and a security risk to the nations, strategic installations and economic assets and trade especially in this region of the world which is a hotbed of the terrorist organizations, drug lords and human trafficking. Street of Khao San Road in Bangkok, Thailand, etc. is an excellent example of this. The availability of a wide range of fakes at tourist places in this area includes paper and plastic ID cards for press, students, cabin crews of major airlines, Interpol, the US Federal Bureau of Investigation and Drug Enforcement Administration, as well as citizenship and driving licenses. It is said that there are also diplomas and certificates identifying the bearer as graduating from any of a number of prestigious universities in the world.

In past, after mid-nineties, when counterfeiting of Indian currency notes, especially of higher denomination took a dangerous proposition in the form of an undeclared and clandestine "economic war", serious attention was paid towards this menace, leading to rapid changes in design as well as incorporation of new enhanced security features along with international deliberations and agreements/pacts. The process of planning for further deterrent and cost-intensive changes in design with upgraded anti-counterfeit features is still under consideration and is now a continuous process. INTERPOL had recommended changes in the design and pattern of bank notes after every 5-10 years along with publicity in the society regarding such anti-counterfeit measures. Research over the years on counterfeit currency, which is a global phenomenon, has revealed several key features attributed to the counterfeit industry.

- The organized activity of local criminal gangs infected youths, majority of them educated, with the **"get rich quick syndrome"**. These groups printed counterfeit notes using easily available digital image acquisition and reproduction technology such as computers, high resolution scanners and printers, color photocopier, digital cameras etc.

- Organized efforts of external agencies to pump in high quality counterfeit currency. High quality and incorporation of some key security features of genuine notes in counterfeit notes indicate that these fakes are products of a regular printing press process involving skilled and trained manpower outside the boundaries of country.

When magnitude of this menace took monstrous shape and proportion as well as endangered our economy and socio –economic fabric, a historical, brave & bold step was taken by the Government of India on 8th November 2016 to demonetize the high value denomination bank notes of Rs. 500 and 1000 to break the backbone of the counterfeiters having collateral motives against the Nation on the one hand and black money racketeers on the other to achieve the noble target of bringing the 'informal economy' or 'grey economy' into main stream 'formal economy' and to curve the anti-national activities.

Achievements and failures of past, effective solutions, appropriate technology use and new concepts are vital to meet the future challenges of faking & counterfeiting of various important documents such as- travel documents, identity documents, access products, security documents & bank notes and therefore, amalgamation of these ingredients generate valuable synergies for secure, high quality printing and production of such secured documents in the new millennium. Achievements from effective implementation of

tried and tested technology, learning from past failures, and new concepts are going to play a vital role in coping with future challenges of counterfeiting/faking.

Therefore, as a proactive measure, it is also imperative that public/ people should know the details of their instrument of payments, security documents and identity documents at least up to the minimum preventive level. This will make them somehow confident about the technical know-how and expertise both in prevention and detection and in turn help with the stability of the larger economy by recruiting/involving the citizens in building this internal defense against malicious efforts. The motive should be – *"Success lies in the details as magnification is the basis of verification and verification is the basis of acceptance"*, therefore share some details and let people know at least up to a detectable and preventive level for defeating the ill motives of the fraudster/counterfeiters.

To achieve this goal, a concerted effort with the working theme of *"prevention is better than cure"* should be implemented. A comprehensive core group formation is imperative & require comprising people from various sectors including forensic document science for planning. Current series of Bank Notes throughout the globe have state of the art security printing, but the security features, which are presumed effective today, may be obsolete tomorrow as *'the technology is revolutionary in execution but evolutionary in nature'*.

Technology is inevitable, hence, either go for it or perish. Innovation of effective technology for the security of money, merchant cards, access products, identity documents, travel and other security documents needs investment of huge magnitude. Even the high cost of new technology won't keep cheats away from printing fakes; even then we need to be always ahead of counterfeiters since currency and security

documents of a country symbolizes nation's soul, pride and economic might of the country on the one hand whereas the access products, identity documents, etc. are pride property of citizens. Some of the remedies may be:

- Increased collaboration and Information sharing between agencies (locally and internationally).

- Equipment: Till now most forensic document examiners use Ultra violet lights for detecting light sensitive security features for detailed physical inspection/ examination. Spectral Comparators as well hyper-spectral facilities for forensic inspection of security documents having anti-counterfeit features along with full database library are used widely. With investment in such technology we can be on par with the world in detecting malicious documents and fake notes

- Widely acceptable stringent laws. Trademark laws and laws related to such crimes need to be reviewed and tightened in perspective of global security, peace and order.

- Global consensus based on security vision and wisdom.

- Machine readable passport and other security/identity authentication and data matching.

- Language Bank, a pool of interpreters on call.

- Continuous Training of enforcement officials.

- Training & Sensitization for the general public.

- Immediate crackdown needed on fake markets, wherever this type of illegal or sponsored free fake market trade is going on unabated illegally.

- Insertion of more and more inevitable electronically verifiable patterns and codes or anti fake/counterfeit features for easy detection and subsequently rejection of the fake/counterfeit through unavoidable electronic verification system.

Digitally Manipulated/Computer/ Generated Documents - *Unwanted Progenies of Modern Technology*

The use of mind set and tricks of conventional forgery coupled with the application of digital image acquisition, processing and reproduction technology has created a paradigm shift in the nature, intricacy and impact in the field of Forensic document Science resulting into various new challenges and dangers. Use of dry transfer lettering, scotch tape and gelatine transfer techniques have been reported in facilitating the transfer or transposition of the genuine signatures to another to create spurious documents. The popularity and easy availability of high quality plain paper copiers and digital technology have added new dimensions to the nature and quality of white collar crimes both in case of their perpetration and detection. With the advancements in digital image acquisition, processing and reproduction technologies, the fabrication of documents has become easier and closer to perfection. This has led to the uncovering of new dimensions and intricacies of white-collar crimes on the one hand and the facing of new challenges of their detection on the other. Extensive examination of such questioned document and its original source document in a forensically sound manner in light of the principle of comparison and individuality revealed that such type of digitally manipulated and machine generated questioned documents are spurious and generated/created with a motive of deceit and hence are 'unwanted progeny' of original source document both in nature and origin perpetrated through modern technology.

Computer/Cyber Crimes - Frauds of 21ˢᵗ Century

Today, computers have proliferated and penetrated everywhere- banks, industry, commerce, railways, police, military, scientific research, health and other governmental agencies in a big way. Under these conditions, damage or intrusion with motive of deceit to any of the computerized or digital infrastructure of an organization or corporate establishment may lead to heavy losses in terms of information, finances and its reputation. *"Any illegal or unauthorized activity involving computers can be termed as computer crime, whether it is against an individual or an organization".* It can even be against the nation, endangering or threatening to endanger its integrity and security. The Computer Crimes can generally be classified as **physical** crime, **data related** crime and **software related** crime. The Organisation of economic cooperation and development (OECD) has defined Computers crimes as "Computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to automatic processing and transmission of data"

The INTERPOL classifies the digital crime as computer crime; computer related crime and network crime. The new types of white-collar digital crimes are either "computer-based" or "computer network based". In case of computer crime, the victim is a computer. Such crimes include piracy, data theft, data manipulation and even time thefts by way of computer break-ins. In computer related crime, the computer is a tool to perpetrate the crime, which mainly relates to bank frauds. In case of computer network crime, the computer is witness to the crime. Investigation of crime and forensic analysis of such crimes is an extremely complicated affair, if the crime is committed by unauthorized access to the computer network, since the number of places where the evidence could be searched for is unlimited. For example when a cheque

is forged, that would be the only disputed instrument or crime exhibit. On the other hand, in computer related white-collar crimes, the evidence could be found in different formats.

In the information age, significant opportunities exist for those who are best at utilizing both, the **technology** and the **information**. Who will do a better job, the criminals or those seeking to detect or investigate the crime? This would be decided by the application of their relative ingenuity in this game of wits. The whole world has become the *operational canvas* for the cyber criminals, since they are not constrained by the national boundaries. In absence of international cooperation to combat transnational crimes, there are many safe havens for the criminals to take shelter. It has become easy for the criminals to operate globally and go absolutely scot-free, while the law enforcement agencies grapple with the maze of procedural tangles involved in investigation and prosecution. The nature of evidence is such that it can be destroyed easily and to recover and prove the authenticity of the evidence is a difficult task. In the process of searching and seizing the evidence in digital format, considerable care should be taken to avoid contamination of its evidential value, for which the investigators need to be specially trained& integrity of the evidence needs to be proved through hash value.Different types of Cyber Crimes are-Hacking, Denial of service attack, Virus dissemination, Software Piracy, Pornography, IRC Crimes, Credit Card Fraud, NET Extortion, ,Phishing, Spoofing, Cyber Stalking, Cyber Defamation, Threatening, Salami attacks, etc.

Due to ever increasing power of information technology and computers, we are witnessing an unprecedented spurt in a wide variety of white-collar digital crimes, which are perpetrated through ingenious means. Different types of cybercrimes have emerged due to the explosive growth of the Internet, e-commerce, D-commerce

and personal computing. Internet crime might be interpreted in a number of ways. One is to limit it to the new forms of crime that can be performed on the Internet. Another is to apply it not only to the new forms of crime, but also to variants of existing crimes that are adapted into the Internet context. The emerging crime trends in the digital world are - *Crime-as-a-Service, Ransom-ware, Criminal use of data, Payment fraud, Online child sexual abuse, Abuse of the Darknet, Social engineering, Virtual crypto currencies-bit coins, Steganography, etc*. In every crime in general and cybercrimes in particular, the identification of the fact that the crime has been perpetrated is not difficult, but the challenge is to connect the crime with the criminal and produce sufficient evidence to convince the judiciary so that the laws are enforced to convict the guilty as the *'laws are flaws, jurisdictions are fictions and reality is virtuality in cyber world of netizens*.

Computer/Cyber Forensics

It is the process of methodically examining the computer media for digital evidence, its recovery, reconstruction and presentation in the court of law while maintaining and establishing the Integrity and chain of Custody. Though it appears to be similar to software skills of data recovery and its presentation, it is a step complicated in terms of handling as the sensitiveness of integrity of data to be maintained and never it to be handled directly.

Computer Forensics/Cybercrime Forensics, a new branch of forensic science, is the scientific collection; examination, analysis and presentation of information held on or retrieved from computer storage media in such a way that it can be used as potential legal evidence. The evidence sought might be from a wide range of computer crime or misuse, including violations of intellectual property rights and fraud. To discover data that resides in a computer system,

or recover deleted, encrypted or damaged file information, the computer forensic scientist can draw on an array of methods. The information generated during the course of the examination would be of help in the investigation of crime and deposition in the courts of law. The expectations from computer forensics are divergent from the more traditional forensic science branches like forensic physics or forensic toxicology etc. Application of **computer forensics** becomes essential to provide scientific aids to cybercrime investigation, since the new age criminals are committing traditional crimes using non-traditional methods. The investigation of such crime needs the investigator to be equipped with the latest technical tools that are available with the computer security people and fine tune them to their needs.

The Computer/Cyber Forensics utilizes Hardware and Software tools including High-end Forensic Work Stations, Hardware based Forensic Imaging Devices, ample number of Integrated Forensic Analysis Kits, Various-Mail Database Analysis Facility, Vivid Mobile Phone Forensic tools to conduct Logical, File System, Physical Level Analysis, Password Bypassing/cracking facility, Decryption of Encrypted data facility, RAM Analysis facility, Server Data Analysis facility, Malware Analysis facilities. Plenty of equipments/tools with generic names are available in the field of cyber forensic such as-X-Ways Forensics, SANS Investigative Forensics Toolkit – SIFT, Volatility, Windows SCOPE, Oxygen Forensic Suite, XRY, Cellebrite UFED, EnCase/ FTK/Belkasoft Evidence Center, etc.

The field of Computer Forensics is also under going huge changes due to rapid technological innovations and advancements in its related areas, therefore, various sub-sections of cyber forensics are emerging to cope with the emerging trends and changing notions of the cyber-crime world –network forensics, mobile

forensics, disc and storage media forensics, chip/SIM card forensics, cloud computing, software forensics ,etc. to cope with the digital crime related with embedded system, open systems and communication systems. Forensic investigation of digital evidence can be divided into three main areas, which are embedded system, open systems and communication systems. Therefore, due to varied nature, mode and media of perpetration of digital crime, dimension and impact, a well-equipped digital or cyber forensic laboratory may look for sub-divisions such as- Physical Media Examination unit, Storage Media Examination unit, Mobile device Forensics, Embedded Forensics unit, Malware Forensics unit, Source code Forensics unit, Crypto Analysis Unit, Information System Auditing Unit, Database Forensics Unit, Cloud Forensic Unit (Cloud Forensics, a new term, is cross-discipline between Cloud Computing and Digital Forensics. Cloud Forensics is actually an application within Digital Forensics which oversees the crime committed over the cloud and investigates on it), IoT (Internet of Things) Forensic Unit within the lab for smooth and proper scientific examination of exhibits conforming to the SOP's of the laboratory.

In information technology, modernization and obsolescence is the norm and not an exception. The reason for the difference in perception is the very high rate at which the computer technology and configuration of the tools both in hardware and software aspect changes. New forms and techniques of data storage are continuously being developed. Similar changes have also taken place in computer applications, which has affected the type of information being stored in computers. The frequent changes in technology and protocols provide opportunities to both hi-tech criminals as well as to forensic investigators.

Therefore, computer forensic methods would not have time to establish themselves like the traditional forensic methods.

Conclusion

The scope, limitations and uncertainties of the final product of various modes of trickery, forgery, reproduction and image acquisition technologies, storage/file formats, digital tools and application software as well as digital processes have become professional hazards, thereby affecting the quality and nature of findings of forensic document and cyber experts. It is therefore imperative for forensic experts of both the domains, who convert uncertainties into certainty, possibility into confirmation and subjective into objective, to address these new forms of evidence by updating their knowledge and skills as well as keeping abreast of the technology and scientific advancement in the field, otherwise society will be deprived of truth and facts, which are of great evidentiary value. Also, the professional acumen, experience and competence of the examiners have a vital role to play in bringing out the truth through innovative skills, continuous thought process and objective interpretation of data related with all those forensic document (hard & soft) problems which are a direct outgrowth of modern technological advancements and innovations. The serious threats of digitized document and digital document frauds, taking the journey of frauds from 'cursive to cursor', to the economy and society are inevitable and growing due to advancement in the field of writing instruments, writing media, digital acquisition, reproduction and core digital technology, hence our forensic readiness and deterrent forensic preparedness are vital and crucial.

References

1. Casey Eoghan, Digital evidence and Computer Crime, Academic Press, London/California, 2000.

2. Comer J Michael, Corporate Frauds, Third edition, Gower Publishing Limited, Gower House, England, 1998

3. Conway, J.V.P. (1959). Evidential Documents. Illinois: Charles C Thomas.

4. Donald H. Sanders, Computers today, Author,. Edition, 3, illustrated. Publisher, McGraw-Hill, 1983.

5. Ellen, D. (2005). Scientific Examination of Documents: Methods and Techniques, Third Edition. Boca Raton: CRC Press.

6. Harrison, W.R. (1958). Suspect Documents: Their Scientific Examination. New York: Praeger.

7. Hilton, O. (1982). Scientific Examination of Questioned Documents. New York: Elsevier Science Publishing Co.

8. Huber R.A. & Headrick A.M. (1999). Handwriting Identification: Facts and Fundamentals. Boca Raton: CRC Press.

9. Jerry Iannacci and Ron Morris; Access Device Fraud and Related Financial Crimes; CRC press, 2000; London, New York, Washington DC.

10. JOSHI Mahesh Chandra, CHOUDHARY Rajat and JASUJA Om Prakash, Transposition Forgery Through Image Processing. A Fresh Approach towards its Examination And Detection Problems of Forensic Sciences 2009, vol. LXXIX, 338–347, Poland/UK.

11. JOSHI Mahesh Chandra, Rajender Singh RANA, Examination of signatures that have been digitally transposed and printed and subsequently inked −a case study, Problems of Forensic Sciences 2016, vol. 107, 582–590, Poland/UK.

12. JOSHI Mahesh Chandra, Abhimanyu Kumar, Sushma Thakur; Examination of a digitally manipulated – machine generated document. A case study elucidating the issue of such unwanted progenies of modern technology, Problems of Forensic Sciences 2011, vol. LXXXVI, 162–173Poland/UK.

13. Joshi M C, Fake (Counterfeit) Documents Industry in India's Neighbourhood, CBI Bulletin,Vol. XXIII, Nos. 4-6, 2016 Page31-36.

14. Kelly Jan Seaman and Lindblom S. Brian Scientific Examination of Questioned Documents, Second edition 2006.

15. Koppenhaver, K. (2007) Forensic Document Examination, Principles and Practice Humana Press.

16. Levinson, J. (2001). Questioned Documents: A Lawyer's Handbook. San Diego: Academic Press.

17. Morris, R. (2000). Forensic Handwriting Identification: Fundamental Concepts and Principles. Academic Press.

18. Suresh K Basandra, Computer Today, Galgotia Publications Pvt Ltd,1995

19. Osborn, A.S. (1929). Questioned Documents, 2nd ed. Albany, New York: Boyd Printing Company. Reprinted, Chicago: Nelson-Hall Co.

Analysis of Prisoners Conditions:
A Case Study on Modern Central Jail Nahan

Somesh Goyal IPS*1

Amit Mandal2

Dr. Chhavi Kabra3

Rohit Malpani IPS4

Abstract:

The research explains about the living condition of inmates in Model Central Jail Nahan along with analysis of barrack infrastructure, food quality and sanitation. The study also aims at explaining various facilities provided to the prisoners with special focus on wage earning avenues and educational programmes. It provides an insight into three major crimes encountered during survey i.e. crime related to murder, crime against women and crime under NDPS Act along with the strategies which can be adopted to curb them. It presents the detailed analysis of the problems faced while sending out the prisoners for medical tests and appearance in the courts with an approach to making the process more convenient. Issues in provision of legal aid to the prisoners is another area this study focuses upon. It concludes with showing trends of crime versus various attributes of a prisoner which must be taken care of to reduce the number of cases and also tries to devolve upon possible solutions to the above mentioned issues with regard to the prisoners in jails.

1.   Introduction

To provide safe, secure, caring and humane environment inside the prison is the mission of the Directorate of Prisons and Correctional Services Himachal Pradesh. This environment can be created inside the jail only by providing the necessary infrastructure, adequate services in terms of food, medical aid, sanitation facilities, legal aid etc. CAG report on social, general and economic sectors for March 31, 2016 pointed out that the state Prison Department had not offered education and rehabilitation facilities for the bulk of the prisoners where only 6% prisoners out of 1116 in the test checked jails had obtained educational qualification while lodged in the jail during 2013-16[1]. This case study attempts to bring forth the existing situation inside the Modern Central Jail Nahan on the above aspects.

Model Central Jail Nahan is located in Sirmaur district of Himachal Pradesh. Currently there are 14 jails in Himachal Pradesh with two Model Central Jails, two District Jail, one Open Air Jail,

Author Intro:

*1   Director General of Prisons, Shimla, Himachal Pradesh

2   Junior Undergraduate, Metallurgical and Materials Science Department, Indian Institute of Technology, Roorkee, Uttarakhand

3   Dr. Chhavi Kabra, MBBS MD, Department of Biochemistry, Nahan Medical College, District Sirmour at Nahan, Himachal Pradesh

4   Superintendent of Police, District Sirmaur at Nahan, Himachal Pradesh

one Borstal Jail and eight Sub Jails[2].Department of Prisons is headed by Director General of Prisons who exercises general control and superintendence over all the prisons in the state.

Himachal Pradesh accounts for 0.43% of total 419623 prisoners in India with average occupancy rate of 110.7%[3]. Occupancy rate for each type of Jail in Himachal Pradesh is shown below with comparison of average rate of all the Indian state.
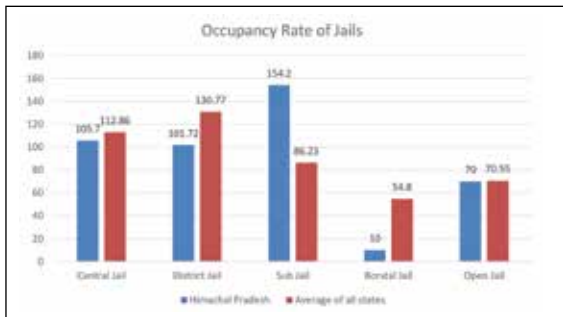

Figure 1: Occupancy Rate of Jails
Data Source: Prison Statistics of India 2015 (NCRB)

2.   Methodology

Data of 200 inmates of Model Central Jail Nahan was collected during the survey. Based on initial study a test survey was conducted with ten prisoners and based on their response further relevant changes were made to the finalized questions. Inmates were interviewed individually and the responses were collected through Google Forms filled in by the surveyor.

Data that was collected during survey is presented below:

1.   Basic Information : Name, Type of Inmate, Gender, Marital Status, Type of Locality (Rural/Urban)

2.   Crime profile : Crime, Term of Sentence, Date since serving, Application status for bail/parole

3.   Additional Information : Educational Qualification, Earning status, Number of family members

4.   Life inside Prison: Rating of barrack, food, sanitation out of 10, Wage earning and educational program, Preference to learn new skill, Wish to continue learned skill, addiction to smoking and alcohol, access to mobile phones, drugs or alcohol inside jail and use of Jail *Vaarta* facility

5.   Medical Aid

   a.   Diseases before and after coming to prison along with the type

   b.   Status of timely medical test and consultation

   c.   Rating of district police guards attitude while escorting (out of 10)

6.   Legal Aid: Awareness of Fundamental Rights, Legal literacy classes, amount spent in availing legal aid

The conditions inside Model Central Jail Nahan were accessed in accordance with the Rights of Prisoners as suggested by All India Committee on Jail Reforms 1980-83[4].

Python and Excel tools were used for data analysis while data was filtered with the help of SQL.

Inputs from Superintendent of Jail, Model Central Jail Nahan and interaction with jail warden, police constables were also included in the research.

4.   Living Condition of Prisoners

To determine the conditions in which the inmates of Model Central Jail Nahan live, questions relating to barrack infrastructure, food quality, sanitation and communication facilities were included.

4.1   Barrack Infrastructure

At present there are four blocks in Model Central Jail Nahan i.e. Block A, B, C and D. Number of inmates living per barrack varies as per the size. Each barrack has well maintained fans

and light in adequate quantities. Inmates are responsible for the cleaning of the barrack which they do by turns. Disinfectant and phenyl is provided once in a week for the cleaning. The problem of overcrowding is not very serious as compared to other central jails[5]. *"Sometimes when a new prisoner comes there is a problem of accommodation and bedding facilities but is sorted after few days"* comments one of the inmates during the survey. Each inmate has his own set of bedding which is being provided by the Jail authorities. Sufficient quantities of blankets are provided during winter season. Every inmate has been given his own set of utensils and bucket. However, problem which prisoners complained during the study was there is no water in taps near the barrack and they have to fetch it from the common source near blocks.

Based on the common parameters prisoners were asked to rate the conditions of the barrack out of 10 and the results are provided below.
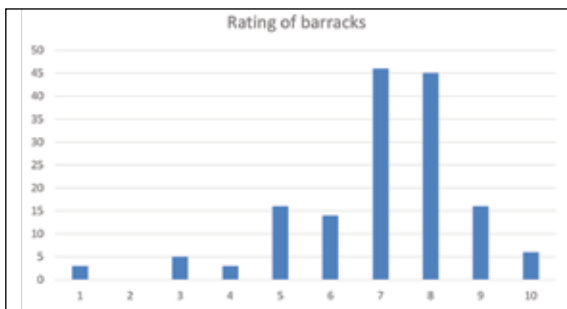
Figure 2. Rating of barracks
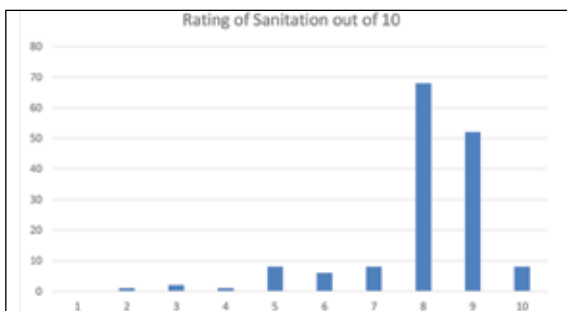
Figure 3. Rating of Sanitation out of 10

Thus the results obtained point to the fact that prisoners are satisfied with the conditions of barracks and jail sanitation. This result also contradicts the general perception about living environment of prisoners where barracks without fresh air stink due to sweating, algae floats in water tanks and no regular service of sewerage and drainage.[4]

4.2   Food

Prisoners are given meals keeping in mind the minimum amount of calories required per day which is 2320-2730 kcal per day for male while 1900-2830 kcal per day for females as prescribed by Model Prison Manual drafted by the Ministry of Home Affairs, New Delhi[4].

There is a canteen facility for the prisoners which has various types of basic products including milk, cookies, pizza. etc.

Inmates were asked to rate the quality of food out of 10 and the results obtained are:
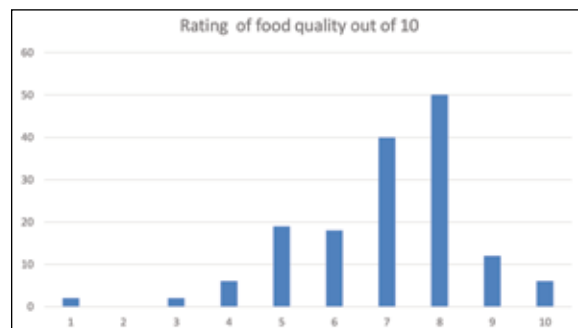
Figure 4. Rating of food quality out of 10

4.3   Communication

Prisoners can communicate to their friends and family through phone call, Video call (Jail *Vaarta* facility) and in person meetings in jail. Phone call is allowed once in a week for 10 minutes. Inmates have to register numbers with the jail authorities to which they wish to make a call.

100% of the prisoners interviewed are regularly using phone call facility. The issue which arises is the number of telephone assigned is one for more than 400 prisoners so there is a shortage of telephone lines.

Jail *Vaarta* is an excellent facility provided by the jail authority to communicate with family via video call. During the survey prisoners were asked about the usage of Jail *Vaarta* facility and the results are:

Figure 5: Use of Jail Vaarta facility

Despite being such a wonderful initiative only 9.6% of the inmates have used Jail *Vaarta*. It was found that this was due to unawareness of the existence of facility and no proper assistance from Jail authorities.

4.3   Wage Earning Programmes for Prisoners

Model Central Jail Nahan provides number of avenues for wage earning which are Carpentry Workshop, Tailoring, Weaving, Bakery, Horticulture, Cutting and other allied workshops. There is an excellent provision of bakery which makes cookies, pizza, bread and which are being marketed and sold in Nahan from door to door under the brand name '*kaara*' (Adopted from kaaravas meaning jail).

Majority of the prisoners enrolled in programs are convicts. There is a provision for each prisoner to serve in the *langar* (kitchen) once every six months and she/he is paid INR 5000 for the same. Under the motto **'Har Haath Ko Kaam'** (initiative started by the Director General of Prisons, H.P. and chosen for HP State Innovation Award Scheme for the year 2016-17) through which majority of the convicts have been enrolled in productive wage earning programmes. There is a very high increase in the wages paid over the last 5 years which is an indicator of increasing

involvement in the program. In 2015 wages paid to the inmates amounted to Rs4.85 lakhs which rose in FY 2016-17 to Rs 80 lakhs and in FY 2017-2018 to more than Rs1 Crore. The factory output also saw an increase from less than Rs. 25 lakhs in 2015 to Rs. 2.5 Cr in 2016-17 and Rs 3.28 Cr in 2017-18. This exponential growth could be possible due to team building, motivation, facilitation, infra creation and expansion, better marketing tools like flagship Pehal stores, two in Shimla, one each in Nahan and Dharamshala and online marketing portal www.kaarabazaar. in. Prison hospital blankets, hospital bedsheets, pillowcases, etc. are on Government E-Market (GeM) portal. A sum of Rs 70 lakh has been paid as wages to these prisoners in the past one year. Following results were obtained from the survey which shows that 58.12% convicts were enrolled in the wage earning programmes.

Figure 6 Enrolment in Wage Earning Programmes

In order to determine how useful this facility would be in rehabilitation of prisoners, they were asked about whether they would like to continue with the skills they have learned during their prison tenure or would opt for something else. Responses recorded are as follow:
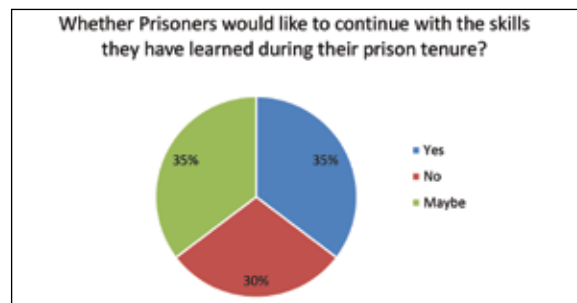
Figure 7. whether Prisoners would like to continue with the skills they have learned during their prison tenure?

35.3% of the enrolled prisoners wished to continue the skills they had learnt while majority of the inmates gave negative response or either they were confused. This shows that wage earning programmes although beneficial inside the prisons could be more helpful in rehabilitating the prisoners with little modifications and appeal to more number of prisoners. Although most of the prisoners said they would like to continue their previous jobs, many of them proposed to learn skills of electrician, plumber, computer skills, setting up business, painters, etc. Since majority of the inmates are from rural areas, teaching them above traits could be more beneficial under the brand name '*Kaara*'.

4.4 Educational Programmes

Prisoners in Model Central Jail Nahan can continue their studies and appear for board exams as well as complete their graduation from various fields from Indira Gandhi National Open University (IGNOU), New Delhi.
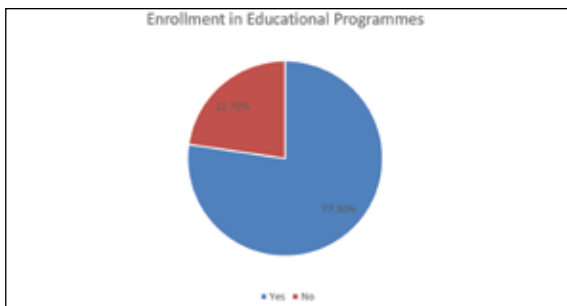
Figure 8. Enrollment in Educational Programmes

22.7% of the surveyed inmates were continuing their studies from IGNOU. More number of inmates must be motivated to enrol in education program as this increases their chance of landing up with a better job and their stay in prisons could be spent constructively.

4.5 Socio Economic Condition of Prisoners

Of the total 200 prisoners surveyed 93% were male inmates. Social life and economic conditions of the prisoners were studied with the help of questions based on monthly income,

place of residence, educational qualification and family background.
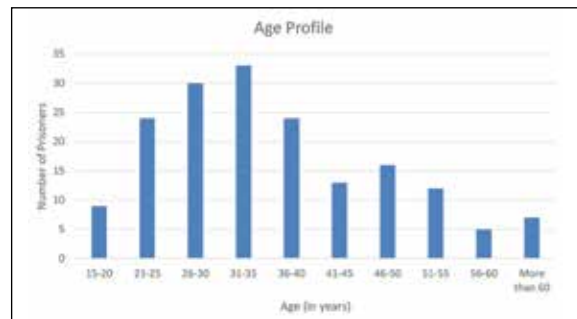
Figure 9: Age Group
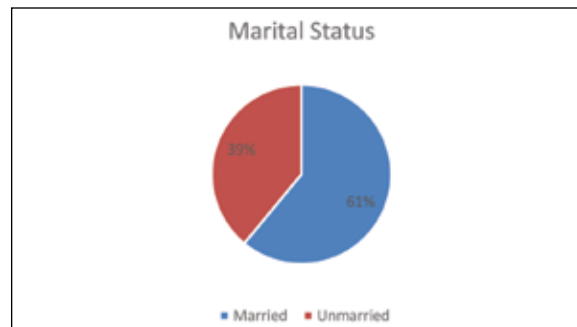
Figure 10. Marital Status
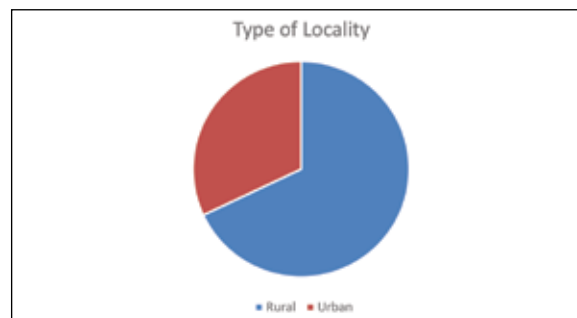
Figure 11. Type of Locality

Educational Background
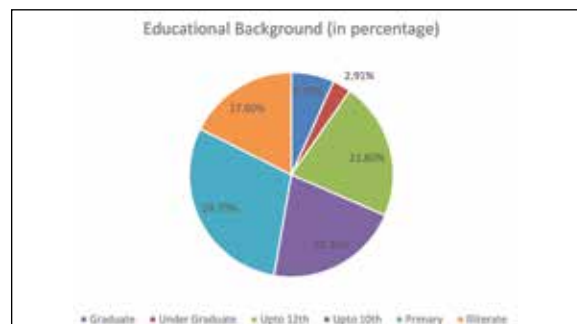
Figure 12: Educational Background (in percentage)

More than 50% of the inmates have highest level of qualification only upto 10th whereas 17.6% are illiterate. This proves the fact that level of education is a major factor beyond indulging in criminal activities.

Family Background

76% of the total prisoners surveyed lived in nuclear families whereas the number of family members per prisoner is represented graphically as below.

55% of the inmates have family members per household greater than average number of members per household in Himachal Pradesh[6].

Issue: Lack of family planning which in turn raises the burden on the earning member of family thereby compromising the quality of lifestyle and education which is a strong factor leading to criminal activities.

Monthly Income

Majority of the prisoners have monthly income below INR 10000 which is less than per capita income of Himachal Pradesh whereas 9% were unemployed[7].
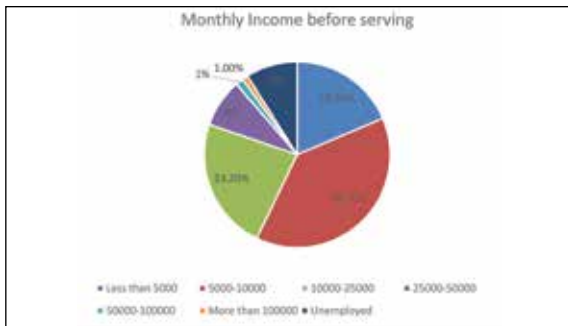
Figure 13: Monthly Income before serving

Of the total inmates surveyed 46.3% were the only earning member of the family, which puts a great burden on the family members at times when the earning member is serving in prison. Hence, cases of such undertrial prisoners who are the only earning member of their family must be taken up with priority for trials as well as giving special attention to their rehabilitation.

Addiction

Results for addiction of inmates to smoking and alcohol are presented below:-
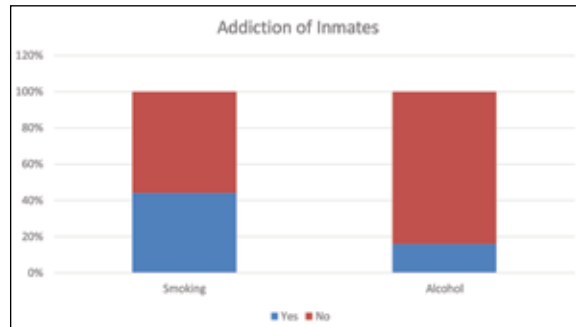
Figure 14. Addiction of Inmates

Bidi is available from the Jail canteen to the prisoners but there is no access to drugs and alcohol by any means inside the jail, confirmed 99% of the prisoners during the survey.

Frequency of de-addiction camps is very less and majority of the inmates claim there have been no such camps since they are serving.

4.6   Medical Aid

Disease profile for the surveyed inmates are shown below:
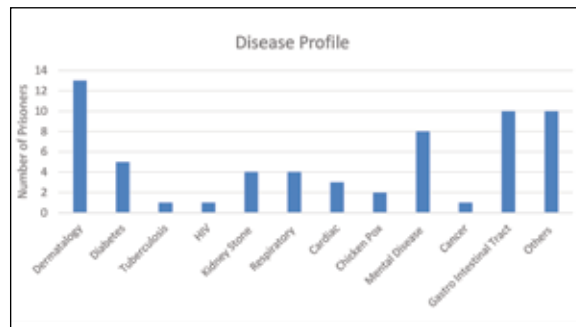
Figure 15. Disease Profile

Although it is mandatory to have a Chief Medical Officer for each prison but in Model Central Jail Nahan this post has been lying vacant for a long time. There is no regular doctor in the prison. There are frequent visit of doctors from the nearby hospital whom the inmates can consult. As there are quite a lot number of prisoners with diseases and thus it is not possible for the

visiting practitioner to check each and every patient. Thus most of the prisoners have to wait for a long time before their turn comes, often aggravating the condition.

There is a pharmacy in the prison which is equipped with adequate type and number of medicines. During the survey it has been observed that prisoners were not satisfied with services of pharmacy. One of the inmates recalled *"For every problem with which you approach the pharmacist he just gives you the painkiller"*. There have been instances where some inmates were even harassed by the pharmacist.

The major problem faced while providing the medical aid to the prisoners is when they are recommended by the doctors visiting the prison for medical tests in the hospital. This request of the prisoner is conveyed to the jail authorities which in turn forward the application to District police for providing guards to escort the inmates to and from hospital to jail.

Issue:

1.   Non availability of guards delays the test
2.   Behaviour of police guards with the inmates

Prisoners were asked to rate the behaviour of police guards escorting them out of 10 and results obtained are as follows:

Figure 16. Rating of District Police Behaviour

Most of the prisoners were uncomfortable with the attitude of the district police. It depended from personnel to personnel but very few rated nine or above nine.

Inmates added that police guards were always in a hurry and if there is a queue in hospital for the medical test, most of the time guards take another date from the hospital staff and return the prisoner to the jail without the test.

4.7   Legal Aid

There are regular legal aid classes conducted inside the prison. Four legal aid lawyers are associated with Model Central Jail Nahan who have weekly visits. Through this facility inmates can avail the free of cost facility of a lawyer. These lawyers also file application for *Jamatalashi*. For each case lawyers were being paid INR 500.

During the survey prisoners were asked about the awareness of their fundamental rights and the amount of money they have spent on availing legal aid services. The results were as follows:

Figure 17: Awareness of Fundamental Rights

Despite the regular visit of legal aid authorities only 31.2% of the prisoners were aware of their fundamental rights. Most of the inmates complained of the fact that representatives of legal aid generally pay no attention to the convicted prisoners and were more interested in the Under Trials.

Figure 18: Amount spent on Legal Aid

This result obtained revealed a very shocking fact that average spending of the surveyed inmate on legal aid was nearly INR 3,00,000. With 45% spending more than 1 lakh and around 10% above 10 lakh was an evidence of the fact that legal aid provisions provided to prisoners did not achieve its purpose. On the other hand this was trapping the poor inmates in a vicious debt cycle thereby aggravating their conditions to even worse.

Thus, special attention must be paid to the competency of lawyers provided through legal aid as most of the prisoners had problem with the capability of the government lawyers. Also those who were using the legal aid facilities complained of a communication gap with the lawyers. In some cases, the lawyers had not been responding for years. Some inmates brought up the fact that generally the lawyers who came for legal aid awareness were interested in under trials and hence convicted prisoners were not paid much attention.

4.8   Crime Profile

Of the survey carried out, two-thirds of the prisoners are convicted whereas undertrials form 31.8% , which is an exception to the report of Prison Statistics India released by National Crime Records Bureau (NCRB) which states *"Two-thirds of the prisoners in Indian Jails are under trials"*.
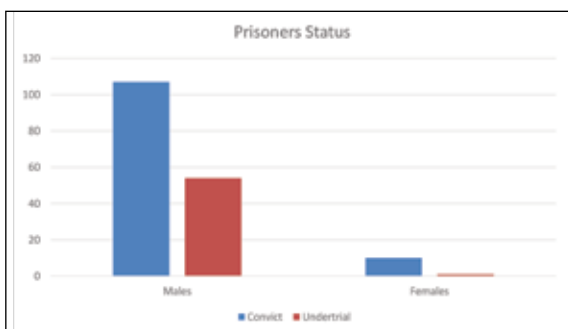
Figure 19

One of the major problems in Indian Prisons is the number of days an undertrial has to serve in a prison. There have been cases where an undertrial has served more than the sentence she/he would have served if convicted[8]. 47% of the under trials have been serving more than 1 year which is a sign of concern as these inmates create the problem of overcrowding and hence their cases must be tried at the earliest.

Figure 20

Only 18% of the inmates who are under trials have used Video Conferencing facility for courts trial. Given the conditions, it is necessary to use this facility to its full potential for speedy redressal of justice. Currently video conferencing facility is being used only for extension of judicial remand of the under trials which should be extended to the court trial of the criminal cases also of the under trial prisoners.

Of the total inmates surveyed their crime profile is as follows:
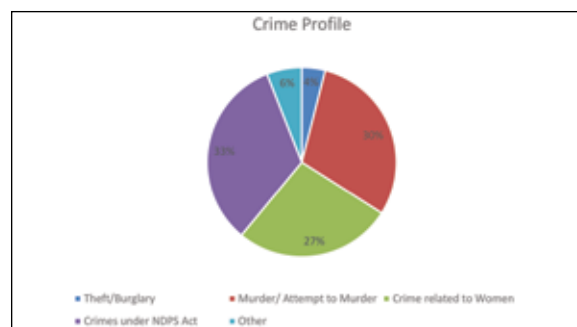
Figure 21

Majority of the prisoners were associated with crimes of Murder, related to women and under NDPS Act. Each of these is analysed below separately.

Crime Type: Murder, Attempt to Murder, Culpable Homicide

Total Number of Prisoners: 52

● Murder cases are concentrated in district areas which share border with other states

Figure 22:Heat Map of Murder Cases

● Age group 26-50 is responsible for the most number of cases

● 67% of the prisoners have studied only upto tenth class
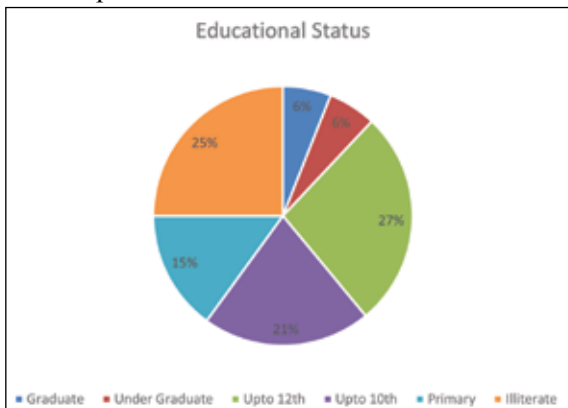
Figure 23

● 58% of the prisoners have monthly income below INR 10000 whereas 11% are unemployed. Cases are concentrated in the area with monthly income below INR 10000 (58%), which proves the fact that people in the lower income group are more probable to commit the crimes. Very

few cases have been encountered with monthly income well above INR 20000.

Figure 24

Crime Type: Rape, Molestation, Stalking and other crimes related to women

● Solan accounts for most number of cases followed by Kullu and Sirmaur
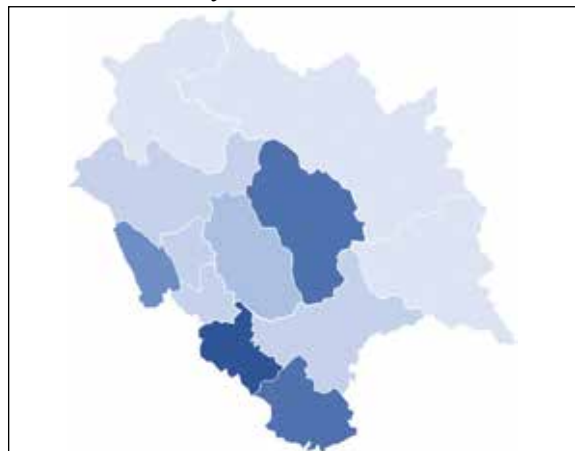
Figure 25:Heat map for Crime related to women

● 67% of the prisoners are educated upto primary school of which 23% are illiterate which shows a strong relation between education and commitment of crime

● Majority of the prisoners belong to the Age Group 17-40 years

● 64% of the crimes are concentrated in rural areas

Crime Type: Under NDPS Act

Observations

● Of the survey carried out the distribution of cases state wise are shown below where

particularly Kullu, Mandi and Una are major contributors to cases in Himachal Pradesh whereas in Punjab, Moga and Ludhiana are the hotspot of NDPS related crimes
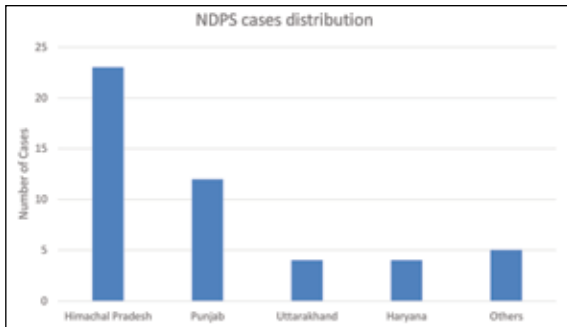
Figure 26

- 60% of the prisoners have monthly income below INR 10000 while 10% of inmates were found to be unemployed which shows this type of crime is prevalent among low income generating group.
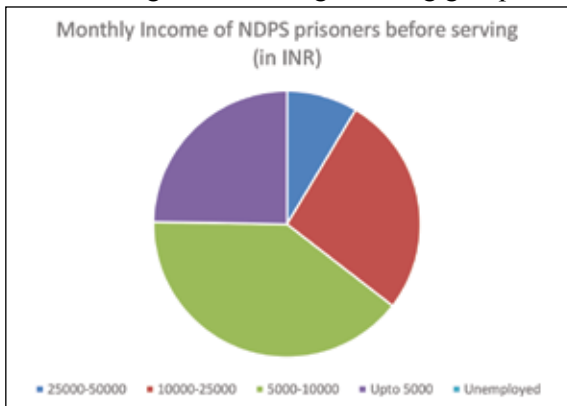
Figure 27

- Relation between income and number of family members shows that majority of the prisoners have family members in range 5-10 whereas monthly income is below INR 10000 which relates to the fact that there is a lack of concept of family planning. From the data obtained it was found that 13 prisoners live in a joint

family and 60% of inmates are the only earning members of the family, which puts a great burden on an individual.

Figure 28

5.   Trend between Crime and Prisoners attributes

- A plot between the level of education and number of prisoners was made, it was observed that crime committed by Under Graduates and above accounts only for 9.75% of the total crimes surveyed. Hence, higher is the level of education, lower is the probability of committing a crime. Trend for Gross Enrolment Ratio of students in Himachal Pradesh shows that number of students opting for Higher Education is decreasing and this can be a matter of concern because as per the predictive model there may be a rise in criminal activities due to this factor.
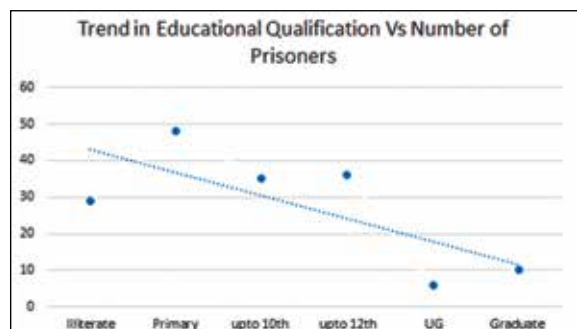
Figure 29
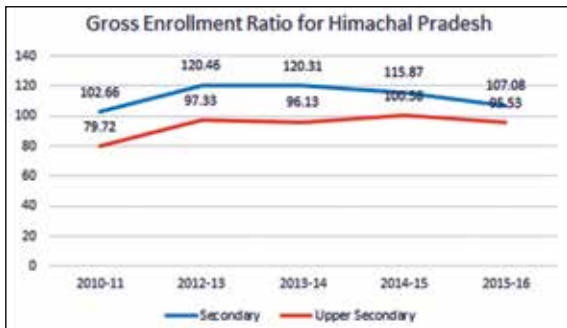
Figure 30
Data Source: NITI Aayog

- There is a strong correlation between monthly income and number of crimes committed by prisoners of that range. Thus people with low income are most probable to commit crimes as compared to that with higher income.

Figure 32
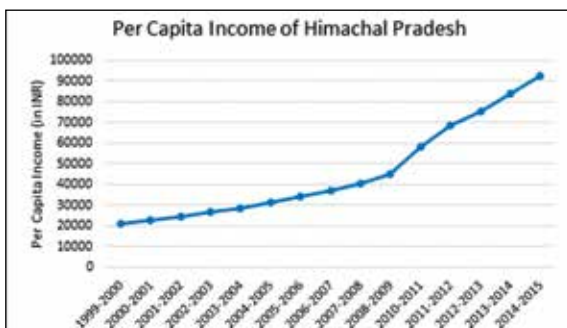
Figure 33
Data Source: Directorate of Economics and Statistics, Himachal Pradesh

Since as the per Capita Income of Himachal Pradesh is increasing, hence as per the trend line we can expect a fall in number of cases in coming years if the increase in growth rate percolates to lower strata of the society, provided the increase in income is constructively utilized in the growth of the society as a whole.

Solutions Proposed:

Better utilisation of Jail Vaarta facility:

1. An awareness about Jail Vaarta should be spread collectively amongst prisoners

2. SMS or email can be sent to the family members about the facility

3. Proper guidance must be given to the prisoners seeking assistance

Improving Medical Test Procedure

1. All the results of the medical test must be e-mailed to the jail administration along with the details of the prisoner. This will do away with the man force required and time delay caused in the treatment

2. As the number of prisoners to be taken out for the medical check-up are frequent, Model Central Jail Nahan can have its own team of guards for escorting the prisoners to the hospitals.

3. Nurse/ health worker can be posted at the hospital who can do the regular basic tests, collect the blood sample of the prisoner and send the samples to nearby hospital for the results which can be emailed to the prison authorities. This will eliminate the provision of availing police guards for the initial stage.

Awareness of Fundamental Rights

1. A printed copy of fundamental rights can be provided to each individual based on the type i.e. Convict or Under Trial

2. Special session only on Fundamental Rights can be conducted with help of NGOs

Curbing Heinous Crimes e.g. bodily offences, e.g. Murder, Culpable homicide, etc.

1. Special attention should be given to Sirmaur, Una, Solan and Kangra districts which are hotspots for the crime and deployment of extra police personnel should be done to maintain regular patrolling in these areas. There is also an issue with number of police personnel deployed in the district. It has been observed that districts with lower number of policemen per lakh population have higher number of cases.

Table 1

District	Population (2011 Census)	Sanctioned strength of HP Police (Inspector Rank to Constable)	Number of Policemen per lakh population (Rounded off to nearest Integer)	Policemen per FIR (year 2017) (Rounded off to two decimal digits)
Shimla	813384	1786	220	1.53
Solan	576670	617	107	1.65
Sirmaur	530164	664	125	1.79
Una	521057	496	95	4.36
Kinnaur	84298	406	481	0.71
Bilaspur	382056	609	159	2.02
Mandi	999518	967	97	2.56
Kangra	1507223	1387	92	2.44
Hamirpur	454293	402	88	2.13
Chamba	518844	687	1324	1.43
Lahul Spiti	31528	239	785	0.67
Kullu	437474	477	109	2.54

Data Source: Himachal Pradesh Police Department RTI Disclosure

1. Education is the most important area which should be stressed particularly in these districts. Quality of education should be improved and children should be motivated to take up higher education.
2. Skill training centres and new ITIs must be set up nearby these areas which will increase the chances of youth getting employed thereby reducing the probability of number of cases
3. For particularly these type of cases more experienced and competent lawyers must be provided through legal aid so as to reduce the financial burden on the prisoners where average spending is more than 4 lakhs per inmate

Curbing Women related crimes e.g. Rape, molestation, etc.

1. Provision should be made for surveillance of crime hotspots either technically by using CCTV cameras or increasing the number of police personnel
2. A regular self-defence training camp can be conducted specifically in rural areas for all the female students
3. Emergency signalling devices can be made available to the females at subsidized

costs whose network will be decentralized within a calibrated area and police station jurisdiction

Curbing NDPS Act, Excise Act, Forest Act, etc. Related crimes

1. Awareness about the NDPS Act must be spread at grassroots level with help of NGOs so as to make people aware of the consequences and make them familiar with lethality of the crime

2. As spending on legal aid by prisoners under NDPS Act is very high, special benches dedicated to this crime can be set up to provide speedy redressal to the prisoners

3. Measures should be taken to spread awareness of family planning

4. Quality of education should be improved in rural areas and students must be motivated to pursue higher education which can increase their chances of landing up in a better job

5. Very strict checking mechanism should be developed to counter this crime at borders specifically with more number of personnel in crack team

Curbing Diseases faced by Majority of Prisoners

Dermatological:

1. Existing patients must be treated first

2. There must be a session on importance of personal hygiene by dermatologists in the prison

3. Blankets used by the inmates must be dry cleaned on quarterly basis

Gastro Intestinal Tract

1. Prisoners must be engaged in more physical activities so as to transform their sedentary lifestyle

2. There must be a provision for deworming for the inmates once every six months

3. More roughage food can be included in the daily menu

Mental Disease

1. Most importantly there must be a dedicated psychiatrist

2. Inmates with mental disorder should be provided with facility of meeting their family and friends more frequently via Open Jail concept, Parole and Jail Vaarta

3. It must be ensured that inmates take their medication timely

In general, one annual check-up for the prisoners should be carried out so as to ensure the healthy environment inside the prison and also rule out the obsolete complaints made by them.

Also the number of pharmacist should be increased to reduce the pressure which is currently on a single worker.

Improving Wage Earning Programs

1. Prisoners must be assigned to a wage earning program considering the fact whether He/She will continue with that professional skill after being released from prison which can be determined by the nature of work available where an inmate resides.

2. A Memorandum of Understanding can be signed between Model Central Jail Nahan and Government Industrial Training Institute (ITI) to train selected prisoners based on their behaviour in various traits like masonry, carpentry, painting, driving, electric fitting plumbing, etc.

Conclusion:

This case study on life inside Modern Central Jail Nahan, has covered various aspects of living conditions inside the jail. Inmates here live in better conditions as compared to those in most of the central jails in India in terms of sanitation, food quality and well-designed spacious barracks.

Wage earning program inside the prison is very crucial for after prison life and hence an attempt has been made to fill the lacunae in the process of skill training by a list of solutions proposed in the paper. The two major issues which are availing the medical aid for the prisoners and amount spent by an inmate on legal aid can be countered with planned strategies and solutions which has been proposed. A low educational level and monthly income of the prisoners before serving were found to be the major trait for indulging in criminal activities. A trend has been predicted which explains that lower rate of enrolment of students in higher education is an area of concern and necessary steps must be taken to increase the Gross Enrolment Ratio. Thus the vision of the state government of Himachal Pradesh to provide Safe Custody, Care and Rehabilitation to the inmates can duly be achieved by taking necessary steps as suggested in this paper.

Acknowledgement

About the Authors

1. Somesh Goyal IPS, Director General of Prisons, Himachal Pradesh

2. Amit Mandal, Undergraduate in Metallurgical and Materials Engineering Department from Indian Institute of Technology Roorkee. Has keen interests include issues related to public policy.

3. Chhavi Kabra, MBBS, MD (Dept. Of Biochemistry), Government Medical College Nahan.

4. Rohit Malpani IPS, Superintendent of Police, District Sirmaur at Nahan (Himachal Pradesh)

References:

1. Report of the Comptroller and Auditor General of India on Social General and Economic Sectors for the year ended 31 March 2016

2. Department of Prisons and Correctional Administration- Himachal Pradesh

3. Prison Statistics of India 2015 by National Crime Records Bureau (NCRB)

4. *Model Prison Manual For Superintendence and Management of Prisons* in India by Bureau of Police Research and Development, Ministry of Home Affairs

5. C.B Ranganathaiah (2014) *Critical Study of Prison Reforms in India an Overview of Prevailing System of Prisons in Karnataka,* Chapter 3

6. Statistical Abstract of Himachal Pradesh 2014-15 , Department of Economic and Statistics

7. Economic Survey of Himachal Pradesh 2016-17

8. Hussainara Khatoon & Others Vs. State of Bihar (1979) SCR (3) 532

Induction of Women Combatants in BSF: Issues and effect on the organization

K Ganesh[*]

1.   Introduction

The Indo-Pakistan War of 1965 necessitated a review of the existing security arrangement and India was forced to examine the loopholes in the system as border management was with the states. There were issues pertaining to uniformity in training, weapon systems and integration issues with the Indian Army in case of a cross border conflict. A group of experts comprising the then home secretary, Shri L P Singh and COAS Gen Choudhary, recommended the raising of an armed force, which will be under the union government, mandated to guard the border with Pakistan. The Border Security Force, thus, came into existence on 1 Dec 1965 with Shri K F Rustamji as its first Director General.

The BSF proved its mettle and demonstrated its capabilities in the Indo-Pakistan War of 1971. BSF independently operated against the regular Pakistani forces and took part in several operations including the famous Battle of Longewala. BSF trained, supported and formed part of "Mukti Bahini" and had entered erstwhile East Pakistan before the actual hostilities broke out. BSF played a decisive role in the Liberation of Bangladesh.[1]

This paper will examine the effect of the policy intervention, which is the induction of women in combat role in BSF and scaling up of their strength to 15%, on the organization as well as these women.

1.1   Role of BSF

BSF has a clear cut role and task for peace as well as war. During peace it is involved in border management which includes maintaining the territorial sanctity of the nation, preventing cross border crimes and smuggling of goods. Similarly during war time, it will augment the war efforts in conjunction with defense forces. The deployment spans the Line of Control in J&K, the salty expanse in Rann of Kutch to the inhospitable Thar Desert in west. It also includes the insurgent-prone north-east with its thick jungles to the mangrove forests in the Sundarbans in the East. The deployment is 24 X 7 in the operational area with no concept of field and peace. Apart from Border Management, BSF has been actively involved in various internal security, counter insurgency, anti-Naxalite operations and duties like providing security during various elections. BSF is also called for various disaster relief operations and is part of the national disaster relief grid with three battalions exclusively earmarked for such operations. The Force is also deployed for various events like the annual Amarnath Yatra where there is a high perception of threat.

Author Intro

*   Border Security Force

1   Bsf.nic.in

1.2 Organization of the Force

The organizational structure of the Force has the Force Head Quarters (FHQ) at the top and deals with issues at a broader level. Down below FHQ is the Command HQ, with one each for the eastern borders and the western borders. The Command HQs have Frontiers (Ftr), headed by an IG (Inspector General), under them which are responsible for the operations. Each Frontiers has 3 to 4 Sectors under it and the Sectors in turn have 3-4 Battalions under them. The Battalions are responsible for conducting the day to day operations in BSF and in other words, the boots on the ground. All formations above the Battalion can be termed having a supervisory role. The rank structure can be divided into three categories. Officers, Subordinate officers (SO) and the Other Ranks (OR). Overall the force has 15 levels in the hierarchy, the Officer cadre has 9 levels with DG at the top and Assistant Commandant at the bottom. The SO category has three levels and the other ranks have 2 levels.

2. Background of Induction of Women in Combat Roles

Fencing gate management is an important aspect of border management as farming activities are carried out by Indian farmers in the 150 meters patch ahead of the border fencing. Women form a sizeable portion of the farm workers who go ahead of the fencing. There was no provision for physical checking of these women as BSF did not have any woman in the general duty cadre. There is a real possibility of these women being used for smuggling contrabands. In the eastern front BSF faces the problem of illegal immigration from Bangladesh, which includes women. In addition to the border management related issues, BSF is being increasingly used for internal security duties which again requires dealing with women. As a result a need for

women in GD cadre was felt and for the first time in 2008, an initial recruitment of 745 Constable/GD (Women) was carried out. Subsequently in 2010, 15 Sub Inspectors (Women) were inducted.

BSF had initially submitted a proposal for raising two exclusive women BNs but was advised by the Ministry of Home Affairs (MHA) to raise the percentage of women in the Forces to 5% in 03 years (the % of women in other CAPFs). BSF revisited its initial proposal and the requirement of women in the general duty (GD) cadre for duties on functional fencing gates, border hats & ICPs (Integrated check posts) was worked out to 11,140 for the entire force. Meanwhile MHA also constituted a committee comprising all DsG (Director General) of CAPFs (central armed police force) under the chairmanship of DG BSF to examine the issue of induction of women and the practical difficulties being faced by the CAPFs in deployment of women due to difficult working conditions and to suggest measures for increasing representation of women in different cadres of CAPFs. The total requirement of women personnel in BSF was assessed as 5000 for 111 battalions deployed in normal areas, mainly on the border, where the services of women constables could prove useful and it was proposed to induct 3000 women personnel in GD cadre in Constable Rank in the initial three years and further raise the number gradually.

2.1 Present Status and Profile

Women at present constitute 1.66 % of the total work force in BSF which includes the medical cadre, ministerial cadre, communication and civilian staff, the total of which works out to 4,147. The women constables constitute the bulk of this, numbering about 3,322.. The recruitment process started in the year 2008 when initially 735 were recruited and bulk of the recruitment was done in 2012 and 2013 when more than 2,300 women constables were recruited. The state wise representation is tilted towards the

eastern region with Bihar, Bengal and Uttar Pradesh contributing more than 50% of the women constables.. More than 70 % of these combatants are very young falling in the age bracket of below 25 years. 20 % are in the age bracket of 25-30 years.

4.   Methodology

The research methodology is based on literature available on the subject, capturing of primary data through questionnaires and collection of secondary data from BSF. A list of 36 questions was prepared based on ground condition as well as experiences of serving BSF officers and staff. These questions relate to the working conditions and instances which have in the past been known to be stress inducing i.e. leave related matters, interaction with superiors, etc. The questions were in multiple choice format to keep it simple and less confusing. The last question was kept open ended so that the respondents could write on issues they think are important. The aim was to elicit response from the women constables on issues like job satisfaction, gender based discrimination, sexual harassment and stressors and motivators. The sample size has been kept at 55 owing to the logistical issues involved and time constraint. The participants are presently serving in North Bengal Frontier and about 8 to 10 women constables were interviewed from 6 different battalions of Siliguri and Kishanganj Sector. The participants were apprised of the purpose of the exercise and written consent was taken in advance before proceeding with the questionnaire. A lady teacher from the BSF primary school was further briefed and tasked with getting the questionnaire filled in as detailing any one from the Force would have resulted in not getting free and frank response from the respondents.

Secondary data was collected from the Force Head Quarters at Delhi. All relevant statistical data, letters and policy papers were collected from the EDP center and the concerned directorates. The information available on the BSF web site was also used for this purpose. The field commanders were also interviewed telephonically and through emails to get their point of view. The commandants of 66 Bn, 93 Bn, 61 Bn, 77 Bn and 22nd Bn participated in this exercise as they have been provided with women constables in their Battalions. The perspectives of company commanders were also taken as they are directly dealing with the women constables on ground.

5.   Issues and challenges

The foremost challenge is the human resource management of the women constables as the organization has a predominantly male oriented culture and adapting to the changing dynamics of a mixed gender organisation will take time. Human resource management basically implies identifying, selecting, training and managing the manpower to efficiently meet the requirements of the organization. BSF is no exception and it has the added responsibility of maintaining a high standard of morale and motivation in view of the extremely difficult and hazardous service conditions. The following issues pertaining to HRM will be examined

- •   Recruitment and selection
- •   Training
- •   Postings
- •   Career management
- •   Sexual harassment and grievance redressal mechanism
- •   Motivation and Incentive

5.1   Recruitment and selection:

Recruitment is a three stage process. The first is the physical standard test (PST) which is

followed by Physical efficiency test (PET). This forms the initial screening of the candidates, those who qualify this part are required to go through a written examination that is conducted by the Staff selection Commission (SSC). Those who qualify this are called for a medical examination and all those who qualify the medical examination are ranked as per their performance in the written examination and call letter is issued as per the vacancy. The physical efficiency requirement has been relaxed for the women candidates and the selection process is also against the reserved vacancies earmarked for them.

The next level where the women are inducted is at the Sub Inspector (SI) level. The process is the same as in constable but has an additional Interview stage as it is a supervisory post. The educational requirement for SI is graduation whereas for the constable it is Class 10. The BSF hierarchy in the general duty stream has 15 levels and entry is at three levels .i.e. CTs, SI and Assistant Commandant (Class 1 officer). The officers are selected by the UPSC. At present BSF is not recruiting any women in the officer grade. Although the process has begun, it will take a few years before they are actually inducted into the service. This is likely to create a problem in terms of representation and in making the organization responsive to gender issues.

5.2   Training

BSF has a highly structured training infrastructure. All recruits are initially put through a basic training for a duration of 46 weeks. For the Constables, this training is carried out in the subsidiary training centers (STCs). There are 13 STCs in different parts of India for this purpose. The training standards have again been reduced as compared to the standards prescribed for

men as the physical capacity varies in case of women. In the article "Army Women"[2], Charles Moskos has cited that average female upper-body strength is 42 percent less than average male upper-body strength. Looked at another way, the statistics mean that on average the top fifth of women in lifting capacity are the equal of the bottom fifth of men on the same measure. As there is no difference in job description at least on paper, this creates an ambiguity and indirectly signals that women are meant for less stern jobs. The training is also in exclusive women only batches, which makes their integration in a male dominated setup even more difficult.

Once these constables successfully complete their basic training, they are posted to BSF battalions where again they are put through a structured probationary training and are mentored by their seniors on ground. This is the hand holding stage and they are not assigned duties independently. Subsequent to completion of the probation training they perform independently the duties assigned to a constable. The Sub Inspectors are trained at the Specialist training school (STS) which is part of the BSF academy[3] or at Training School and Center, Hazaribagh. Specialized training in Weapons and Tactics is given at CSWT (Central school of Weapons and tactics)[4], similarly there are other specialized training centers available for skill upgradation.

5.3   Job description & employment

So what should a women who is inducted as a constable expect to do? Constables form part of a section which is lowest formation in the organizational hierarchy. The duties performed by a constable can be broadly categorized as

•   Operational duties specific to border like Observation Post (OP) duty, patrolling, ambush, gate management

---

[2]   http://www.theatlantic.com/magazine/archive/1990/08/army-women/306156/ (August 1990)
[3]   Acy.bsf.gov.in
[4]   Csw.bsf.gov.in

- Raid, Cordon and search, Road opening Party (ROP) in a Counter Insurgency/ Internal Security deployment
- Camp security
- Preparation and maintenance of defense in Border out post
- Administrative duties

At present the women combatants are used in a limited way and are generally used for gate management, OP duty and patrolling with their male colleagues. All duties are jointly performed with their male colleagues, as assigning them duties independently is considered physically risky. High risk assignments like ambush and night duties in the border are not assigned to them. The women combatants have been inducted for the border deployed battalion in less sensitive areas and not for deployment in Line of Control (LC) in Kashmir or in the militancy affected areas of North East.

If we correlate this with the response given by the women constables, of the 55 interviewed, 21 women feel they are as capable as their male counterparts and are fit enough for all assignments whereas 23 women, the opinion is evenly divided and with the passage of time they will be more than willing to shoulder the responsibilities on par with their male colleagues. With scaling up of the percent of women in the force, assigning independent responsibilities will become inevitable and the present mindset of treating them as a vulnerable group will have to go. The training standards will have to be re-examined and they will have to be made more competent and confident. Another fact that has come out is that most women have shown some sort of reluctance for night duties and prefer camp duties to duty at border, as this is a recurring theme in the open ended question given to them. The Commanding Officers have also stated in the interview that this is an outcome of softer duties being allocated to them ever since their

induction.

The problem is that these vacancies are not additionally created ones and the women combatants are recruited against the sanctioned post of the constables in the force. The current strength of women combatants is around 3,500 and when it is scaled up to 15% of the force's strength it will be close to 30,000 women combatants. The problem for the organization would be how to maintain the operational efficiency when 15% of the force has to be given soft jobs only. The current mindset will have to give way to equality in employment irrespective of the gender. Otherwise it will only increase the work load on their male colleagues. Typically, not more than 40% of the force is available for border duties at any point in time. The rationale being that 30% are on leave, 15% on temporary duties, courses, transit, sick leave , attachment with higher headquarters, sports team etc. 15% are required for various administrative duties/ training at the battalion headquarters. Since only about 40% are available for the actual duties on border it is imperative that each and every person is employed to the fullest potential. The other issue is that the organization will permanently be blocking about 30,000 posts of constables in places which are considered soft and less threatened and as a result the male colleagues will be serving longer duration of their service performing tough assignments in difficult locations. There are 177 BSF Battalion locations, which have been classified as extremely hard (19), hard (52) and soft (107). The women are at present being posted only to locations classified as "**soft**". The battalion commandants who were interviewed, feel that this is likely to be an issue for discontent among the men

5.4   Posting & Transfers

At the battalion level the constables are seldom posted and the idea behind this is to develop

a sort of regimentation among the troops. Cohesion is an important aspect among the troops as it helps them cope with tough situations and service conditions. Constables are posted out of a battalion only when they are deputed to some external organization like NSG/ SPG etc. or when they get posted to a static headquarters or training center within BSF. Other than this an individual may request for posting to a particular location due to a medical or family problem on compassionate grounds, which will be considered as request posting. In almost all the cases they return to their parent battalion when the tenure is over. The identity of a battalion is therefore very strong and so is the camaraderie between the troops. In the case of women constables, their posting is more location and tenure specific as per the SOP (standard operating procedure). They serve in a frontier location for 5 years and then they are posted to a different frontier. This results in their being posted out of outgoing battalion and getting posted in incoming battalion during changeover of battalion which is not the case for other members of the Battalion. The comfort of cohesion and bonding that makes the troops work in extremely stressful conditions is not available to them. They are also not fully integrated in the battalion because of this policy. Most married respondents (31% of the sample data) have indicated that posting should be in their home state for a better work life balance and have shown a high level of dissatisfaction due to separation from family and not being able to look after their children. As more and more young women start getting married the problem is likely to get aggravated.

5.5   Career management

The Women Constables in due course of time will pick up the rank of a Head constable and subsequently become an Assistant Sub Inspector (ASI) commanding a section. A section commander requires all round skills and command capability. As per the career progression and opportunities available to them, a women can expect to retire as an Inspector. The current role and task of the women constables will put them in a disadvantageous position as they lack the exposure required for the appointment. Second will be the effectiveness in commanding a predominantly male detachment. Same will be case for a Sub Inspector, who is usually promoted to the rank of an Inspector in 5-6 years and should aspire to retire as a Deputy Commandant. Inspectors are the Second-in-Command in a Company and in most cases command a company as officers are not present all the time. This again will create command and control issues which are not good for the organization.

5.6   Motivation

The main reason for these women for choosing a career in BSF appears to be financial security. If we look at the survey data, only six have said the compensation is poor and the majority think either it is good or satisfactory. In addition to the salary component there are allowances to compensate the risk element and hardship due to service. Added to this they have a liberal leave entitlement, access to health care for self and family, canteen facilities and a host of other welfare schemes. More than 80 % have said that the reason for joining BSF is for employment or for financial reasons. Only 11 out of 55 have said they are in the service for serving the nation. More than 50% of the respondents have said they will quit in less than 20 years and only 18% want to serve till the retirement age. The majority of the respondents feel that their status in the community has gone up because of their joining BSF. Is there any trend in terms of resignation from service?

Year	Vol Retirement	Resignation
2012	0	9
2013	1	3
2014	0	5
2015	0	0
	Source: LS QUESTION NO 1296 ANSWERED ON 03.03.2015	

5.7   Sexual harassment and Grievance redressal mechanism.

Ruth Rosen in the article "The invisible war : sexual assault in American military"[5] has stated that "more than 26,000 soldiers, mostly women, but also men, had experienced sexual assault in 2012, based on an anonymous survey as estimated by Pentagon. Most do not report the assault to their commander, and in about a quarter of the cases, he was the rapist or abuser. Reporting of sexual assault is considered a career breaker. A commanding officer is vested with immense powers and generally such incidents are brushed aside so as not to damage the unit's image and guilty are let off".

The supreme court of India in the judgement passed in 1997 a set of guidelines for dealing with sexual harassment cases in work places which is known as the Vishaka Guidelines. These were further superseded by the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. The parliamentary committee on "working condition of women in police force[6]" has examined this issue and is satisfied with the existing mechanism for dealing with such cases. Ministry of Home Affairs (MHA) is also monitoring all such cases and BSF is sending a monthly report pertaining to such incidents and the progress on action taken. Only 9 such cases have been shown pending or not settled in the report for the month of Dec 2015 and action has been initiated by BSF as per the guidelines. This can be said to be fairly satisfactory considering the fact that more than 4000 women employees are currently serving in the force.

Gender based discrimination and sexual harassment	Always	Sometimes	Never
Remarks about physical attributes made by male peers/ superiors	1	0	54
Inappropriate physical contact/touch	2	2	51
Jokes of Sexual nature	1	3	51
Explicit /Implicit request for sexual favours	0	1	54
Unwanted attention through phone/letters/messages	2	3	50
Discrimination at work place	2	16	37
Are men & women given different job assignments	16	28	11
Do peers differently because of gender	2	15	38
Less opportunities because of gender	10	23	22

The survey also validates the above findings as out of the 55 respondents 54 have never experienced any implicit or explicit request for sexual favors nor any remarks made at them about their physical attributes. Similarly 51 respondents have said they have never been subjected to any sort of inappropriate touching/ physical contact or any jokes of sexual nature directed at them. But at the same time 4 have experienced some sort inappropriate physical

---

5   The Invisible War: Sexual Assault in the American Military – Ruth Rosen. Huffington Post (July 2014)

6   COMMITTEE ON EMPOWERMENT OF WOMEN (2012-2013) (FIFTEENTH LOK SABHA)
    WORKING CONDITIONS OF WOMEN IN POLICE FORCE' Presented To Lok Sabha On 6th September, 2013

contact and sexual jokes directed at them. The number could be more as in the open ended question a large number of them have indicated some sort of verbally inappropriate behavior and issues like staring.

The force has a proper grievance mechanism in place[7]. In a battalion the second-in-command is the designated grievance officer and in case an individual is not satisfied with the redressal mechanism she may approach the higher headquarters. There is a toll free number available for registering complaints against superiors and complaint can be lodged through a specific module available in the BSF intranet available to all serving personnel. In the survey, about 50 % have said the existing mechanism needs improvement and are not satisfied with the current system. The options available for grievance redressal needs to be disseminated properly for the system to be more effective. The perception about the existing mechanism does not vary among the married and unmarried combatants.
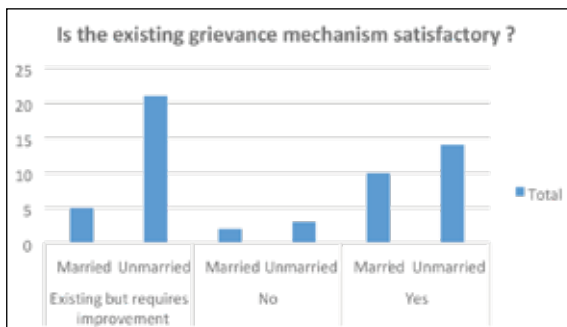
6. What are the major stressors?

Are women more stressed out in the para military forces as compared to the men? An article in Times of India[8] has come out with a figure that 40% of suicides in central paramilitary forces are committed by women who constitute less than 2% of the strength of these forces. The article citing NCRB data for the year 2014, cites marriage related problems and family issues constitute more than 40 % of reason for suicides. The fact that these women remain separated from their families for long duration of time, gives them little time to attend to issues related to marriage and family, which is a major cause of stress. BPR& D (Bureau of Police Research and Development) carried out a study on occupational stress in BSF[9]. Some of the factors which have been identified in the study as stress causing are

- Inadequate rest/ sleep
- Poor communication and inaccessibility of seniors
- Leave related issues
- Poor infrastructure and lack of basic amenities
- Separation from family

In a report submitted on "Working condition of women in Police Force" by a parliamentary committee on empowerment for women in the 15th Lok Sabha[10], timely availability of leave, long duty hours and absence of child care facility combined with separation from family has been identified as a major cause of stress among the women.

Charlotte Woodhead in her thesis "The mental health and well-being of women in the UK Armed Forces" (2012)[11] writes about Women Combatants being exposed to an additional set of stressors, such as living and working in a male-dominated environment, balancing work and issues related to being the primary caregiver.

---

[7]   http://bsf.nic.in/doc/welfare
[8]   http://timesofindia.indiatimes.com/india/Women-account-for-2-of-central-forces-but-40-ofsuicides/articleshow/48180814.cms (23 July 2015)
[9]   "Emotional Intelligence & Occupational Stress" A study of BSF Personnel (M.K.Chhabra, 2009)
[10] COMMITTEE ON EMPOWERMENT OF WOMEN (2012-13) (15th LOK SABHA) TWENTY FIRST REPORT 'WORKING CONDITIONS OF WOMEN IN POLICE FORCE'
[11] The mental health and well-being of women in the UK Armed Forces. (Charlotte Woodhead, 2012).

6.1   Rest and Sleep

Jennifer Soong in the article "How sleep loss affects women more than men "[12]examines the various factors and finds women to be more vulnerable. According to Soong "The reason could be the hormones and further it could lead to lesser life span. The other health issues could be increased incidence of type 2 diabetes, weight gain and depression". Yasmin Anwar in her article on sleep loss and psychiatric disorder[13] has examined results from a brain imaging study which suggests that while a good night's rest can regulate your mood and help you cope with the next day's emotional challenges, sleep deprivation does the opposite by excessively boosting the part of the brain most closely connected to depression, anxiety and other psychiatric disorders. None of the respondents have said that they get more than 8 hours of sleep and 17 have claimed that they get less than 6 hours of sleep.
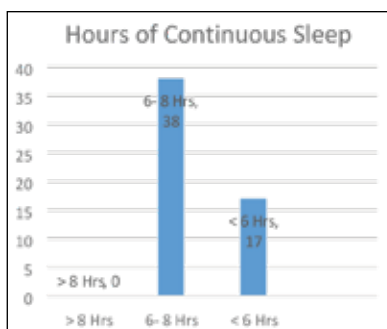
6.2   Child care and separation from family

There is a crèche facility available at the Battalion HQ but it will not meet the requirement in case the mother has to perform duties at the border. At present these women are entitled for a maternity leave of 180 days for up to two children and in addition they are also entitled for a Child Care leave of 2 years which can be taken any time

till the time the child is a minor. Effectively in a twenty year service a women having 2 children will not be available for 3 years. This will further add up to the deficiency and some thought will have to be given to this aspect, like having a reserve, if we have to scale up the percentage of women to 15% in the force. Even with all this, there can be no substitute for full time child care which will be a problem area for most women in BSF as compared to their civilian counterpart. 18 of the respondents were married and out of which 10 were mothers. Only 4 were taking care of their children and the others were dependent on their parents or in-laws. The commandants also feel there is no institutional mechanism for operating a crèche at battalion locations and more funds and manpower will be required for having such a facility in the proper sense. A majority of the respondents have said this is a major area of concern for them. BSF will have to think of a mechanism where child care can be provided at the place of duty, otherwise this will be a major cause of discontentment among women in the force. Almost all the women have stated that the initial posting should be in their home state. This again is not feasible as the recruitment is not restricted only to the Border States and women constables are being recruited from all over the country.

6.3   Leave

Not getting leave when required especially in case of a family emergency is one of the major stressors among the troops. Cases of fratricide have been triggered due to denial of leave. Ensuring timely availing of entitled leave by the troops in particular is considered a command responsibility. Leave is being sanctioned liberally and some commandants feel that the women constables avail far more times than their male

---

[12]   http://www.webmd.com/women/features/how-sleep-loss-affects-women-more-than-men: Jennifer Soong, WebMD Magazine Feature

[13]   Sleep loss linked to psychiatric disorders (Yasmin Anwar, 2007) UCBerkeley News

colleagues. A majority of the respondents have availed more than 3 times in the previous year and almost all of them have said that leave is granted on demand and as such is not a problem area.
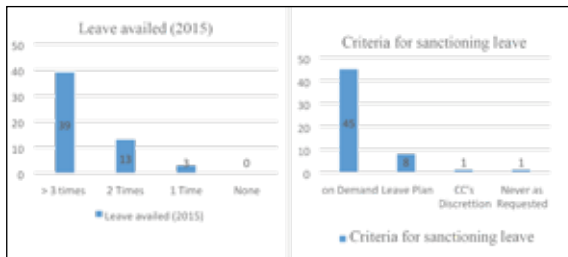
6.4 Living accommodation

It will take some time before separate barracks are actually constructed. At present a separate living space has been earmarked out of the buildings already existing in the BOP. This being a stop gap arrangement, the respondents feel is too cramped and needs improvement. The problem will increase once the full strength is available. BSF will have to plan this aspect as a proper accommodation is a basic necessity. The issue of availability of toilets have also been raised as 20 respondents have said they don't have any access to toilet at the place of duty where they are present for 6 to 8 hours at a stretch and even when it is available there is no provision of water which makes it difficult for them to use it. BSF can procure portable toilets and provide them at all such places where these constables are performing duties.
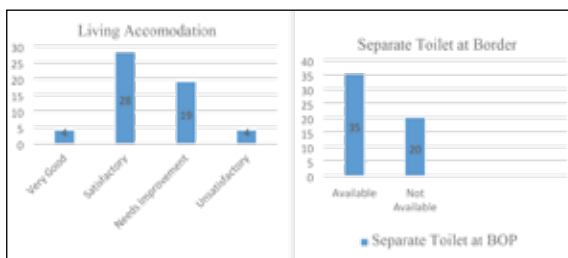
6.5 Other issues

Some of the issues that were projected by the respondents in form of feedback were:

Medical: 40 of the 55 interviewed have said they don't have access to a lady doctor. The force will have to have more lady doctors on contractual basis in addition to the existing strength of doctors and frequent visits to be made to the border so that the medical problems specific to these women can be attended. Another issue was rest during the menstrual cycle as almost all feel it is physically very demanding for them to perform duties at the border. Although it might not be a feasible idea to take them off the roster completely but they can be assigned relatively less strenuous duties like camp guard etc.

Out Pass: There is an overly cautious approach and the women feel they have far less freedom to leave the Bop for visiting local market etc. for personal work as compared to their male colleagues.

Some have said that they don't get more than 1 out pass in a month. The issue could be their safety outside the campus and this could be resolved by sending them in groups along a male colleague.

Gender sensitivity: use of cuss words is very common and has more or less has become a part of the vocabulary and this has been termed an offending behavior by most of the respondents. The male members of the force will have to be sensitized about the language they use keeping the sensitivity of women working along with them.

7. What are the Policy Options?

The way out can be having an exclusive women battalion which, like in CRPF, will have women in the entire hierarchy up to the command level. These battalions can be @ of one per Frontier. This will have many advantages over the present setup as women constables will have a better sense of identity. It will not affect the structure or functional efficiency of a

regular battalion and also there will not be any functional ambiguity. Second option could be go for a short term appointment, similar to the short service commission in Army, for period of 10 years after which they can be moved to state police organizations in their respective home states or CRPF/CISF where the nature of duty is less strenuous and at the same time has a wider geographical presence. This would keep the age profile of the constables young and at the same time they will have the incentive of going back to their states with assured re-employment.

The third option would be to move them to less stressful administrative jobs after 10 years within the organization. They can be retrained and used as nurses, radio operators, clerical staff etc. This will have a limited scope as the number of administrative openings are limited. A combination of the above two options can also be worked out. More than the induction it is equally important to have an exit and rehab plan otherwise the force will face the risk of an aging disgruntled work force that will be difficult to deal with. Since women are being used operationally in a limited way, their role and job specification should be clearly defined and training should also be designed specifically keeping in mind their work profile.

Further, efforts should be made to improve the ratio of women at the officer and subordinate officer level. Although it is in the pipeline, an ideal situation would have been opening up of proportional vacancies at all the three levels simultaneously. This would then to a large extent take care of the grievance redressal mechanism as these constables would feel much more comfortable approaching women superior officers with their grievances.

Deployment of these women should not be restricted only to battalions locations categorized

as normal but at all locations and the mindset that they are only meant for gate management should be done away with, if the 15% quota is to be implemented. Otherwise the ratio of men in hard and extremely hard locations will be skewed and similarly all soft locations will have a higher percentage of women, which will lead to discontentment in the force.

Training and selection standards should be comparable if not uniform. US Marine Corps training standards for men and women are almost comparable with difference in terms of time and not standards[14]. By having a different standard at the induction level itself, a message is being sent that there will never be any parity in the nature of work. Training should be conducted in mixed batches which will result in better cohesion right from the training stage.

Better organizational support in terms of childcare, living accommodation and grievance redressal mechanism is required to reduce work related stress. The US Army, Navy and Airforce run a combined childcare program that looks after more than 200,000 children at over 600 locations in US and abroad. The child development centers (CDC) are standardized and have trained manpower, and can take care of children from 6 months to 12 years. They also have the concept of family child care (FCC), where a family is certified to take care of a child for an extended period[15].

Such practices can be replicated here also.

9.   Conclusion

Having women combatants is a challenge as well as an opportunity. BSF needs to have a long term strategy on how to assimilate these combatants in the organization and plan their career growth, training and retention. The induction has been more of a knee jerk reaction with not

14   USMC PFT Score Charts. Source : Military.com
15   Options for improving the military child care system. (Gail L. Zellman et al. 2008). Source : www.Rand.org

much thought given to the HR issues and other organizational challenges discussed above. The pressure for increasing the representation of women in the forces is only going to increase so it will be in the organization's interest to have a well thought out plan to address these issues arising out of induction of women in the force. The approach should not be one of having separate silos for the male and female combatants but how well they can be integrated right from training to deployment. There is a lot to be learnt from other countries as well, especially Israel and the US and the policies should take into consideration the best practices these countries have implemented. A holistic and long term view and approach is required to deal with this issue, so that BSF as a premier border guarding force is able to maintain its operational efficiency.

References

1. Louisa Blackwell and Daniel Guinea-Martin, 2005.Occupational segregation by sex and ethnicity in England and Wales, 1991 to 2001. Health and Care Division, Office for National Statistics, National Statistics feature.
   http://www.ons.gov.uk/ons/rel/lms/labour-market-trends--discontinued-/volume-113--no--12/occupational-segregation-by-sex-and-ethnicity-in-england-and-wales--1991-to2001.pdf. (Downloaded on 19/9/15)

2. Kathleen F. Kirk, LT, USN, 1988, Women in Combat. Faculty of the School of Education. San Diego State University
   http://calhoun.nps.edu/bitstream/handle/10945/23446/womenincombat00kirk.pdf?se quence=1 (downloaded on 10/09/15)

3. Charlotte Woodhead, 2012. The mental health and well-being of women in the UK Armed Forces. Thesis submitted for the degree of Doctor of Philosophy at King's College London. Department of Psychological Medicine.
   https://kclpure.kcl.ac.uk/portal/ (downloaded on 10/9/15)

4. Arundhati Bhattacharya, 2012. Women in Military in India: A cry for parity, Mediterranean Journal of Social Sciences, Vol. 3 (2) May 2012.
   http://citeseerx.ist.psu.edu/viewdoc/ download; jsessionid = 5D008FD762D9C619EE86B9 A3C7E63228?doi = 10.1.1.476.4354 & rep=rep1 & type = pdf (Downloaded on 20/9/15)

5. Aharon S.Finestone, Charles Milgrom, RanYanovich, Rachel Evans, Naama Constantini, and Daniel S.Moran, 2014. Evaluation of the Performance of Females as Light Infantry Soldiers. Hindawi Publishing Corporation, Volume 2014, Article ID 572953, 7 pages

6. M.K.Chhabra, 2009."Emotional Intelligence & Occupational Stress" A study of BSF Personnel. Bureau of Police Research & Development Ministry of Home Affairs New Delhi.
   http://bprd.nic.in/writereaddata/linkimages/9402946977-Executive%20 summary.pdf (downloaded on 15/12/05)

7. Gail L. Zellman et al. 2008. Options for improving the military child care system. Source: www.Rand.org (Accessed on 01/03/16)

8. Committee on empowerment of women (2012-13) (15th Lok Sabha) twenty first report 'working conditions of women in police force' http://164.100.47.134/lsscommittee/Empowerment%20 of%20Women/16_Empowerment _of_ Women_2.pdf (Downloaded on 15/12/15)

Child Abuse: Two Case Reports Showing an Under-Reported Diagnosis in India

Dr Abhishek Yadav[1]

Dr Mahesh Kumar[2]

Dr Mansi Kumar[3]

Dr Sanjay Kumar[4]

Abstract

Physical Child abuse also known as Battered baby Syndrome (BBS) or Non Accidental Injury (NAI) occurs when the child suffers repetitive physical injuries by a parent or guardian. It can cause severe injuries to the children and even death. We report two autopsy cases in which both the children were brought dead to the All India Institute of Medical Sciences (AIIMS), New Delhi by the guardians with no complaint of foul play. During autopsy the characteristic findings of physical abuse were found and were reported to the investigation officer. It led to the arrest of the guardians and legal proceedings were initiated. The western countries have developed a centralized reporting system for child abuse but the cases of physical and mental abuse of children mainly at their home from parents or guardian are highly under-reported in India. The authors intend to highlight the importance of interpreting such injuries not only during autopsy but also in clinical setups so that perpetrators of child abuse are not spared. The authors have given recommendations about the steps which could be taken to detect child abuse at an early stage and save the life of a child.

Keywords:

Physical Child abuse, Battered baby Syndrome, Non Accidental Injury, Child neglect, Torn Frenulum.

Introduction

Child maltreatment is the abuse and neglect that occurs to children under 18 years of age, which includes all types of physical and/or emotional ill-treatment, sexual abuse, neglect, negligence and commercial or other exploitation, which results in actual or potential harm to the child's health, survival, development or dignity in the context of a relationship of responsibility, trust or power[1]. Physical Child abuse is also known as Battered Baby Syndrome (BBS) or Non Accidental Injury (NAI) and occurs when the child suffers repetitive physical injuries by a parent or guardian[2]. The western countries have

---

Author Intro:

1.   Assistant Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences (AIIMS), Ansari Nagar, New Delhi, India

2.   Assistant Professor, Department of Forensic Medicine and Toxicology, Rama Medical College Hospital and Research Centre, Nh-24, Hapur, Uttar Pradesh

3.   Assistant Professor, Department of Obstetrics and Gynaecology, Rama Medical College Hospital and Research Centre, Nh-24, Hapur, Uttar Pradesh

4.   Associate Professor, Department of Forensic Medicine and Toxicology, Vardhman Mahaveer Medical College & Safdarjung Hospital, New Delhi, India

developed a centralized reporting system for such cases,[3,4] with many studies and cases also being reported in Medical Literature[5-11]. In India, the protection of children is ensured through 'The Juvenile Justice (Care And Protection Of Children) Act, 2015'[12] and 'The protection of Children from Sexual Offences Act, 2012'[13] also known as POCSO but the cases of physical and mental abuse of children mainly at their home from parents or guardian are highly under-reported.

We report two cases in which both the children were brought dead to the All India Institute of Medical Sciences (AIIMS), New Delhi by the guardians. Police did not report any foul play as there were no complainants. During autopsy the characteristic findings of physical abuse were found and were reported to the investigation officer. Subsequently the guardians were immediately arrested and legal proceedings were initiated. The authors intend to highlight the importance of interpreting such injuries not only during autopsy but also in clinical setups so that perpetrators of child abuse are not spared.

Case No. 1

An eight year old male child, who was living with her step mother, was brought to emergency department, Trauma centre, AIIMS, New Delhi, by his step mother with alleged history of fall from chair. The child was found brought dead and a medicolegal case was registered. The mother and father of this child had been divorced and married to different persons again and presently this child was staying with his step mother.

Autopsy revealed multiple old and fresh injuries all over the body in the form of patterned abrasions, contusions and laceration (Image-1). Infective Dermatitis was present over face, lips, forearms, ears and neck (Image-2). Burn injury was present over gluteal region and penis suggesting cigarette butt burns (Image-3).

Multiple bruises were present over the forehead. Subdural haemorrhage was present over both the parietals and occipital regions of the brain. During the course of investigation, the investigating officer (IO) produced an electric iron (Image-4) that was allegedly used to burn the gluteal region of child for correlating the burn marks.

IMAGE-1: Case-1: Multiple Patterned abrasion, contusion and Laceration in different stages of Healing present over the Body

IMAGE-2: Case-1: Patterned abrasion and Infection Dermatitis over right forearm.

IMAGE-3: Case-1: Burn marks in different stages of healing over Genitalia, gluteal region and Right Thigh.

IMAGE-4: Case-1: Electric iron used to inflict burn marks on child.

Case No. 2

A three year old male child, who was brought to emergency department AIIMS, New Delhi with alleged history of fever and unconsciousness. The child was found brought dead and a medicolegal case was registered. The IO gave the history that the child was sold by his biological parents to a lady of Jharkhand, who came to Delhi and started working as a house maid through a couple working as placement agent. She was not allowed to bring the child along with her and usually handed him over to the above mentioned couple. This lady went missing for about a month and the child was left with this agent couple who brought the child to emergency department of AIIMS.

Autopsy examination revealed multiple old and fresh injuries all over the body in the form of patterned abrasions and contusions (Image-5). Infective Dermatitis was present over face, lips, ears and neck (Image-6). Cauliflower appearance was present over left ear indicative of repeated slapping (Image-7). On radiological examination recent fracture of lower end of shaft of left humerus and old fracture of shaft of left

radius bone were found. Liver was lacerated, and spleen and kidney were showing hematoma in the parenchyma. Diffuse subdural haemorrhage was present over right parieto-occipetal region of brain (Image-8).

IMAGE-5: Case-2: Multiple Imprint Abrasions, Contusions and Lacerations in Different stages of healing with Infective Dermatitis present over the body.

IMAGE-6: Case-2: Cauliflower appearance over left ear.

IMAGE-7: Case-2: Recent fracture of Left Humerus and old fracture of radius bone.
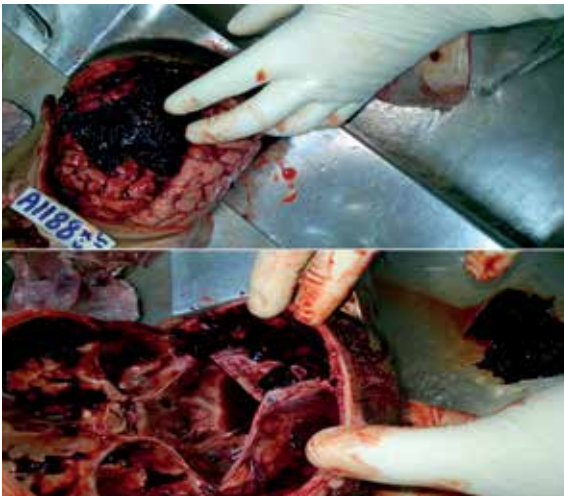
IMAGE-8: Case-2: Subdural haemorrhages over cerebrum.

Discussion

The child abuse can be diagnosed clinically by the following classical sign and symptoms, in **different stages of healing**:[2,14,15]

1. Bruises may be patterned, particularly on back, buttocks, genitals, ears and back of hands.
2. Multiple abrasions and lacerations.
3. Fractures in long bones.
4. Burns reflecting the pattern of object or method of injury.
5. Torn Frenulum-considered as a reliable indicator of child abuse.
6. Eye injuries such as bleeding into vitreous humor, dislocation of lens, retinal detachment, and retinal hemorrhages.
7. Dislocation and injuries of teeth and gums.
8. Bite marks.
9. Scars.
10. Pulling of scalp hair.

The head injury is the most common cause of death as evident in both of the cases. Both the cases had multiple injuries at different stages of healing. Skin infection was present indicating the neglect of children. In case no 2, the child had Intra-abdominal injuries also, which are the second most common cause of death in battered children[2,14]. His whole body X-ray revealed fractures of long bones of different age. In cases of suspected child abuse, radiological investigations are vital in identifying bodily fractures and head injury[10]. The child abuse is more prevalent in males and children are more likely to cause severe injuries as seen in our cases[11]. The burn injuries on the penis and gluteal region of child in case no1 by cigarette and electric iron show the brutality the child was subjected. We can clearly infer by the autopsy findings in both the cases that the children were subjected to physical abuse, which was also confirmed by the police investigations into the cases.

In united Kingdom, National trauma audit is performed by the Trauma Audit Research Network (TARN), which includes data from 96% of acute hospitals in England and Wales reported severe injury (ISS >15) due to NAI in 9.7% of children below 2 years with Mortality rate of 7.8% and in 2.1% of children above 2 years with Mortality rate of 27.6%[4]. This indicates the urgent need of a similar Trauma registry network in India for children. In the reported cases the culprits would have got off scot-free with dead children getting no justice if the autopsy surgeons had not diagnosed child abuse.

Recommendations

1. The emergency doctors, paediatricians and doctors in trauma management like orthopedician, surgeons, neuro-surgeons etc should be trained and sensitized to diagnose the cases of child abuse properly so that it can be identified at an early stage and the life of the child could be saved. But care should also be taken to prevent any misdiagnosis which could cause the harassment of innocent parents or guardians.

2. Private family practitioners should be given training and professional to interpret the sign and symptoms of child abuse and report it to the police or child welfare committee.

3. Whole body X-ray should be mandated in all the autopsy cases of children dying with no clear history.

4. A Paediatric Trauma registry network should be started by Government of India which could connect with the major district hospitals all across the country.

5. The same can be implemented by starting initially at the central govt hospitals and then gradually involving hospitals at state level, then district level and so on.

References

1. World Health Organization. [Internet]. [Cited 2016 Nov 21]. Available From: http://www.who.int/topics/child_abuse/en/

2. Saukko P, Knight B. Knight's Forensic pathology. 3rd Ed. London: Arnold; 2004. Ch-22, Fatal Child Abuse: p461-479.

3. National data archive on Child abuse and neglect. [Internet]. [Cited 2016 Nov 21]. Available From: http://www.ndacan.acf.hhs.gov/about/about-mission.cfm

4. Trauma audit and research network. England & Wales "2 Years of Severe Injury in Children" January 2013-December 2014. United Kingdom. [Internet]. [Cited 2016 Nov 21]. Available From: https://www.tarn.ac.uk/Content/ChildrensReport2/files/assets/common/downloads/TARN%20Leaflet.pdf.

5. Falcone Jr RA, Rl Brown, Garcia VF. Disparities in child abuse mortality are not explained by injury severity. J Ped Surg. 2007; 42(6):1031-6. doi:10.1016/j.jpedsurg.2007.01.038

6. Lane WG, Dobowitz H. What factors affect the identification and reporting of child abuse-related fractures? Clin Orthopaedics Rel Res. 2007;461:219-25.

7. Thomas NJ, Shaffer ML, Rzucidlo S, Shirk BJ, Dias MS. Temporal factors and the incidence of physical abuse in young children: decreased non-accidental trauma during child abuse prevention month. J Ped Surg. 2007; 42:1735–1739. doi:10.1016/j.jpedsurg.2007.05.032

8. Kemp AM, Dunstan F, Harrison S, et al. Patterns of skeletal fractures in child abuse:systematic review. BMJ. 2008; 337:a1518. doi: http://dx.doi.org/10.1136/bmj.a1518

9. Töro K, Fehér S, Farkas K, Dunay G. Homicides against infants, children and adolescents in Budapest (1960-2005). J For Leg Med. 2010; 17: 407-411.

10. Bajaj M, Offiah AC. Imaging in suspected child abuse:necessity or radiation hazard? Arch Dis Child. 2015; 100: 1163–1168. doi:10.1136/archdischild-2015-308418

11. Davies FC, Coats TJ, Fischer R, Lawrence T, Lecky FE. Emerg Med J. 2015; 32: 921–925. doi:10.1136/emermed-2015-205285.

12. Government of India. Child Related Legislation. Ministry of women and Child development. Government of India. [Internet]. [Cited 2016 Nov 21]. Available From: http://www.wcd.nic.in/sites/default/files/JJAct2015.pdf

13. Government of India. Ministry of Law and Justice. 2012. Protection of Children from Sexual Offences Act 2012. [Internet]. [Cited 2016 Oct 07]. Available From: http://policewb.gov.in/wbp/misc/2013/22-11.pdf.

14. Kliegman MR, Behrman RE, Jenson HB, Stanton BF. Nelson Textbook of Paediatrics. 18th Ed. Philadelphia: Elsevier Saunders; 2007. Ch-36, Abuse and Neglect of children.

15. DiMaio VJ, Dimaio D. Forensic Pathology, 2nd Ed. Boca Raton: CRC Press; 2001. Chapter 12, Neonaticide, Infanticide and Child homicide.

Police Mandate and Functions in UP
- A study based on UP 100

Dr. Amit Thakre[*]

Abstract

The present study aims to assess the nature of policing work and categorize it based on event types. This shall provide an understanding of policing work within and beyond the policing mandate. The existing literature on the classification of policing work is predominantly done by American and British scholars showed that only 20-30% of policing work was related to crime, rest all fell under the category of '*potential risks*'. The key research question of the present study is 'whether the phenomenon of a major part of police work is beyond policing mandate stands true in Indian policing system as well?' This highlights a gap in the literature on empirical researches on Indian policing. Past studies in India has ignored the quantum of workload beyond policing mandate. The present study utilized UP 100 data to assess the workload of police and found that nearly 62.2% (3288383 cases in 2 months' time) of policing work in UP was beyond policing mandate. This finding calls for the integration of concerned stakeholders to act accountable and take steps to alleviate excessive workload over the police department. The present study also identified hot-spots, major categories of serious event types, time and seasonal patterns of major event types based on information shared by UP 100. This study has three aims; one, to establish grounds for well-informed police image amongst masses; two, to recommend replication of initiatives like UP 100 in the other States of India as well and; three, to integrate other relevant public service departments. This shall not only hold the concerned department accountable and reduce the burden on the police department but shall also improve the efficiency of the police department by rendering a focused approach towards core crime related issues.

Keywords:

Digital Map, GIS data store, Police Station Web Module, Police Supervisory Application, policing mandate, RoIP, UP 100, Stakeholders and Workload

Introduction: About UP 100

As of 2016, the population of UP was 220 Million. The area of UP is 240, 948 sq. km. with 75 districts, 16 Municipal Corporations, 689 Towns and Cities, 107452 Villages and 1562 police stations. If UP had been a Country, it would have been the 5th largest in the world. To manage such a huge population, UP-100 was established with a vision to provide prompt response to public distress calls across space and time, 24 X 7, round the year. This system is based on the integration of police-fire-medical services

Author Intro:

[*]   Assistant Professor, LNJN-National Institute of Criminology and Forensic Science, New Delhi.

to provide emergency response at anytime and anywhere in UP. For efficient communication between police and public, dedicated vehicles were deployed across the 75 districts in UP state. Special soft skills training was imparted to police personnel who come in direct contact and interact with the citizens in distress. UP has majorly 8 languages and all modes of communication were utilized for proper interaction. As a result of UP-100, police are taking 100% calls from the general public, responding politely and promptly to information received from the public. UP 100 is different from Dial 100 service on many levels. UP 100 is a 2-tier i.e. State and District level service. There is a well-established contact center which can be reached by the public via mobile call, social media- Twitter, Facebook, WhatsApp, email SMS, web or App whereas Dial 100 is only call based. UP-100 provides round the clock services and its monitoring and assessment is a continuous process which was absent in Dial 100 services. Due to UP-100 SoPs, the delivery of services is uniform across the state. UP-100 has made all the police services centralized, prompt and independent of the local police station. The impartial and regular monitoring of operations has made police more accountable for their actions.

The history of UP-100 is fresh as the foundation of Head-Quarters was laid in December 2015 and by November 2016; UP-100 finalized administrative approvals, signings of contracts and issuance of resources. The implementation in various districts started during December 2016 and by the end of January 2017 all the 75 districts had launched UP 100 in their jurisdiction. The implementation of UP 100 is done with the help of an advanced technology which involves Business Intelligence, Dashboard (an application created for the supervision of all the activities of UP-100 by the nodal and senior officer. This feature provides detailed and live information of all the proceedings. Senior officers can scrutinize the number of delayed FIRs and Non-Cognizable Reports, complaints registered against police and PRVs), Digital Map (UP Police collected information on digital maps of 1.07 lacs villages and then police stations and their jurisdictions were designated in these maps. The mapping of urban areas was also done to pin-point precision. The mapping of locations has made computerization of UP-100 more effective), Geographical Information System Data Store (UP police have developed an android application to collate GIS data store of rural and urban areas. During August and October of 2016, with nearly 11,000 resource persons in more than 1500 police stations, 28 lac points of identification were mapped on GIS. After data cleaning and quality assessment, nearly 15 lac points were integrated into UP-100 digital map), Intranet portal, Police station web module (all the police stations are connected to UP-100 via a convenient online interface. All the police stations can monitor all the recorded incidents in their jurisdiction from the computers installed in their respective police stations), Police Supervisory Application (all the senior level officers of UP Police shall be provided with new mobile application that shall provide information on all the UP-100 PRVs and incidents) , Radio over Internet Protocol (with RoIP, all the police personnel are connected with PRV and police stations on the radio network. RoIP also provides an option for video conferencing. RoIP is also integrated with digital GPS devices), Patrol Management System and E-learning Module (training related information shall be provided in E-learning option. The trainee officers shall also be able to learn via live streaming of lectures of e-module). The data center of UP-100 calls is stored in Lucknow, Uttar Pradesh whereas in case of a disaster situation, the data can be retrieved from a disaster recovery center located in Bengaluru, Karnataka.

The operational process of UP-100 can be subdivided into 3 categories, viz., sense, reach and secure. These three processes involve:

1. Sense: The public may sense the presence of UP-100 from various social media platforms. The calls made by the public are transferred to communication officers who interact in the required language and dialect with compassion. All call details are processed, recorded and recorded in secure database. Non-actionable calls are closed whereas actionable calls are transferred to Dispatch Officers who take necessary action as per Standard Operating Procedures. Apart from calls, citizens may also record the video of the incident and upload on UP-100 portal which will be available to the respective local police station for taking further necessary action.

2. Reach: The Dispatch Officer then forwards the information to Police Response Vehicle (PRV) and keeps local police informed. Once the PRV acknowledges the information, it immediately proceeds towards the scene of the incident. The PRVs are geographically distributed as per Patrol Management System to be at disposal of local police round the clock. So far, the UP-100 is operating 3200 Cars and 1600 Motorbikes in Uttar Pradesh. PRV vans are allocated as per geographic area, population density and non-residential regions like forest, river and barren lands. The relative placements of PRV are made in such a manner that it shall take on average 15 minutes in urban and 20 minutes in rural areas. The PRVs are assigned random patrolling routes daily which spreads across night and day shifts, streets and highway patrol. As per UP-100 mandate, a nodal officer is designated to supervise patrolling routes in rural and urban areas who shall also nominate resources based on the requirement of the situation. All the activities relating to the movement of PRVs are monitored through UP-100 App by Field Jurisdictional police officers. In case of emergency situations,

UP-100 App is designed to assist police in the identification of lost and unknown persons as well.

3. Secure: Once the PRV reaches the site of incidence or site of emergency, the area is protected to preserve evidence and maintain the sanctity of procedural investigation. Police also ensure to speak with the victim and if needed secure victim from troublemakers. Under UP-100, police are provided with more than 500 comprehensive standard operating procedures for various possible situations. In matters pertaining to the closing of the case, for minor cases, the police dispose of the case at the site and inform the local police. If needed the police may apprehend the offender and turn him/her over to the jurisdictional police station.

As part of the operational process, the PRV submits its Action Taken Report (ATR) to UP-100. To improvise the delivery of services and maintain accountability, the UP-100 also takes feedback from the complainant. The final ATR is then submitted to UP-100.

As per the event counts, as on Feb 2018, UP-100 has rendered assistance to 53,06,386 calls of which less than 5% calls were classified as high priority events. On average, UP-100 is handling nearly 12, 000 calls a day out of which nearly 500 are high priority events. On average, nearly 100 victims are hospitalized on daily basis. UP-100 received maximum grievances calls during Holi and Diwali (two major festivals in Hindu Calendar of India). UP-100 software also has an integrated feature to establish patterns of crime events based on call records. As on Feb 2018, the top 5 events in UP includes Dispute (majorly with neighbors or relating to property matters), Domestic Violence (majorly against senior citizens followed by female and child), Accident, Sexual Harassment and Theft. Hot spots of Domestic violence showed that it is majorly concentrated more towards the eastern

UP region. The distribution of incidents on time scale showed that maximum disputes occurred during 1800 Hrs. to 2200 Hrs whereas second maximum event pattern showed a high concentration of property disputes during 1000 Hrs to 1400 Hrs, female harassment during 1700 Hrs to 1900 Hrs and finally major domestic violence cases occurred during 2000 Hrs to 2300 Hrs (Source: UP-100).

Need for evidence based policing

Criminological research on policing has proven to be important across the world. Researchers used crime data to establish crime patterns over time and space continuum which has been helpful in doing evidence-based- effective policing. Such similar trends were also established in understanding patterns of offending and victimization. Further, the police data in American, British and European states are also used to conduct advanced level cross-sectional research to explore the correlation between seemingly unrelated variables. In India, there is a dearth of evaluation research on policing. This not only leaves many questions unanswered relating to the understanding of crime patterns but also makes it difficult to assess the effectiveness of policing. To fill this gap, media houses have taken the role of portraying police image to the masses. One of the major limitations of media portrayal of Indian policing is that it is majorly politically-opinionated driven approach rather than empirical based approach.

The democratic set up in India promotes a strong media presence across various platforms and this arrangement has made masses highly opinionated about issues relating to the Criminal Justice System. Police are one such subject of mass public scrutiny on daily basis. They are majorly viewed in negative lights by masses in India. Unfortunately, not much research has been done to demystify the complexity involved in police image formation in India. Media criticism of police is an outcome of select few incidents which were aggressively reported by media houses. Due to the lack of systematic research on policing in India, the police image is ill-formed and biased in nature. The importance of research for the betterment of policing in India has been largely neglected. However, the US has been successful in taking assistance from the academic institutions for improving their policing. Drawing from one such example of research-based policing in the US, in June 2009, the Court in Los Angeles cited paper findings published by the John F. Kennedy School of Government, Harvard University to release LAPD from Federal Government for better policing.

Police being the first respondent of the Criminal Justice System must face greater wrath of public criticism. It may be likely that the superficial examination of policing by media may depict the problems rooted in the system but that does not imply that these are causes leading to failure of policing. With this problem at hand, the author of this paper is of the view that a systematic research is required to ascertain the credibility behind the negative police image in India. For that, the author examined UP-100 policing scheme which is one of its kind initiatives in the country and has a rich repository of distress calls made by citizens to seek assistance from the police. The objective of this study is to classify the nature of policing work which has recently been also called as 'economics of policing' by academicians and practitioners. The classification shall be done to assess the nature of policing work and understand the quantum of work done by the police beyond their mandate. This shall have two benefits; one, it would help in presenting a well-researched examination of police work to shape well-informed police image among masses and second, the excess workload identified as beyond police mandate shall be resolved by roping in concerned stakeholders/ public service department.

Economics of policing is a wider term that covers police accountability, operational cost, resources available to meet the demands and budget allocated to the police department (Griffiths et al., 2015). The study of the economics of policing requires rich data on diverse variables (Kempa, 2014) which is available with UP-100 police repository.

Mr. J. Ahmed (personal communication, 2018) being the former Chief Police Officer of Uttar Pradesh State Police expressed concern over the excess burden over police services. The similar concern was resonated in findings of the previous empirical research done by Demers et al., (2007) which showed that only 20-30% of police work was related to criminal incidents and rest all is beyond policing mandate, imposed upon policing system due to failure or incompetency of other public service departments. The assessment of police work by Demers et. al., was done by calculating the incident wise percentage of policing working hours and by examining calls for services made by citizens in distress. The findings of Demers et al. study shows that police are overburdened and doing nearly 70-80% of work that is supposed to be done by other public service departments.

The issue regarding policing work is not exclusive to the 21st century but was raised earlier as well. The National Police Commission (NPC), Government of India in its reports published between 1979 to 1981 recommended numerous reforms in Indian police system. Following are the major recommendations of NPC reports relating to policing mandate (Source: Humanrightsinitiative website):

a)   2nd Report of NPC: To appoint 'Criminal Justice Commission' to ensure that all the pillars of CJS functions with accountability. Also, to appoint 'State Secretary Commission' in each State to formulate guidelines for police duties that shall be service oriented as per the provisions in the Constitution or laws. This is to protect police system from external influences/interferences.

b)   3rd Report of NPC: To protect weaker sections, it was recommended to establish special investigation cell at the State level. Also, there shall be a provision for adequate funds at police station level for legitimate expenditures required on routine basis.

c)   5th Report of NPC: It was recommended that in areas where police department require active cooperation from other department and concerned stakeholders, the District Magistrate shall act as the 'Chief Coordinator'.

The recommendations of NPC reports were not implemented in principle by any State in India due to vested interests. This has led to unprecedented burgeoning of workload on police department in India.

Webster (1970), Reiss (1973) and Ryan (2003) in their study in rural and urban areas made an anecdotal claim that only 30% of police work comprises crime related activities. Similar to J. Ahmed's concern mentioned above, Dale McFee (former Head of the Canadian Association of Chief of Police) stated that 70-80% calls to police were beyond their mandate (McFee, 2013). Also, the Royal Canadian Mounted Police in British Columbia recently reported that only close to 30% of incidents reported to police are crime related (Institute for Canadian Urban Research Studies aka ICURS, 2014). The patterns in the US, UK, and Canada show that a limited number of calls made to police are criminal in nature. However, there is a lot of subjectivity behind 'what is considered as criminal activity?' and 'what is the scope of police mandate?' The present research shall be addressing the subjectivity associated with police mandate in

data interpretation part. Further, considering the concern raised repeatedly by veteran police chiefs from different countries, an attempt has been made in this research paper to identify and discuss event types within and beyond the scope of policing mandate.

The scenario is the same for India as well wherein police department is heavily criticized without considering the big chunk of work done by the police which is beyond its mandate. It may seem that the police mandate in India is wider and overlapping with the mandates of other public service departments. The negative criticism of police services in India may not only due to ignoring accountability from other public service departments but also harboring higher expectations from police departments by the public. However, this is found to be a universal phenomenon wherein public expectations from police have increased manifolds (Caputo and McIntyre, 2015). A clear understanding of the nature of policing work shall readjust public expectations from police to a justified level. There is no systematic study on the nature of policing work in India and the present study is aimed to fill that gap.

As per Bureau of Police Research and Development, Government of India, the role of police is to uphold rule of law, protect citizens, preserve public order and to prevent crimes (BPR&D report, 2017). Prevention of Crime has a wider scope in society and it may not be achieved without optimal performance and collaboration by other agencies as well. In India, maintaining order solely by police is a complex problem because poor delivery of public or health care services also poses a threat to peace and order in both rural and urban settings. It is evident from here that failure of any public service delivery system shall put excess burden over the policing system. Vaughan et al. (2016) in their study stated that due to the failure of the State to effectively deal with mental health cases

mostly lead to criminality when the condition of the patient gets worse. This puts the excess burden of mental illness induced criminality over the police which are otherwise preventable if better health care systems were in place. It goes the same for education, environment, public social services, and transportation system.

This paper intends to understand the nature of the police job in the Uttar Pradesh State. To ascertain the classification of police work, the author examined data repository of UP-100. The data comprises calls for police service from different phases (based on the availability of data); 20 November 2017 to 8 February 2018 (Duration: 2 months 19 days) and graphical images below represent data from 20 November 2016 to 7 February 2018 (1 year 2 months 19 days). Through this research papers, the author addresses the following research questions:

- To understand the classification of services provided by the UP police based on citizen's calls received by UP100?

- What percentage of work done by UP Police is beyond policing mandate?

- To identify hot spots with their area-wise distribution of patterns of calls for police service.

The aim of this study is not to scrutinize or undermine any of the services provided by the police but to raise the areas concerned and event types that shall require the attention of public service organizations concerned. To call for departments concerned to gear up and put in efforts to reduce burden over the police department.

Event Type Classification

The data received from UP-100 for the period 20 November 2017 to 08 February 2018 (2 months and 19 days) were classified into more than 60

event types by UP-100 and further subclassified into nearly 250 categories. However, the researcher, keeping in view the objectives of the present study, performed data cleaning for simplification of event types which led to a reduction of event types to 50. Regarding the confidentiality of data and terms of condition with UP100, the researcher shall not divulge information obtained from UP100. However, for the purpose of understanding policing work within and outside policing mandate, UP-100 data was interpreted from a broader perspective by adopting the inductive approach. The specific event type wise data shared by UP100 was used to draw a conclusion pertaining to the quantum of police work beyond the mandate.

The major event types examined for the purpose of this research included cases relating to Accident, Animal-Related, Assault/Riot/Commotion, Attempted Murder, Child victimization, Cybercrimes, Dispute, Domestic Violence, Economic crimes, Female harassment, Fire, Forgery, Gambling, Robbery, Theft, Threat and Traffic Jam. There are such other categories of event types as well, amounting to a total of 50 different types of event heads. The data revealed numerous event types that were out of policing mandate or found to be ignored by other stakeholders concerned. These include accidental explosives, fire and firing accident, road accident and traffic jam, animal-related issues, copying in the examination, matters related to differently abled people, dispute, domestic violence, encroachment, gambling, missing persons, information registered against other government departments, mobile assisted crimes, pollution, and lifesaving related issues.

Event types falling beyond policing mandate are interpreted from a wider perspective. In Table 1 below, the non-core policing event types are identified along with their respective public service departments concerned (the non-core policing events, public service department concerned and their mandates). This amounts to 3288383 calls for service beyond police mandate which is 62.2% of all event types. As per UP 100 data for the period 20 November 2016 to 07 February 2018, the UP Police have rendered assistance in 5306386 cases out of which 13249 events were high priority events, i.e. only 3.3% which means remaining 44% are core policing events with moderate priority type. This shows that most public distress calls are non-core policing work (62.2%), putting the unsolicited burden on the police department.

Table: 1 List of 'non-core policing' event types derived from UP100 data, comparison with US/UK and identifying concerned departments in India that needs to deal with 'non-core policing' work.

S. No.	Non-core policing event type	Concerned organizations in U.S./U.K. dealing with it	Concerned Departments in India shall be dealing with it	Mandate of the concerned department in India with respect to event type
1.	Accident Explosive	Bureau of Alcohol, Tobacco, Firearms and Explosives (US)	Petroleum and Explosives Safety Organization, Ministry of Commerce & Industry, Govt. of India	'under the *Explosives Act 1884* and *Petroleum Act 1934* and the rules made there under related to *ensure public safety in the areas of manufacture, transport, storage, handling, etc. of explosives*' (Source: www.peso.gov.in)

S. No.	Non-core policing event type	Concerned organizations in U.S./U.K. dealing with it	Concerned Departments in India shall be dealing with it	Mandate of the concerned department in India with respect to event type
2.	Fire and Firing Accident	The US Fire Administration (US) Fire and Rescue Services, England	Directorate of Fire Services (State Government)	As per United Provisions Fire Service Act, 1944 (*U.P. Act No. 3 Of 1944*), *'to improve the fire-fighting arrangements in certain towns of this Province and, in particular, to constitute and maintain a Provincial Fire Service for staffing and operating the fire brigades in those towns'*
3.	Road Accident and Traffic Jam	U.S. Department of Transportation's *Federal Highway Administration* & U.K. Department for Transport	Ministry of Road Transport and Highways (MoRTH), Govt. of India MCD, State Government	MoRTH also administers 'The Control of National Highways (Land & Traffic) Act, 2002'. Also, as part of mandate, MoRTH *'Collects, compiles and analyses road accident statistics and takes steps for developing a Road Safety Culture in the country by involving the members of public and organising various awareness campaigns.'* As per Chapter 5, Section 114 (29, 30, 31) of Municipal Corporation Act (1959), to ensure smooth exchange of traffic and maintenance of traffic signs.
4.	Animals related	Animal Control Services, U.S. (for example, New York's American Society for the Prevention of Cruelty to Animals) & Wildlife Removal and Pest Animal Control, U.K.	Lucknow Municipal Corporation	As per Chapter 5, Section 115 (22) of Municipal Corporation Act (1959), the responsibility of officials of municipal corporation is also to confine and control animals causing nuisance.

S. No.	Non-core policing event type	Concerned organizations in U.S./U.K. dealing with it	Concerned Departments in India shall be dealing with it	Mandate of the concerned department in India with respect to event type
5.	Copying	U.S. Department of Education & U.K. Department of Education	Department of Higher Education; and Department of School Education and Literacy, Ministry of Human Resource Development, Govt. of India and Department of Higher Education and Secondary Education, Govt. of UP	The exam board of secondary and higher education is responsible for monitoring and prevention of copying during examinations. The effective preventive measures involve online registration and allocation of examination centers; and installation of CCTVs in examination centers.
6.	Differently abled people	Office for Disability issues, U.K.	Department of Empowerment of Persons with Disabilities (DoEPD), Ministry of Social Justice and Empowerment, Govt. of India	'The DoEPD facilitates empowerment of the persons with disabilities. These include persons with Seeing, Hearing, Speech, Movement, Mental Retardation, Mental Illness, Multiple Disability and any other disabilities.' (Source: www.diabilityaffairs.gov.in) As per Chapter 5, Section 115 (1) of Municipal Corporation Act (1959), covers taking care of infirm, disabled or handicapped and providing them shelter in appropriate State's institution
7.	Dispute	Alternate Dispute Resolution, U.S. Department of Labour	For matters relating to dispute between workers & laborers- Ministry of Labour and Employment	Mandate of MoLE provides *welfare measures, regulating conditions of work and strengthening enforcement of labour laws'.* (Source: https://labour.gov.in/mission)
			For matters relating to dispute due to parking, green tree chopping, road rage, road digging, sewer and neighbor dispute- MCD	For matters pertaining to maintenance of residential areas (found to be major cause for dispute cases) lies with the Municipal Corporation Department. As per Chapter 5, Section 114 (3 to 9) of Municipal Corporation Act (1959) covers maintenance of residential areas related clause.

S. No.	Non-core policing event type	Concerned organizations in U.S./U.K. dealing with it	Concerned Departments in India shall be dealing with it	Mandate of the concerned department in India with respect to event type
8.	Domestic Violence	Office on Violence Against Women, The U.S. Department of Justice For matters pertaining to domestic violence and abuse dealt by Department for Work and Pensions (DWP), Home Office, U.K.	Ministry of Women and Child Development (MoWCD), Govt. of India	The mandate of MoWCD promotes empowerment for women to live in environment free from violence. The Protection of Women from Domestic Violence Act, 2005 provides *'protection of the rights of women guaranteed under the Constitution who are victims of violence of any kind occurring within the family and for matters connected therewith or incidental thereto.'*
9.	Encroachment	U.S. Immigration and Customs Enforcement;	MCD	As per Chapter 5, Section 114 (24) of Municipal Corporation Act (1959) covers removal of obstruction or projections in public spaces. This shall extend to dealing with encroachment as well.
	Gambling	U.S. Department of Revenue; &	Department of Revenue, Ministry of Finance And Reserve Bank of India	Regulating use of crypto or virtual currency (ex. bitcoins) used in funding online gambling
			MCD, State Government	As per Chapter 5, Section 114 (19) of Municipal Corporation Act (1959) deals with regulation and debarring professions of dangerous nature.
	Missing	Department of Justice	National Tracking System for Missing, Ministry of Women and Child Development, Govt. of India	-
10.	Information against other Government Department	-	Concerned Government Department to take disciplinary or legal action against defaulter as mandated in respective Act/Rule book.	-

S. No.	Non-core policing event type	Concerned organizations in U.S./U.K. dealing with it	Concerned Departments in India shall be dealing with it	Mandate of the concerned department in India with respect to event type
11.	Mobile assisted Crimes	Cyber Division, FBI Head Quarter, U.S. National Cyber Crime Unit, U.K.	Telecom Regulatory Authority of India, Department of Telecommunications, Ministry of Communications, Govt. of India And Headquarters of Social Networking Sites in providing requisite information pertaining to cyber criminal	-
12.	Pollution	U.S. Environmental Protection Agency Department of Environment, Food and Rural Affairs, U.K.	Central Pollution Control Board, Govt. of India	As part of its mandate *'Plan and cause to be executed a nation-wide programm for the prevention, control or abatement of water and air pollution'* (Source: http://cpcb.nic.in/functions/)
13.	Life saving	Life Saving and Fire Safety Division, United States Coast Guard, U.S. Dept. of Homeland Security	MCD	As per Chapter 5, Section 114 (2) of Municipal Corporation Act (1959) states for securing dangerous/risk prone buildings or areas.

The second objective of the present study is to understand the area wise distribution of patterns of calls made by citizens for police services. As per UP-100 data on event types (20 Nov' 2017 to 08 Feb' 2018), the major event types in UP were Dispute (1503515), Domestic Violence (844252), Dispute (468801), Accident (373621), Female Harassment (332362), Attempted Murder (163879), Gambling (133461), Threat (102718) and Traffic Jam (101674).

The district wise event count for top 20 event types is mentioned below:

Table 2: District wise major event counts in UP (Source: UP 100 Data)

S. No.	District	Type	Event Count
1.	Lucknow	Dispute	30336
2.	Kanpur City	Dispute	21173
3.	Ghaziabad	Dispute	18234
4.	Gautam B. Nagar	Dispute	17247
5.	Lucknow	Domestic Violence	14279
6.	Meerut	Dispute	13668
7.	Kanpur City	Domestic Violence	11859

S. No.	District	Type	Event Count
8.	Lucknow	Accident	9074
9.	Kanpur Rural	Dispute	8947
10.	Lucknow	Theft	8510
11.	Ghaziabad	Domestic Violence	8402
12.	Ghaziabad	Theft	8353
13.	Meerut	Domestic Violence	7791
14.	Lucknow	Traffic Jam	6428
15.	Ghaziabad	Accident	6280
16.	Gautam B. Nagar	Theft	6199

S. No.	District	Type	Event Count
17.	Gautam B. Nagar	Accident	6011
18.	Kanpur City	Accident	5737
19.	Ghaziabad	Traffic Jam	5482
20.	Kanpur City	Theft	5445

In table 2 above, 'dispute' was found to be a major contributor in event types in Lucknow (30336), Kanpur City (21173), Ghaziabad (18234) and G B Nagar (17247). Table 3 below further illustrates on the major events types and their percentage share in 6 Districts of UP.

Table 3: UP top 6 Districts and their share of major event types (Source: UP 100)

S. No.	District	Total Events	Highest contributing event		2nd Highest contributing event	
			Type (Count)	Percentage share	Type (Count)	Percentage share
1.	Lucknow	105842	Dispute (30336)	28.7%	Domestic Violence (14279)	13.5%
2.	Kanpur City	72254	Dispute (21173)	29.3%	Domestic Violence (11859)	16.4%
3.	Ghaziabad	69498	Dispute (18234)	26.2%	Domestic Violence (8402)	12.1%
4.	GB Nagar	52757	Dispute (17247)	32.7%	Theft (6199)	11.8%
5.	Meerut	50095	Dispute (13668)	27.3%	Domestic Violence (7791)	15.6%
6.	Kanpur Rural	25993	Dispute (8947)	34.4%	Domestic Violence (4779)	18.4%

The district wise event count (data available for the period January 2017 to July 2017) showed that Lucknow (105842), Kanpur City (72254), Ghaziabad (69498), Gautam Buddha Nagar (52757), Meerut (50095) and Kanpur Rural (25993) are top 6 areas in terms of highest number of calls for service made by citizens. The grand total wise top 10 events recorded in Uttar Pradesh were: Dispute (824025), Domestic Violence (397284), Property Dispute (228140), Accident (147607), Theft (140799), Female Harassment (117106), Gambling (63088), Attempted Murder (52876), Traffic Jam (44216) and Female Sexual Harassment (42297).

The UP 100 software has a unique ability to customize its data analysis to render to the ad-hoc needs of result-oriented policing. For example, as per UP 100 data, from 20 November 2016 to 7 February 2018, the top 10 events in UP came out to be Dispute, Domestic Violence, Property Dispute, Accident, Female Harassment, Theft, Attempted Murder, Gambling, Traffic Jam, and Threats. These events are also documented on hot-spots giving a pictorial overview of the concentration of a problem. The figures below indicate the hotspots of two major event types in UP, i.e Dispute and Domestic Violence.

Figure 1: Hot spots of Dispute in UP
(20 Nov 2016 to 7 Feb 2018) *(Source: UP 100)*
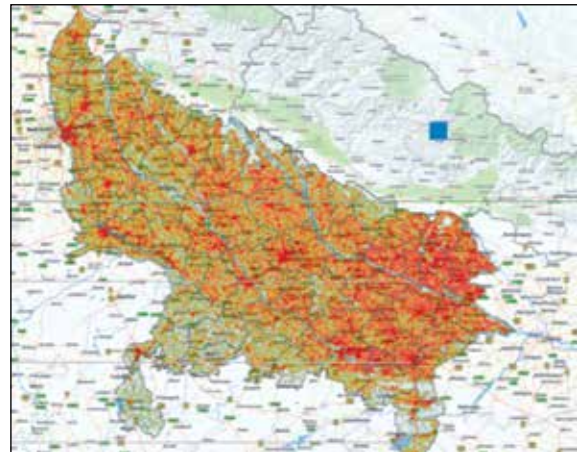
Figure 2: Hot spots of Domestic Violence in UP
(20 Nov 2016 to 7 Feb 2018) *(Source: UP 100)*

The hot spots of Dispute and Domestic Violence on UP Map show their higher concentration in the lower eastern region of UP.

The advanced software available with UP-100 is capable of live broadcasting Police Response Vehicle on UP map, call patterns and events attended by UP 100, estimate police response time, assessing nature of crimes against women, plotting of event types on 24-hour timescale. This feature is vital in effectively strategizing existing resources with the UP Police for optimal performance and efficient policing. The sample excerpts from UP-100 data analysis are discussed below in brief.

Figure 3: Screenshot of PRV deployment in UP State

(Source: UP-100)

The PRV deployment can further be located at the level of district, police station and village boundaries.
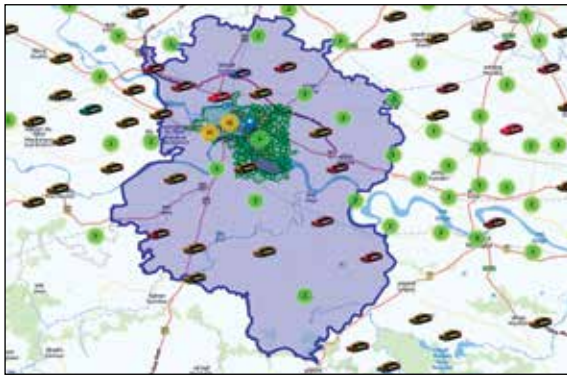
Figure 4: PRV deployment at district, police station and village boundaries level *(Source: UP 100)*

Figure 5: Events attended by UP 100
(20 Nov 2016 to 07 Feb 2018) *(Source: UP 100)*

The event type category-wise distribution of calls shows peaks during Holi and Diwali festivals. Such insights are crucial in strategically deploying PRVs as a form of predictive policing.
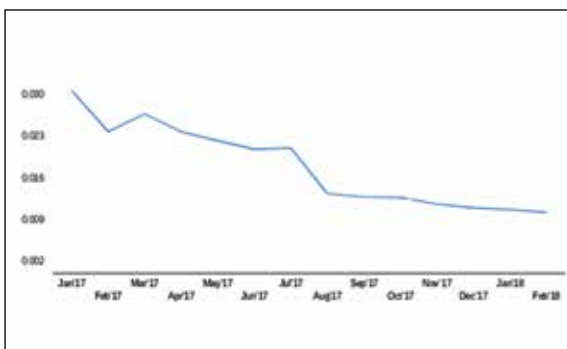
Figure 6: Police response time
(7 January 2017 to 7 February 2018) *(Source: UP 100)*

In past one year, the police response time of UP 100 has reduced from average 30 minutes to 15 minutes in urban and 20 minutes in rural areas.

Figure 7: 24 Hour time plotting of event types

Source: UP 100

In the figure above, it is apparent that dispute is a major form of event types which starts escalating from 0600 Hrs up until 2300 Hrs and then it starts declining. However, after disputes, various forms of events take peaks during different time zones. Such as, neighborhood disputes were found to be higher during 0600-1600 Hrs, followed by female harassment during 1700-1900 Hrs and night time is dominated by domestic violence from 2000-2400 Hrs.

The graphical information illustrated above shall be useful for integrating with concerned stakeholders and strategically channelizing resources based on event types hot-spots, marking basecamp for PRVs, peak seasons, improving police response rate and 24 hrs time wise incident rate.

Discussion

UP 100 data showed that police are dealing with only 3.3% of high priority events, rest 96.7% are medium or low priority events. Police are majorly burdened with events which are beyond policing mandate. Wuschke et. al. (2017) in their study on UK police data of 14 years found such similar results, wherein, UK police work comprises only 20-30% of crime-related work, remaining fell under the category of 'potential risk'. The potential risk is a broad term, and this

involves the role of other stakeholders as well. This problem needs to be acknowledged before forming the police image and be resolved with advanced measures for effective policing and ensuring a safer society. It is proposed that the model of UP 100 needs to be extended to further integrate public services departments, institutions, centers, and concerned ministries. The UP 100 data shall be utilized to highlight the problem areas and issues that demand attention on a priority basis by holding public service departments concerned accountable. Presently, UP 100 has integrated health and fire services, it shall be useful if UP 100 further integrate Electricity, Education, Environmental Protection, Public Broadcasting, Public transportation, Waste Management, Water Supply and all the relevant department under State and Central public services framework.

The integration of other public services is more important because looking at the crime trends in UP in the last 10 years, it is rising exponentially. According to NCRB Report (2007 to 2016), the crime rate in UP has increased to 61% in the last 10 years, as shown in the figure below. This shows a significant increasing trend and it has also led to a subsequent increase in public demand for police services. However, assessing police workload based on only crime rate may be misleading because police in UP are dealing with work beyond police mandate which may also be increased considering exponential rise in UP population (from the year 2001 to 2011, the population of UP rose from 16.62 Cr. to 19.98 Cr. respectively; an increase by 12% in 10 years). Also, research shows that with an increase in population the crime rate may appear less, but it puts consistently increasing pressure on the policing system (Wuschke, et. al., 2017).
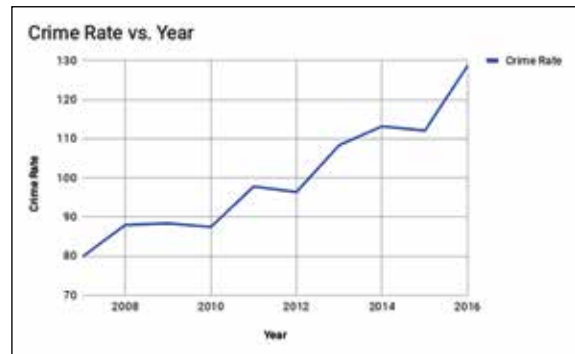
Figure 8: IPC crime rate during last 10 years in Uttar Pradesh State (2007 to 2016)

Source: Crime in India Report (2007 to 2016)
Website: ncrb.gov.in

Apart from that, the forms and intensity of crimes have evolved, needing more specialized police services. Wuschke et. al. (2017) in their research found that with increasing complexity in event types, the police are facing an increasing workload from incidents which are beyond police mandate. The National Crime Records Bureau Report (2016) stated that a total number of cognizable crimes in India were 48,31,515 out of which Indian Penal Code (IPC) crimes were 29,75,711 and Special & Local Laws (SLL) crimes were 18,55,804. The Indian police were established to deal with IPC crimes only, have dealt with SLL crimes as well which constituted nearly 38.4% of all crime incidents in the year 2016, consuming significant working hours of policing in India. The crimes under the SLL category cover issues pertaining to dowry, domestic conflict or municipal laws. In such situations, it is important that the major chunk of police burden shall be redistributed to other stakeholders to allow police to do their job in a more focused and specialized manner. In words of Balachandran (2017), "It is not because of the lack of policemen that we are unable to maintain public order, but due to the use of the police for non-police duties. There will be no improvement in performance unless the workload is lightened, and responsibility diversified."

Recommendations

The aims of present study were to encourage research on policing, replicate UP 100 model and integrate other relevant departments. Keeping in aims and major findings of the present study in mind, it is recommended conducting evidence based policing in India. The police departments have to collaborate with academic institutions to start joint projects and publish findings on regular basis. Secondly, the work done by the police beyond its mandate need to be classified and accountability to perform shall be fixed on respective department concerned. The District Magistrate shall be chief coordinating authority (as mentioned above w.r.t 5th report of NPC). The mobilization of stakeholders concerned needs to be intensified during Holi and Diwali (duration when public grievances calls reach at peak). However, during routine phase, Municipal Corporation, civil society groups, State and National level Commissions for vulnerable sections need to be integrated with police services during 1000 Hrs to 1400 Hrs and 1800 Hrs to 2200 Hrs for effective crime control and prevention. The duration of integrated services may be further extended depending on crime trend analysis. The response time to public distress call is positively correlated with distribution of responsibility. From 2016 to 2017, UP-100 PRV response time reduced from 30 mins to 15 mins. The integrative service system shall further reduce response time. The concept of integrated services may be initiated in phase wise manner. Phase-I to include Lucknow, Kanpur City, Ghaziabab, Gautam Buddha Nagar, metrut and Kanpur rural (top 6 districts with highest number of distress call reported to UP-100).

Presently, UP-100 is deploying PRV based on hot-spots of distress calls. It is recommended that a further analysis be done to examine the phenomenon of 'displacement of crime' and 'diffusion of benefits'. The police-

academician partnership shall also test existing criminological theories relating to policing in India. This intellectual exercise shall improve the effectiveness of strategic placement of PRV in future and add to the existing criminological knowledge on evidence based policing in India.

Conclusion

The police perform their duty beyond the framework of its mandate, respond to those incidents also which are vaguely associated with maintaining order and upholding the welfare of citizens. As crime rate is an ever-rising trend and police are heavily criticized, apart from studying causes behind crimes, it becomes even more important to understand the nature of policing work as well. V. Balachandran (former IPS officer, Maharashtra Cadre) in his recent empirical based article published in the Outlook Magazine (4 Dec 2017) stated that the dual responsibility of investigation and managing internal security is putting Indian police under extreme pressure. Balachandran in his article emphasized the problem of police overburdened with non-policing function. The police in India are asked to demolish structures, resolve encroachments, collect fines, issue licenses, deal with stray animals, dead bodies, beggars, protect environment from human activities, regulate entertainment, detect modern forms of vices, keep watch over social networking sites, render assistance to political intelligence, protect installations of public importance, serve summons, escort citizens entrapped in the cycle of the Criminal Justice System and maintain internal security. There is a need for rationalization of policing functions.

This paper aimed at understanding the nature of policing work and identifying locations in UP that need immediate attention. This analysis was possible with the help of data provided by UP 100. The findings of the paper highlight that

'with the data like UP 100, it is now possible for Indian police to categories policing work in order to understand the distribution of event types and rope in sister public service departments to assign event types to respective organizations'. This shall not only hold the department concerned accountable and reduce the burden on the police department but shall also improve the efficiency of the police department by rendering a more focused approach towards core crime related issues. As per UP 100 data, only 3.3% event type falls under 'high priority events'. Also, out of 51 categories, 18 major event types were evidently beyond policing mandate (Table 1 above), which constitutes to an extra 62.2% of workload (i.e., 3288383 cases). Given the rising complexities of event types, unless other stakeholders are integrated and held accountable, the burden on UP Police is less likely to reduce.

The spatiotemporal analysis of the area-wise distribution of event types in UP showed the highest concentration of crimes in lower southeast region of UP. Such insights are developed with the help of data available with the UP 100, which is a major development in Indian Policing System. The data provided by UP 100 is not only helpful in categorizing policing work but also provides useful information for doing predictive policing in near future, the work on which has already been taken by Sh. Javeed Ahmed, Dr. Arvind Verma and UP 100 Team. This exercise shall be useful for future researches in India as well to explore ways to improve policing services for a better society.

Acknowledgment

Endnote

The website of UP 100 is http://up100.uppolice. gov.in/ ; the citizen app of UP-100 is available at google play store http://up100.uppolice.gov. in/en/pages/AppDownloadSuggestion.aspx   ; email id of UP-100 is up100-up@gov.in; Twitter account is twitter.com/up100 and facebook address is facebook.com/callup100

References

Ahmed, J. (2018, February 9). Personal Communication.

Balachandran, V. (Dec 4, 2017). What's to be done with our cops? *The Outlook Magazine*. Retrieved on 15th Feb 2018 from https://www.outlookindia.com/ magazine/story/whats-to-be-done-with-our-cops/299556

Bureau of Police Research and Development Report. *Functions, Roles and Duties of Police in General*. Retrieved from http://bprd.nic.in/WriteReadData/ userfiles/file/6798203243-Volume%202. pdf on 9th June 2018.

Caputo T and McIntyre ML (2015) Addressing role and value in policing: toward a sustainable policing framework. Policing: An International Journal of Police Strategies & Management 38(2): 265–278.

Demers S, Palmer A and Griffiths CT (2007) Vancouver Police Department patrol deployment study. Vancouver, BC: Vancouver Police Department. Available at: http://vancouver.ca/police/assets/pdf/ studies/vpd-study-patrol-deployment.pdf (Accessed on 10 June 2018).

Griffiths CT, Pollard N and Stamatakis T (2015) Assessing the effectiveness and efficiency of a police service: the analytics of operational reviews. Police Practice and Research 16(2): 175–187.

Institute for Canadian Urban Research Studies (2014) Economics of Policing: Complexity and Costs in Canada, 2014. Burnaby, BC: Institute for Canadian Urban Research Studies.

Kempa, M. (2014) Understanding the Historical Relationship Between Economics and Change in Policing: a Policy Framework.

Canadian Police College Discussion Paper Series. Ottawa, ON: Canadian Police College.

McFee D (2013) Standing Committee on public safety and national security. 41st Parliament, 1st session, January 31. Available at: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId¼5950911&Language¼E&Mode¼1#Int-7860663 (accessed 17 January 2017).

Reiss AJ Jr (1973) The Police and the Public. New Haven, CT: Yale University Press.

Ryan JF (2003) Community policing and the impact of the COPS Program: A potential tool in the local war on terrorism. In: Roberts AR (ed.) Critical Issues in Crime and Justice, 2nd edn.Thousand Oaks, CA: SAGE, 134–147.

Some selected recommendations of the National Police Commission. Common Wealth Human Rights Initiative website. Retrieved from http://www.humanrightsinitiative.org/old/index.php?option=com_content&view=article&catid=91%3Ashiva&id=746%3Apolice-reforms-indiathe-national-police-commission-npc&Itemid=100 accessed on 21 Nov 2018.

Vaughan AD, Hewitt AN, Andresen MA and Brantingham PL (2016) Exploring the role of the environmental context in the spatial distribution of calls-for-service associated with emotionally disturbed persons. Policing: A Journal of Policy and Practice 10(2): 121–133.

Webster JA (1970) Police task and time study. Journal of Criminal Law, Criminology and Police Science 61(1): 94–100.

Wuschke, K, E., et. al. (2017). What do police do and where do they do it? International Journal of Police Science and Management. 1-9. Sage Publication. DOI: 10.1177/1461355717748973

Drones - A new frontier for Police

Pankaj Kumar Singh[*]
IPS (Raj : 1988)

Abstract

Remotely Piloted Aircraft systems or UAV's or Drones are being used the world over for a variety of purposes today. Made popular by the usage of drones for combat purpose by the US Air Force, drones today are being used extensively by governments, individuals and corporates in law enforcement, agriculture, mining, oil and gas industry, sports, media, for delivering packages and might even begin to carry passengers in the near future.

The government of India has lately come up with a new Policy to govern the flying of drones in the country. This policy aims to regulate the operations in a manner to ensure a high level of safety for the aviation sector while at the same time facilitating commercial usage of drones also. The possibilities of usage of drones are endless and will only be limited by the creative potential of its users. However, along with the right kind of users, another category of rogue users has also come forth who are coming up with anti-social, nefarious and negative uses of this technology. To counter all this a number of Anti-Drone technologies have also evolved. How the government is able to keep tabs on all the creative churnings in this area by tweaking its policy at regular intervals, only time will tell. But the fact remains that this new technology is indeed a game changer and its right usage can not only cut down on time and costs but also help in optimal decision making.

The recently announced policy by the Ministry of Civil Aviation has aroused the interest of one and all in Remotely Piloted Aircrafts (RPA) or Remotely Piloted Aircraft Systems - better known as *UAV's* or **Drones**.

The term **drone** is widely used as a name given to an unmanned aircraft system which includes a ground control station, data link, support equipment and a remotely piloted aerial vehicle. Some other similar terms which are used for drones are Unmanned Aircraft Vehicle System (UAVS), Remotely Piloted Aircraft System (RPAS) etc. Thus, drone basically implies a system that does not carry a human operator, is remotely operated from ground, is at times expendable or even catered for multiple uses and may or may not carry a lethal payload.

The Government of India has been operating military drones for quite some time. These military drones do not carry lethal payloads for

---

Author Intro:

[*] Additional Director General of Police, Rajasthan Jaipur, Rajasthan.

attacking or neutralizing the enemy forces. The common knowledge of public regarding drones is largely shaped by the use of military drones by the US Air Force. The US today has more than 10,000 military drones - carrying out operations in Afghanistan, Pakistan, Iran, Syria and other places through their long range Global Hawk, Predator and Reaper drones.

For the sake of simplicity, this article will henceforth use the term 'drone' only wherever they are addressed by other names also as UAVS/ UAV/ RPAS etc.

I.   Drone Policy in India

The Directorate General of Civil Aviation announced a policy on the 27th of August 2018 for the operation of civil remotely piloted aircraft systems. This policy came into effect on the 01st of December, 2018 and it has categorized drones into five different kinds of civil systems as per their weight categories :

- Nano   -   Less than or equal to 250 gms.
- Micro   -   more than 250 gms to 2 kgs.
- Small   -   more than 2 kgs to 25 kgs.
- Medium -   more than 25 kgs to 150 kgs.
- Large   -   More than 150 kgs.

Civil aviation requirements are applicable on all civil remotely piloted aircraft systems. The new policy talks about a *Unique Identification Number* (UIN) in order to uniquely identify any drone. This UIN will be issued through a Digital Sky Platform. The drones in Nano category and those operated by intelligence and security agencies are exempted from obtaining UIN.

The new policy also mandates the requirement of *Unmanned Aircraft Operator Permit* (UAOP) which will be required for those using small, medium and large drones. All such persons should be 18 years of age or older, should have passed the class 10th exam in English and should have

undergone practical training. The new policy is very conscious of the safety requirements by insisting that all drones, except those in the Nano category, be equipped with horizontal and vertical positioning system, automatic flight termination mode, returning to home option, have anti-collision lights, SIM card based real time tracking, fire resistant UIN and also flight data logging capability. The Indian Air Force and Airports Authority of India have been given the responsibility to coordinate and monitor the movement of drones in the entire country. The loss of any drone is to be immediately reported to local police, BCAS and DGCA. All drone operations must be done during day time and that too within the *Visual Line of Sight* (VLOS) only.

The drone operators, except those in Nano and Micro category, are required to file their flight plan at least 24 hours before the actual operations to the authorities concerned and also inform the local police formations in writing prior to commencement of their operations.

The policy has listed out certain restricted areas in metros, near civil airports, defence installations, international border, sea coasts etc. which are out of bounds for all drones. No aerial photography or remote sensing can be carried out in these areas. In case any violations are noticed, DGCA can suspend the UIN or approach police for the registration of a police case under appropriate provisions of Indian Penal Code, Aircraft Act-1934 or Aircraft Rules- 1937- as the case may be.

Task Force

The Government of India has also constituted a *Task Force* to come up with a road map for further development of Drone/ UAV technology in the country. This task force comprises government officials, industry experts and certain special invitees depending upon their area of specialization. This task force was formed on

the 11th of April, 2018 - has its headquarters in Ministry of Civil Aviation, New Delhi- and was to submit its report within six months. Their recommendations will apply to Central Government, State Government, industry and other research institutions.

Past Policies

Historically speaking, the first policy in India to talk about civil remotely operated aircraft systems came up in the year 2014. This policy talked about the civilian use of drones in the field of agriculture, natural calamities, survey of infrastructure as in power lines, pipelines, aerial mapping etc. and also talked about the rapid spread of such systems for recreational and entertainment purpose. A public notice was issued by the DGCA on 07th of Oct 2014 which talked of the large civilian use of drones within the country and warned about the dangers of unregulated operations. Civilian operations of all drones were restricted unless they had approval from Defence, MHA, security agencies or the DGCA. To take matters forward and to involve all stakeholders the Ministry of Civil Aviation published Civil Aviation Requirements on the civilian use of drones on 02nd of November, 2017 and invited suggestions from all stakeholders before a final policy was put in place. These draft regulations were almost on similar lines to the policy that was announced on the 27th of August, 2018.

In India the civilian sector has seen an increasing use of drones in agriculture, exploration, mining, sports, photography and other areas. The use of drones in India has increased considerably for recreation and industrial purpose and today a variety of different models are easily available on e-commerce sites as Flipkart, Amazon, Indiamart, Snapdeal, OLX, Paytm mall etc. Today drones made by Chinese and French companies have flooded the Indian market. Chinese company DJI alone has 75 percent market share of the civilian drone global market. A recent report by Goldman Sachs talks about the global spending on UAV's in the next five years to be reaching approximately 100 billion US dollars.

II.   Drone Policy in other Countries

USA

The Drone policy of USA is regulated by the Federal Aviation Administration (www.faa.gov/uas). Separate rules exist for Recreational hobbyists, Commercial drone fliers and Educational users. The Commercial operators need to be registered with the FAA and must also possess a Remote Pilot certificate to fly drones. Their height limit is restricted to 400 ft and speed to less than 100 mph. Drones in USA can fly during daytime only and that too within the visual line of sight. Recreational drone fliers are exempted from having a Remote Pilot certificate, but need to comply with other conditions. Certain *No fly zones* have been laid down for all types of fliers.

Israel

Drone flying in this country is controlled by the Civil Aviation Authority of Israel (www.en.caa.gov.il). Separate rules have been laid down for Recreational and Commercial drone users. A commercial operator needs a license to fly whereas the hobbyists are exempted from this. However all drone fliers must fly below 50m height, only during the daytime and within the visual line of sight only. *No fly zones* have been earmarked by the CAAI.

France

The French Civil Aviation authority (www.ecologique-solidaire.gouv.fr) has set the rules for flying of drones in the country. All drones of weight 800 gms or more need to be registered on a public portal- Alpha Tango- and the unique

registration number given must be prominently displayed on the drone. Commercial drone pilots must pass a theoretical exam and also undergo basic training. Drones must not be flown over people and private property and must stick to the height limit of 150 mts. Only day flying is permitted and that too in the visual line of sight only.

UK

Civil Aviation Authority of UK (www.caa.co.uk) regulates the flying of drones in UK. Registration of drones and online safety tests for drone pilots will become mandatory from 30th Nov 2019. A height limit of 400 ft has been set and the drones are to keep a minimum distance of 50 m from people and property to cater to privacy issues. A separate category of *Tethered drones* and those weighing more than 20 kg have also been mentioned in the policy which are governed by a different set of rules. Clearly demarcated *No fly zones* have been listed to ensure safety and security of important places and the local police has been empowered to seize drones and penalize them for violating laid down rules.

China

Drone flying in China is governed by the Civil Aviation Administration of China (www.caac.gov.cn). Any drone weighing more than 250 gms has to be registered after which it gets a QR code which is to be displayed on the drone for identification. Drones flown for commercial purpose need a license issued by CAAC. The maximum altitude permitted is 120 mts and anything flown higher than this requires a commercial license. *No fly zones* have been earmarked and flying is permitted only within the Visual line of sight.

Japan

The Ministry of Land, Infrastructure, Transport and Tourism (www.mlit.go.jp/en/koku/uas.html) regulates the flying of drones which weigh more than 200 gms. These are permitted to fly during daytime and that too within the visual line of sight only. Limitations are placed on their flying in densely populated areas and in areas designated as *No fly zones*. Current rules do not permit carrying of hazardous materials and dropping of objects from drones.

III.   Areas of interest for Police

The following are areas where drones are being extensively used. These areas can be of vital interest for the Law Enforcement authorities as the role played by the drones directly affects the safety, security and well being of the citizens of the country and also has a bearing on the Law of the land. Some interesting areas are -

(1) **Urban Policing** – City based police forces in India have been using drones for traffic management, tackling law and order situations and also for crime control. Drones are being used for controlling and diverting traffic to ensure smooth traffic flow and also to keep an eye on emerging law and order situations. These have been found to be very useful in keeping an eye on the trouble creators/ mischief mongers in law and order situations by providing incontrovertible photographic evidence from a safe distance. Hi-Tech police command and control centers are these days using drones to fly over crime prone areas at designated times to keep an eye on the general situation in the area thereby thus proving to be a deterrent for criminals and anti-social elements, lest they be caught by the '*camera in the sky'*.

(2) **Jungle operations -** Drones have also been found to be very useful in anti- insurgent/ Maoist operations in jungles, hilly terrain and forests by providing that '*eye in the sky*'. These drones fly high and are able to give a bird's eye view of the exact dangers

lurking beyond the line of sight to prepare the troops for any exigency. These help in making operations more predictable, safe and secure. These can also give the exact location of the enemy hiding ahead and thereby giving the police forces that extra information to counter the threat successfully.

(3) **Border patrol** – Police forces manning the border areas are using drones to check illegal infiltration and cross border smuggling. These have been found to be very useful in keeping an eye on any suspicious movements on the border at all times of day and night. This kind of a usage on the one hand saves on manpower and at the same time provides accurate video graphic evidence of any untoward movement thereby preparing the border force to counter any nefarious designs in a pro-active manner.

(4) **Disaster relief** – Police forces have been using drones in times of natural and man-made disasters. These systems are designed to enable police to locate and reach stranded people, by reducing the time taken to activate rescue operations, send immediate food and relief material and thereby making the difference between their life and death. Such drones were used during floods in Kedarnath, Srinagar, Chennai, Kerala and cyclone in Odisha etc. Police and fire-fighting agencies have also been using drones in cases of man-made disasters as fire in multistoried buildings, building collapse etc. Drones have also kept a strict vigil to prevent any kind of mishap or disaster as was done during Kumbh Mela at Prayagraj recently.

(5) **Passenger Drones -** A number of firms the world over have been experimenting with passenger drones that can be used like an ordinary car or even summoned with a smartphone app. A number of firms as Airbus, Bell, Workhorse and Joby Aviation in US, EHang in China, Aeromobil in Slovakia and Lilium and Volocopter in Germany have been experimenting with passenger drones for some time. Safety is a primary concern herein and so these drones are equipped with a number of extra safety features as back-up manual controls, extra fuel for emergency and even parachutes for exigency. Test flights of such passenger carrying drones have already been carried out in Dubai. The government in Dubai plans to see 25% of Dubai's entire traffic to be done by such driverless vehicles by 2030. Police needs to keep an eye on this kind of development as these drones will fill up the sky and create a *'traffic jam up there too'*. New traffic rules will have to be thought of to regulate the flight path, flight times and ensure safe travel of these piloted/ driverless drones.

(6) **Underwater drones** – From airborne to underwater drones. An entirely new field has come up of having more 'eyes in water'. These drones are being used by police in some countries to locate capsized boats, missing/drowned persons, underwater obstacles and other lurking dangers below water surface. An interesting difference between airborne and underwater drones is that since the radio waves are not able to travel underwater, hence these drones are normally tethered by a long cable. Such drones are being used by defense forces for carrying surveillance in coastal areas on underwater submarines and other spy devices which enemies may plant in or around the land or ships of another country.

(7) **Illegal Mining** – Police and revenue authorities are using drones to study

topography of the mining areas to decide on the exact area and the title status regarding the extent of mining that can be done. Drones are being used to reach the exact spot where illegal mining and blasting is being carried out to assess the exact amount violation being done and the amount of material being dug out. The drones are able to show exactly the amount of illegal mining that has been done and the extent of penalty that can be levied. All this can be done safely, with accuracy and also in a discreet manner.

(8) **Medical relief –** There are times when the Police department creates a '*Green corridor*' in an emergency situation when the life/ lives of people are at stake and vital organs have to be sent to a distant place. The entire objective of this exercise to provide a quick, safe and non-stop passage for an ambulance carrying vital organs to the hospital where the patient is admitted.

Some agencies have found drones to be particularly useful in Rwanda in Africa to drop off packages of blood for transfusion and also deliver vaccines and other life saving medicines to remote and far flung areas. This approach is useful in countries with inadequate infrastructure, inhospitable terrain and poor road network. Valuable, important and life saving drugs can be moved quickly, safely and cheaply obviating the requirement for expensive packaging, need for refrigeration and even security issues.

IV.   Drone usage - Other areas

(i)   **Sports -** Drone racing is a new sport that has caught everyone's fancy. The World Drone Prix conducts drone racing and offers cash prizes amounting to approximately 1 million dollars. World Organization of Racing Drones (***WORD***) is the organization behind this idea and it has held races in Dubai and Hawaii. This involves the use of a remote control to operate and fly drones. This racing is of two kinds - freestyle and track racing. Freestyle involves a person to fly his drone in the most adventurous and thrilling manner in a stipulated time limit. Track racing, on the other hand, means flying the drone on a predefined track for a fixed number of laps in the shortest possible time. Experts claim that the drone racing market, estimated at $ 500 million today, is likely to reach $ 3 billion by 2020.

(ii)   **Internet from sky -** Facebook has already tested the flying of ***Aquila*** drones at about 60- 90 thousand feet up in the sky which will beam Internet to people on earth. A fleet of such solar powered drones is expected to beam Internet from space and ensure non-stop connectivity across the globe. These pilotless drones will weigh about 1000 pounds, have a wingspan larger than a Boeing 747 and will be controlled by a ground station crew. The idea behind this concept is to provide Internet connectivity to almost 4 billion people who are today in far flung areas which are the '***dark zone***' for Internet.

(iii)   **Agriculture -** Today drones are also being used for monitoring the variability in crops, deciding the optimal level of irrigation, pesticides and fertilizer mix for the crops. These drones are fitted with multispectral cameras- sensitive to specific wavelengths of light. These enable them to detect health related changes in plants before they are visible to naked eyes. Such multispectral photography also helps in finding out the disease likely to affect the crops and assess the correct yield in a season. Since all

these results are available in a much faster and scientific manner than ever before, it leads to savings in time and input costs, leading to improved yields in agriculture, revenue and better profits for the farmers.

(iv) **Urban development** – A number of issues in urban development can be successfully tackled using this technology– ensuring balanced development of any area, planning out expansion of city by correct assessment of topography and natural resources, ensuring optimal allocation of available budget, correct placement of public utilities, checking for encroachment/ illegal construction etc.

(v) **Media -** Journalists in US, UK, Russia, France, India and a number of other countries are using drones to capture photographs of celebrities, VIP's, important events etc. from unheard of angles, inaccessible and unsafe places, which otherwise would take a long time to reach. Journalists are acting as remote-control-pilots and covering riotous situations, natural and man-made disasters and at times also intruding into the privacy of celebrities and other well-known persons to beam photographs that would not have been possible earlier. They have found that this option is much cheaper, faster and safer than hiring of helicopters and airplanes.

(vi) **Oil and Gas industry -** Drones are being used to look for leakages in oil and gas pipelines. They are also able to check for pilferage or theft of oil being done from over ground pipelines. Drones are also being used to service off -shore oil and gas platforms by permitting dropping of supplies in all weather conditions without risking human pilots. Underwater drones are being used by oil companies to carry out underwater inspection of oil rigs in the sea to check for any damage, fault or acts of espionage and also to check inside of oil tanks for damage or cracks in order to pre-empt any damage or oil spill.

(vii) **Power industry** – These companies are using drones to do a quick check on any damage to power lines, solar panels and windmills without exposing the linesman to any risk and thereby saving on time and costs.

(viii) **Delivery services -** Google and Amazon have already been testing delivery of packages to consumers by drones. However, the regulation that the drone operators have a *line of sight contact* with the drone comes in way of full-scale commercial operations. Experts in this area have suggested that a *low altitude air space* can be carved out for drones exclusively so that it falls out of the line of manned aircraft and low flying helicopters. This kind of a provision can go a long way in enabling delivery of goods by enabling drones to fly over highly populated areas, thus saving on time and costs.

(ix) **Space -** Drones have been used in the International Space Station since 2006. This drone called **SPHERE** (Synchronized, Position, Hold, Engage, Reorient, Experimental satellite) is a 30cm cube which uses jets of carbon dioxide to propel itself In the Space Station. NASA is currently planning to introduce a new kind of drone called **Astrobee** in the Space Station which will compress air available onboard and use it for propulsion. It will be able to relieve the astronauts of routine tasks and will form the virtual eyes for scientists at the ground station to keep track of things that have gone missing or have changed their places in the space station because of zero gravity.

(x) **Use in Defence -** US armed forces have

been using drones since 2002 in Iraq, Yemen, Afghanistan, Syria, Libya, Somalia and Pakistan. The US Army uses long range drones as Predator, Reaper, Puma, Global Hawk, Raven etc. which can fly non-stop for over 24 hours at heights of over 30,000 ft and can fire missiles with amazing precision. To counter the attack of these military drones, ISIS has also started using drones to counter the US threat. All this has led the US to adopt new strategies and technology to counter such attacks.

(xi) **Military Drones in India -** The Indian Air Force today has Israeli Harop killer drones which can act as *kamikaze* drones. The forces also have Israeli Heron and Searcher-II drones which undertake combat missions and carry out routine surveillance. The Indian government has been in recent talks with the US government to procure combat drones armed with missiles and capable of flying for over 25 hours. The US government has recently cleared the sale of 22 Guardian drones to India and the country is also on course to buy another 10 Heron drones from Israel.

(xii) **Other areas (Insurance, Banking, Environment) -** There are a number of other areas where the usage of drones is picking up or can be thought of to save time, money and boost efficiency in the system. The *Insurance* sector can use drones to assess the damage at any site without actually reaching the site or at places which are difficult to reach. *Banking* sector can make use of these to quickly restock the ATM's which are in far and inaccessible areas. Multispectral cameras onboard can be used to check *pollution* levels in lakes and rivers without the requirement for physically going to

each of the suspected spots. The *Forest* department has been using drones to keep an eye on poachers, clamp down on poaching and even red flag encroachment areas in the forest.

V.   Anti Drone Technologies

The sheer versatility of drones have made them an attractive tool in the hands of anti-social and anti-national elements. As a result there is no dearth of rogue drones up there in the sky. Radioactive material landing on the roof of Japanese Prime Minister's office in Tokyo, French nuclear plants being surveyed by unknown drones, drone crashing in White House lawns, criminals using drones to send drugs, mobile phones and weapons into the prison are few such examples. Drones were used to conduct reconnaissance of Reau prison, in the outskirts of Paris, to study the security set up, after which the famous criminal Faid escaped in a helicopter.

Trials have been conducted of anti-drone systems to counter the rogue fixed-wing planes as well as quad-copters. Techniques as listening and identifying the sound of incoming drones, using thermal imaging cameras for identification, flooding the radio frequency in which the drone is operating so as to cancel out its signal are being tested. Techniques have also been developed to hijack or take over the controls of incoming drone. More basic techniques as shooting down an incoming drone or catching it and retrieving it in a net have also been thought of to destroy rogue/enemy drones whose threat is very real today. Terrorists have also been talking about delivering bombs and other payloads as nerve gases through drones in crowds and heavily populated places to kill people and spread panic. Some of the technologies being used the world over are -

(a) **Drone gun –** This gun looking contraption jams the radio/GPS/ mobile signal

between the drone and the pilot and is able to ground the suspect UAV. This weapon, designed in Australia, has an effective range of about 2 kms.

(b) **ATHENA** – This weapon targets big drones by firing a high energy laser beam which completely destroys the enemy drone. The full form of this weapon system is *Advanced Test High Energy Asset*. This has been tested by the US Army.

(c) **Drone Catcher** – There are times when it would be desirable to bring down the suspect drone safely so that all incriminating evidence can be preserved, studied and then used at a later date. This system comprises of a drone which approaches the enemy drone, locks onto it and then catches the enemy drone by throwing a net around it.

(d) **Skywall 100** – This system is the grounded version of the Drone catcher. The ground-based gun fires a net at the suspect drone and then brings down the suspect drone safely using a parachute. The effective range for this drone is about 100 mts.

(e) **Sky Fence** – This system uses a range of signal disruptors geared to jam the flight path of the suspect drones and prevent them from entering secure and sensitive places and VITAL installations.

(f) **Drone Malware** – This technique implies hacking of the suspect drone by planting of a malware remotely, taking control of its software and pilot and thereafter taking it in custody.

(g) **Use of Eagles** – The Dutch started using this technique to pluck out enemy drones from the air. The eagles because of their big wingspan, keen eyesight and sharp talons were quite successful in this, but due to inconsistent behavior of the birds this technique has of late been shelved.

Anti-drone technologies are being experimented with in India also. In 2018 the Government invited a number of local and foreign players to exhibit their technologies in this vital area. The idea was to set the ball rolling so that appropriate mechanisms can be put in place to counter the threat of rogue drones. A number of government agencies as Ministry of Civil Aviation, Pawan Hans Limited, IAF, CISF, NSG, DRDO etc. participated in the process along with local and foreign firms to decide on the technology best suited under Indian conditions.

VI.   Conclusion

With a draft Policy in place, it is only a matter of time before flying of RPA's/drones becomes legal in India. There are thousands of drones which are already being operated by different players in the country for sports, recreational and commercial purpose. All these will have to incorporate the latest provisions given in the new Policy to ensure that matters related to licensing, flying and safety are adhered to. The opportunities are endless and there is no dearth of creativity on ground. It remains to be seen as to how people take to this policy and explore newer areas for drone usage. The Government also needs to keep its ears on the ground and ensure that the Policy remains dynamic and is able to cater to the demands of the industry and end users by regularly incorporating newer provisions in the policy. All this will open up newer areas and ensure goods and, maybe even passengers are transported faster, cheaper and safer. Technology will help make quicker assessments for optimal decision making to reduce the down time in critical infrastructure, energy supply and open up newer areas for exploration of ground-based minerals and energy supply. Such a scenario can ensure a win-win situation for the different industries and the government.

Bibliography

- Requirements for Operation of Civil Remotely Piloted Aircraft Systems (RPAS), : *"Office of Director General of Civil Aviation",* 27 August 2018.

- Constitution of Task Force…., *"Order, Ministry of Civil Aviation",* 11 April, 2018.

- Draft Regulation of CAR on Civil use of Drones, *"Ministry of Civil Aviation"*, 2 Nov 2017.

- Use of Unmanned Aerial vehicle (UAV)/ Unmanned Aircraft Systems (UAS) for Civil Applications, *"Office of the Directorate General of Civil Aviation"*, 7 Oct 2014.

- Months before man escaped in helicopter, drones scouted jail: *"Jailbreak inspired by Hollywood"*, Indian Express, 3 July 2018.

- Ready for takeoff: *"Drones in a Box",* Indian Express, 23 July 2018.

- With Radars and nets, Pentagon tests tech to destroy Islamic State drones: *"Terror outfit's drones have mostly targeted Iraqi troops and Syrian Militias"*, Indian Express, 25 September 2017.

- NSG, CISF may get the power to shoot 'rogue' drones: Hindustan Times, 11 September 2017.

- India seeks US Combat drones, but settles for Spy ones for now: Times of India, 26 June 2017

- Armed with drones, refugee vows to halt drowning at sea: *"Lending a helping hand",* DNA, 26 August 2016.

- Help from above: *"Medical drones in Africa",* Indian Express, 6 July 2016.

- A drone start-up explores underwater: DNA, 29 July 2016.

- Drone Racing 101: DNA, 31 January 2016.

- Google aims to begin drone deliveries: Gen-Next Tech, DNA, 4 November 2015.

- Astrobusybee: Drones in Space, Indian Express, 29 September 2015.

- Copping a copter: Dealing with Rogue drones, Indian Express, 7 May 2015.

Hot Spot Policing:
An Overview of 'She Teams'

A. Sneha Vardhani[*]

Abstract

Can an approach undertaken by the law enforcement agencies that is beyond traditional interventions have a potential to empower women and generate a feeling of safety and security among women in the society? One such intervention to endeavor is through an increased police presence at places where women feel vulnerable is likely to result in *reduction of fear of crime among women*. Places (*micro-geographical locations*) facilitate unique behavioral settings for crime to occur and such places are classified as high-risk areas [*hot spots*]. Those places where *a likely offender* comes in contact with *a suitable target* in the *absence of guardianship* does not make occurrence of crime inevitable but creates an *opportunity* for crime ['Routine Activity Theory']. The purpose of this research is to analyze the effectiveness of the intervention of *hot-spot policing* in controlling a social problem affecting women. Hot spot policing strategy to combat crime against women and ensure her safety was not a focus until recently. She Teams as a forerunner in hot spot policing towards crime control and crime reduction [precisely the offence of eve-teasing] is producing tangible results. With over hundred teams operating in 350 listed hot spots, the city of Hyderabad is attempting to end crime against women.

Keywords:

She Teams, Eve-teasing, Violence against women, Hot spot policing, Hyderabad.

Introduction

Use of the term "Eve teasing" as a euphemism for sexual harassment of women is questionable. Regardless of the seriousness of an offence committed against women, police intervention by the Women Safety Wing of Telangana State is proactive. One such programme taking a lead in reducing gender-based violence across the State of Telangana is 'She Teams'. *"The programme was started with the approval of the State Government in the year 2014 with the aim of curbing eve-teasing in all aspects, in all forms,* *at all places, providing safety and security to women in the society…"* (She teams Webpage).

The scope of eve-teasing is expansive, varies from acts such as staring to inappropriate physical touch. Moreover, nature of the act of eve-teasing is in a manner that most of the victims fail to prove perpetrator(s) guilty for lack of evidence. Another dimension to the problem of eve-teasing in most cases is that victims resist reporting the incident due to lack of awareness, lack of courage, are concerned about family honor and other societal factors.

Author Intro:

[*] Master of Laws (LLM) in Crimes & Torts, II Year Student, Osmania University, Hyderabad.

Incidents of eve-teasing reported to She Teams are filed under provisions of Indian Penal Code, 1860[1] or Hyderabad City Police Act, 1348[2]. As there is no exclusive provision to deal with 'eve-teasing' in the IPC or any State Act, a need for specific legislation to tackle the menace of eve-teasing was felt in Tamil Nadu (implemented Tamil Nadu Prohibition of Eve-Teasing Act, 1998); and Anti-Eve-Teasing Bill (2017) of the Telangana Government is pending for approval[3].

According to Tamil Nadu Prohibition of Eve-Teasing Act, 1998, Section 2(a) defines *"eve-teasing" as any indecent conduct or act by a man which causes or is likely to cause intimidation, fear, shame or embarrassment to a woman, including abusing or causing hurt or nuisance to, or assault, use of force on a woman.*[4][5]

Eve-teasing in public places is almost ubiquitous and unvoiced and to address victimization of women by following the traditional procedure of having to file a complaint at the Police Station followed by an investigation and a trial is grueling for the victim if she is to report stalking or catcalls etc. An unconventional approach from the law enforcement agencies is the need of the hour towards crime prevention and reduction.

Hot Spot Policing

"Crime does not occur evenly over the landscape. It is clustered in small areas, or hot spots, that account for a disproportionate amount of crime and disorder" (National Institute of Justice, 2009).[6] For example: Eve-teasing commonly occurs at crowded locations such as bus stops, railway/metro stations, educational institutions, cinema theatres, parks, place of festival, temples, activity places, in public transport vehicles, dim lit streets or isolated areas etc. Accordingly, She Teams had adopted the Hot spot policing strategy by identifying over hundred troubled areas (as *hot spots*) within the city of Hyderabad and a minimum of three hot-spots in each district of Telangana as most troubled areas.

"Hot spot policing is often used to refer to place-based policing where the focus of resources or policing strategies is on the locations where crime is highly concentrated" (Weisburd & Telep, 2014).[7] A review of available research by National Research Council suggests that *"there is strong evidence that the more focused and specific the strategies of the police, the more they are tailored to the problems they seek to address, and the more effective police will be*

---

1   Sections invoked in case of eve-teasing: Section 294 (Obscene acts and songs), Section 354 (Assault or criminal force to woman with intent to outrage her modesty) and Section 509 (Word, gesture or act intended to insult the modesty of a woman). [Hereinafter 'IPC'].

2   Section 70 (c) *use of any threatening, insulting or obscene words or gestures, likely to disturb public peace or causes public nuisance, shall be punished with imprisonment for a term which may extend to eight days or with fine which may extend to fifty rupees.*

3   The proposed Bill is pending with Ministry of Home Affairs as reported in: Press Trust of India, *Telangana Government planning to bring in anti-eve teasing law,* July 3rd, 2017. Available at: https://www.indiatoday.in/pti-feed/story/telangana-govt-planning-to-bring-in-anti-eve-teasing-law-991804-2017-07-03; last accessed on 19/03/2019.

4   [Act 44 of 1998]. Tamil Nadu is the first and currently the only State to have a State legislation to deal with eve-teasing. Delhi Prohibition of Eve-Teasing Bill, 1984 had lapsed in 1988.

5   Section 4: Penalty for eve-teasing- *Whoever commits or participates in or abets eve-teasing in or within the precincts of any educational institution, temple or other place of worship, bus stop, road, railway station, cinema theatre, park, beach, place of festival, public service vehicle or any other place shall be punished with imprisonment for a term which may extend to one year or shall be liable to fine which may extend to ten thousand rupees or both.*

6   National Institute of Justice, *Hot spot Policing Can Reduce Crime* (2009), available at: https://www.nij.gov/topics/law-enforcement/strategies/hot-spot-policing/pages/welcome.aspx; last accessed on 12/03/2019.

7   David Weisburd, Cody W. Telep, *Hot Spot Policing: What We Know and What We Need to Know*, Sage Publication, Volume 30, Issue II, p.200 (March 12, 2014), available at: https://journals.sagepub.com/doi/abs/10.1177/1043986214525083; last accessed on 20/03/2019.

in controlling crime and disorder" (Skogan & Frydll, 2004 as cited in Braga, 2015).[8] The object of hot spot policing strategies is to make the high-risk areas safer. The *social characteristics* of a place are a contributing factor in designating an area as a *hot spot.* For effective crime control and long term results, the purpose of policing should be to change these places in a way that the prevalent social features [risk factors] are less conducive to crime. *For example:* One high risk area where eve-teasing occurs is on dimly lit streets, so, an increase in street lighting alongside frequent patrolling will create deterrence on part of the offender of being watched. However, the law enforcement agency must adopt an interdisciplinary approach to bringing in changes to the social features of a high-risk area [hot spot] i.e., by partnering with other agencies/departments. In absolute terms, hot spot policing is based on the premise that *places provide opportunity for an offender to commit crime.*

Limitation: Hot spot policing includes wide-ranging strategies and tactics; however, the researcher in further sections of this research paper will examine the strategies adopted by 'She teams' and draw an analysis based on the results generated by such policing.

Criminological Background

According to the *General Theory of Crime*, by Michael Gottfredson and Travis Hirschi (1990), criminal decision-making is a function of two facts: *low-self control and opportunity* (as cited in D.Walters, 2015).[9] Further introspection into

the second factor of the *General Theory of Crime* is more relevant for this research i.e., to answer *when does an 'opportunity' to commit an offence occur?*

Cohen, L.E., and M. Felson in 1979 introduced 'Routine Activity Theory' to the field of criminology which link criminal behaviour to activities of daily routine [taken as an influencing factor]. We all have different routines of life once we step out into the society- that involve dispersion of activities away from households, our social behaviour and social interactions etc. This theory posits that the nature of routine activities he/she engages in regularly have a tendency to influence the situations that he/she encounters, consequently, any changes in the routine activity pattern will result in change in the situations he/she faces.[10] According to Cohen and Felson, the point of inclination towards criminal behaviour is theorized as: In (the) course of routine activities when *likely offenders, suitable targets converge in space and time in the absence of capable guardians (triad), criminal acts are committed.* Thus, likelihood of '*opportunities*' are created from dispersion of activities away from household in the absence of effective control system. "For example: *women's participation in the labor force and access to higher education, commuting time, as well as an increase in vacation length trips outside the city, or permanent relocation increased contact with possible offenders and left homes empty and unprotected."*[11]

Hot spot mapping guides effective police action where as task of mapping is guided by

8   Anthony A. Braga, *New Perspectives in Policing: Crime and Policing Revisited*, National Institute of Justice, (September 2015), available at: https://www.ncjrs.gov/pdffiles1/nij/248888.pdf; last accessed on 13/03/2019.

9   Glenn D. Walters, *The Decision to Commit Crime: Rational or Non-rational? Criminology,* Criminal Justice Law & Society, Volume 16, Issue 3, p. 10 (2015).

10   Oxford Bibliographies, *Routine Activity Theory*, July 2018 (rev.,) available at: http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0010.xml; last accessed on 14/03/2019.

11   *The Encyclopedia of Theoretical Criminology*, J. Mitchell Miller (ed.,), Wiley Blackwell, Volume I (A-K), p.735 (2014).

criminological theories.[12] Thus, identification of such geographical locations where there is a probable congregation of triad is the object of She Teams alongside other policing strategies.

She Teams

"States have an obligation to act with due diligence to address and respond to all acts of violence against women" (CEDAW, 2013 as cited in Information Series of OHCHR, 2015).[13]

Forms of violence against women occurring in public spheres and private sphere alter but *violence against women affects women everywhere*.[14] Any method adopted to condemn violence against women should be versatile, in order to ensure security of women. While the research advocates that criminal activities are fairly clustered in few areas over others, it is important to note that women are likely to be aware of such high-risk areas, but their routine activities require stepping out of their own comfort zone. And eve-teasing is an insidious daily-problem where the probability of victimization is also high.

She Teams is a mission undertaken by the Women's Safety Wing (Special department of Telangana Police), initially to curb the menace of eve-teasing but has eventually expanded its scope of policing to offences such as cyber bullying, sexual assault, sexual harassment, domestic violence, dowry related violence, trafficking, child abuse and child marriages. She Teams is still at the beginning stage in thirty-three district areas with available police personnel managing

an additional task of She Teams. Whereas, She Teams is sternly operational in the city of Hyderabad and this research studies the model as adopted in the metropolitan area.

The Model of She Teams

*   Following factors have been considered in identifying the 'hot spots':
    i.   Places bustled with people.
    ii.   Public areas without sufficient guarding.
    iii. Premises of Working Women Hostels, Educational Institutions [Women's Colleges and All-Girls Schools.
    iv.   Areas with large number of cases lodged as per Police Station records

Note: Pinpointing of incident prone areas was done using: CCTV camera footages; feedback from NGOs working for welfare of women, police officers involved in regular beats and victims; and from available data on number of complaints registered. There are about 350 listed hot spots within the city of Hyderabad [East Zone and West Zone].

*   Hot spot policing strategies used by She Teams include the following:
    i.   **Dedicated Patrols:** According to the Routine Activity Theory, a likely offender part of his/her daily routine encounters criminal opportunities and decides whether to take action or not. In such case, visible police presence will deter

---

12   John E. Eck, Spencer Chainey, James G. Cameron, Michael Leitner, and Ronald E. Wilson, *Mapping Crime: Understanding Hot Spots,* National Institute of Justice, Special Report, 2005, p.1, available at: https://www.researchgate.net/publication/32894301_Mapping_ Crime_Understanding_Hot_Spots; last accessed on 20/03/2019.

13   Committee on the Elimination of Discrimination Against Women (Referred to as CEDAW), *General Recommendation* 19, para. 9; *General Recommendation* 28 (2010) on core obligations of States Parties, para. 13; *Special Rapporteur on violence against women, its causes and consequences,* A/HRC/23/49 (2013) as cited in *'Information Series on Sexual and Reproductive Health and Rights'* by Office of United Nations High Commissioner for Human Rights (OHCHR) (2015) available on https://www.ohchr.org/Documents/Issues/ Women/WRGS/SexualHealth/INFO_VAW_WEB.pdf; Last accessed on 16/03/2018.

14   *Report by OHCHR., Supra n.13.*

criminal conduct. And on a general note, possibility of crime control or reducing fear of crime is viable from target oriented policing than through random patrolling.

ii. **Police Officer's Decoy Operation:** This is a policing strategy where women/women police personnel especially constables disguised as decoys, assist She Teams in nabbing the eve-teasers on spot with evidence.[15]

iii. **Stop and Detain:** This is a policing strategy where if a She Teams officer in good faith has reasonable suspicion on an individual that he is about to or likely to commit a crime, can stop and detain him. Further, levy charges substantiating with relevant evidence.

iv. **Proactive Arrests:** She Teams has adopted Zero Tolerance Policy towards women safety. Zero Tolerance Policy means the act of punishing all criminal or unacceptable behaviour severely, even if it is not very serious (as defined in Cambridge Dictionary). The following are various laws under which the cases are filed: Indian Penal Code, 1860; The Criminal Law (Amendment) Act, 2013 (also called the Nirbhaya Act); Hyderabad City Police Act, 1348 (cases within the jurisdiction of Hyderabad); Information Technology Act, 2000; Protection of Children from Sexual Offences Act, 2012 and Preventive Detection Act, 1950 in case of repeat offenders.

- 'A Team' of She Teams (policing at hot spots) include:
  i. A Sub-Inspector heading the team,
  ii. Assistant Sub-Inspector or a Head Constable,
  iii. A lady constable and two or more male constables.

Note: The police personnel on beat are equipped with discreet body-worn cameras to record the act and produce it as evidence against the perpetrator. Team members maintain a 'job sheet' in which details of duty-activities are entered regularly. Police officers working with She Teams undergo specialized training and are accountable to Deputy Superintendent of Police.

With the given pace of developments in technology there is optimal access to police services across the country. Ambit of Section 154[16] of Criminal Procedure Code, 1973 has also been stretched by few states to enable online registration of FIR (e-FIR). She Teams is one step ahead in its commitment to make their services more accessible over various online platforms, resultantly, half of the complaints made by victims are through internet (e.g., as shown below in Table 1.1). Identity details of victim are confidentially maintained by She Teams, and police responding to complaints made via social media is a boon for victims in fear of social stigma.

---

[15] Decoy Operations by Police Officers disguised as victims has been curbing street crimes such as rape, assault, purse-snatching and robbery in United States has reduced the occurrence of such criminal activities. Source: William R. Carlsen, Police are curbing Street Crimes With Decoys Disguised as Victims, New York Times, July 10, 1977, available at: https://www.nytimes.com/1977/07/10/archives/police-are-curbing-street-crimes-with-decoys-disguised-as-victims.html

[16] Section 154 (1) Every information relating to the commission of a cognizable offence, if given orally to an officer in charge of a police station, shall be reduced to writing by him or under his direction, and be read over to the informant; and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.

Table 1.1: To understand the *accessibility* of She Teams

Complaints Received by She Teams.

Year	At Hot spots	On Complaint	E-mail	Facebook	Whatsapp	HawkEye	Twitter	Dial 100	Total
2014	12	7	8	0	0	0	0	71	98
2015	54	36	72	250	32	6	0	634	1084
2016	62	324	143	80	157	51	3	590	1410
2017	75	508	255	6	46	45	0	203	1138
2018	123	633	326	6	240	20	4	39	1391
Till Feb 2019	7	94	20	0	70	2	0	12	205
Total	**333**	**1602**	**824**	**342**	**545**	**124**	**7**	**1549**	**5326**

Source:http://sheteamhydpolice.telangana.gov.in/objectives.html (2019); Last accessed on 16/03/2019.

The perpetrators are warned strictly or undergo counseling or are booked under provisions of Indian Penal Code depending on the degree of offence. As per the enforcement statistics of She Teams for the year 2018: Out of the 1,391 petitions received, 724 perpetrators were counseled and followed up (Table A1). Only about 109 petty cases were booked against the offenders under various statutes (Table A2); which show the unwillingness of victims on registering a First Information Report in the Police Station.

Nevertheless, She teams asserts to victim for an FIRs to be filed at the Police Station in order to enable an investigation followed by taking cognizance of the offence.[17] This is a prerequisite at least for cases where the accused is not within the jurisdiction of the State of Telangana and more so in cases of cyber harassment.

•   A Different Approach: The model of She Teams has been replicated as it is in Uttar Pradesh (Anti-Romeo Squads), Andhra Pradesh (Shakti Teams) and as dedicated patrolling units in Rajasthan (Lady Patrol Unit), Maharashtra (Nirbhaya), Gujarat (Nirbhaya Squad), Karnataka (Rani Chennamma Squad), Chhattisgarh (Patrolling Vehicles), Kolkata (Winners), South Delhi (Raftaar Bike Patrolling), Jaipur (All Women Patrolling Squad), Kerala (Pink Police Patrol). But, She Teams is still a staunch model of programme not only for its victim-centered approach or taking a reformative action against the perpetrator, but also for its well organized-well monitored [dedicated] policing strategy; and its immense top-level support from the Government.

Fig. A: Flow chart to show the structure of She Teams in dealing with the parties.

---

[17]   Section 157 of the Code of Criminal Procedure, 1973 prescribes the Procedure for investigation preliminary inquiry over the information received by an officer in charge of a police station.

Conclusion

The problem of eve-teasing is ubiquitous but Police cannot be omnipresent. Awareness among citizens especially in the rural areas about She Teams is the need of the hour. Hot spot policing technique can only be applied to eve-teasing and harassment of women at public places. This strategy is not helpful in guarding against the violence that takes places within four walls of a home and against cybercrime victimization when perpetrator acts in isolation. Thus, She Teams also involves itself in prompt rescue service which is a reason for Dial 100 call for service being widely used to report an offence (eg., as shown in Table 1.1.). Further, the policing technique must be complemented with various other interventions and initiatives. For example: She Teams has launched a programme 'Cyber Rakshaks' in association with TASK [Telangana Academy for Skill and Knowledge] where hand-picked students receive training and become ambassadors for digital safety; Programme 'Bala Mitra' where one teacher from each school will act as a bridge between school children and She Teams by reporting child sexual abuse; Increase in installation of CCTV cameras up to ten lakhs across the streets of Hyderabad for continuous monitoring. Identification of incident prone areas require multiple techniques, at the same time, there is no universal method to battle all types of crime.

She Teams with the motto "For You..With You..Always" has been successful in creating a safe city for women. The model based on hot spot policing is deterring criminal conduct and making women feel protected. Hot spot policing technique reduces the opportunity of crime which cannot be statistically represented but the Routine Activity Theory proposes that when opportunities are created in the absence of effective control system, a crime is likely to take place.

References

- Akhtar, Eve teasing as a form of violence against women: A case study of District Srinagar, Kashmir, International Journal of Sociology and Anthropology, Vol.5 (5) p.168-178, (2013).
- Information Series on Sexual and Reproductive Health and Rights by Office of United Nations High Commissioner for Human Rights (2015).
- Michael Gottfredson and Travis Hirschi, A General Theory of Crime, Stanford University Press, Stanford, Calif, (1990).
- Skogan and Kathleen Frydll (ed.,), Fairness and Effectiveness in Policing: The Evidence, National Research Council, Wesley National Academies Press, Washington DC, (2004).
- Sharon L. et al., What is Eve Teasing? A Mixed Methods Study of Sexual Harassment of Young Women in Rural Indian Context, Sage Publications, (2017).

Internet Based Resources:

- Hyderabad City Police Act, https://www.hyderabadpolice.gov.in/acts/CityPoliceAct.pdf
- She Teams Webpage, http://sheteamhydpolice.telangana.gov.in/sheteam.html
- Hyderabad Police Official page, http://www.cyberabadpolice.gov.in/she-team.html
- Registering of e-fir, https://www.livelaw.in/online-registration-of-firs-need-of-the-hour/
- National Police Foundation: https://www.policefoundation.org/publication/the-police-foundation-displacement-and-diffusion-study/
- Office of the United Nations High Commissioner for Human Rights, www.ohchr.org

News Report:

- Installation of CCTV camera: https://www.thenewsminute.com/article/telangana-police-install-15-lakh-cctv-cameras-across-state-over-next-3-years-94223

- Bala Mithra Initiative: http://www.greattelangaana.com/balamitra-for-child-protection/

- Cyber Rakshak Initiative: https://www.thehindu.com/news/cities/Hyderabad/over-100-she-teams-working-incognito-for-womens-safety-dgp/article26572514.ece

APPENDIX A
SHE TEAMS ENFORCEMENT STATISTICS

Table A1: To show the number of perpetrators counseled or received a warning.

Year	No. of persons brought and counseled			No. of persons warned and let off		
	Major	**Minor**	**Total No. of persons**	**Major**	**Minor**	**Total No. of persons**
2014	58	16	74	7	12	19
2015	158	126	284	19	53	72
2016	439	111	550	278	111	389
2017	543	133	676	418	137	555
2018	625	99	724	459	99	558
Till Feb 2019	82	11	93	64	11	75
Total	**1905**	**496**	**2401**	**1245**	**423**	**1668**

Source:http://sheteamhydpolice.telangana.gov.in/objectives.html

Table A2: To show the underused service of registering an FIR.

No. of petty cases booked under various laws				
Year	**Cases booked**	**Fined**	**Jailed**	**Pending**
2014	39	39	0	0
2015	115	89	26	0
2016	141	126	15	0
2017	89	50	38	1
2018	109	37	71	1
Till Feb 2019	9	2	7	0
Total	**502**	**343**	**157**	**2**

Source:http://sheteamhydpolice.telangana.gov.in/objectives.html (2019); Last accessed on 16/03/2019.

Virtual surveillance of cybercrime and accelerating global response: A legal perspective

Dr. A. Md. Shamiulla[*]

Abstract

Cybercrimes have increased with the increased use of computers. Measures have been developed at the national level to address the cybercrime issues; however, due to the nature of the crime, there is a need to adopt global frameworks. Various nations have developed internal legal measures to prevent cybercrime. The success of the measures can be fully effective through global integration. The international conventions have been developed to bring nations together and ensure that they join hands in fighting cybercrime. This paper addresses the history and introduction of cybercrime and their implications at the global level. Also, it analyzes the various measures used in addressing the crime and the challenges faced. Based on the analysis, the future of cybercrime can be easily analyzed to determine based on the effectiveness of the existing measures and policies governing cyber criminology and justice systems globally.

Keywords:

Cybercrime, internet, cyber-terrorism, impulsivity

Introduction

According to Lee, & Sanchez (2018), cybercrime is on the high increase, and this presents a major threat to various organizations. Cybercrime developed as a result of the high technological advancement and the increased use of internet among the populations. The new trends of cybercrime are arising, and they are committed by both individual and groups. Companies have majorly invested in the data automation where they can store all their data digitally. The electronic system allows easy retrieval of important information that may be needed for business transactions. On the other hand, such companies are also at high risk of suffering from the cybercrime, and this requires that they advance their security systems to ensure data integrity and avoid loss associated with data breach(Rana, 2018). Additionally, cybercrime influences moral erosion and threats to the internet users who are likely to be exposed to the material or contents they did not intend to see. Furthermore, the increasing terrorism threats have been advanced by the online radicalization. Apart from the internal organization, policies are developed at the national and international levels to curb the highly increasing and threatening menace. The purpose of this paper is to explore the legal perspective of the global response to cybercrimes.

Author Intro:

[1]   Assistant Professor, Institute of Law, Nirma University

According to Jigar (2016), internet usage continues to increase globally, and this means that the risks of cybercrimes and the victims increase significantly. For example, the number of internet users in India by 2016 was estimated to be 462,124,989(Jigar 2016). With the increasing internet penetration, there is a need to safeguard the citizens from the growing cybercrimes. The common forms of cybercrimes may including hacking into an individual's or company's information systems and accounts, forgery, online gambling, cyber trafficking, child pornography and cyberbullying among others(Sarre, Lau, & Chang, 2018). Also, more dangerous forms of cybercrimes may include the cyber-terrorism, distribution of the pirated software, cyber warfare and possession of unlawful information (Sarre, Lau, & Chang, 2018). As a result, the general society is at high risk of suffering from any of the threats the more they use the internet. The purpose of this study is to explore the global legal framework used to prevent the cybercrime and the challenges experienced in the process.

Legal Response

The Internet has made the world a global village where people can engage and communicate easily regardless of their geographical distance. All the internet users are at risk of cyber crimes which may be committed by people from other parts of the world other than where they are located (Kerstens, & Veenstra, 2015). Due to this, there was a need to develop transnational policies that foster global security for all internet users. Therefore, a real and sound response to cybercrime requires international cooperation which involves equal input from all the parties involved in the international community (Sarre, Lau, & Chang, 2018).

On the other hand, some challenges are present in the process of developing the legal frameworks to reduce incidences of cybercrimes in the society. Some of the common challenges include lack of cooperation and laxity among the members to enforce the global prevention programs and lack of legal measures to use in investigation and response to the threats (Lee, & Sanchez, 2018). The risks associated with cyber threats were minimal when the internet was first introduced. Throughout the historical experiences, people have been seeking to expand the scope of internet use in international integration as others seek to achieve their self-interests. The increasingly technological development mainly propagates the game power of the cyber threat. The development of cyberspace has developed both possibilities and threats as new players emerge and people scramble for opportunities, as well as others fighting to dominate the space.

New technology and the ubiquity of the internet has led to the world getting more connected than ever. The internet increment across the world is rapid. This has been seen to be more helpful. However, it has come with negative implications too. Cybercrime, software piracy, illegal downloading, hacking and cyberbullying are some of the negative vices. Illegal downloading has led to problems such as copyrights and loss of large amounts of money from companies. Hacking can pose security problems and also be devastating to individuals, companies, or countries alike. Illegal downloading of software, movies, and most music has become an issue of concern. Some studies have tried explaining downloading and online piracy, and they include the social learning theory and self-control theory. Peers go online, find a copy of a movie and download it for free, download a CD illegitimately under these circumstances. As a result, the social learning approach associates deviant peers with an increased likelihood of committing software crimes, movie or music piracy. Research concerning digital piracy and self-control is scarce and often done in

conjunction with social learning theory. The peers would go to the website with the intention of downloading the CD under this circumstance (Patney, 2017). This does not specify whether the CD is a movie, music or software. Thus the author encompassed all the possible types of digital piracy, and at the same time being difficult to differentiate them. Thus, low self-control and the impulsivity subscale are significantly associated with the intention of illegal privacy.

Indian Cybercrime Laws

The modern driven age and ensuring online privacy is becoming a major challenge. The exponential growth in the internet use presents both advantages and disadvantages. The initial cybercrime case was recorded in 1820 and the incidences have continued increasing daily thus triggering a lot of emotional, legal and political responses(Rana, 2018). The cyber laws in India are part of the general legal system dealing with cyberspace, internet and their respective legal issues(Rana, 2018). Cyber laws mainly cover the various elements including the freedom of expression and access to usage of the internet and ensuring online privacy. The information Technology Act of 2000 was passed in India and its main role was to deal with the cybercrime and the electronic commerce. The law was reviewed and emended in 2008 to incorporate section 66A which penalizes people for sending offensive messages(Rana, 2018). In addition, section 69 allowed the authorities to monitor and decrypt information through the computer resources. Furthermore, laws were developed to protect children from porn and other harmful materials. People transmitting absence or abusive materials online or in electronic form are subject to punishment as per the Indian legal system. In addition, the Indian Computer Emergency Response Team was created as an agency to respond to the computer security issue as per the definitions in the Information Technology

Amendment Act 2008 (Rana, 2018).

Comparatively, cyber police were the strongest amongst all the agencies in tackling malicious online activities (Efthymiopoulos, 2016). The control went above beyond the imagination of people from the outside world. Users should only go online and do what is right or else be tracked down by the police. Those found guilty would be blacklisted, secretly detained and investigated or even publicly arrested. Those who violated the laws and regulations would face punishment of different severities depending on the crime committed. However, the actual controllability of online misconducts have been weak, this is due to outdated computer protection equipment imported in the 1980s and 1990, and the related slow development of computer protection products.

The major means for the control of cybercrimes was a blockage. This was to create an 'internet' exclusively with the Indian internet. This once seemed impossible, but later it materialized, this included limiting access to banning certain contents. The most effective way to control online activities was through control over access to the network. In the 1990s and early 2000, cyber cafes were a very popular business in India, which was facilitated with the then newest generations of computers and fastest network connections (Li, 2015). This could become the center of law enforcement as online conducts and messages could be tracked here. As a method of blockage, closing down of cyber cafes was an idea which was greatly welcomed by the police officers, which in other terms could benefit them by ways of transferring equipment under their control or by taking bribes from owners of the businesses (Jaishankar, 2018).

Surveillance by the governments can be an important measure of deterring the cybercrime levels in the society. Additionally, society can be educated on the measures of crime prevention and mitigation. The International Conference

on Cyber and Computer Forensics is enforcing international relations aimed at fighting the cybercrimes; however, the success of such measures depends on the willingness of the various nations to enforce policies that deter the crime. For example, the Indian Information Technology Act deals with the acts where the computer is used as a tool for a criminal offense (Sarre, Lau, & Chang, 2018).

Internet was introduced sometimes back, and it presents various advantages to the users. The increasing advantages of the internet make it pleasing to many people. As a result, the number of people using the internet on a daily basis continues to arise. The increase is also attributed to the social sites where people can interact in a virtual environment and communicate with one another (Farrell, & Birks, 2018). The communication role attracts new users each day. Unfortunately, some of the users do not understand the potential threats they are likely to encounter from the internet use. For instance, some people may come across non-useful materials such as pornographic material which is harmful especially to the youths.

Additionally, lack of proper security measures caused by lack of awareness also contributes to the increasing threats resulting from the internet use (Udris, 2016). However, the global integration works to ensure that internet users are safe and can only surf contents they have strategically planned to access. On the other hand, total inhibition of the cyber threats cannot be achieved 100% because the perpetrators use new techniques daily. The uniqueness and dynamic nature of the techniques used by the cyber offender limit the application of the international policies (Moore, 2014).

Educating the public on the threats of cybercrime is an important and essential step of reducing the negative effects associated with the experience. The awareness ensures that the users keep their accounts safe by having secure passwords and being cautious with the people they interact with online considering that some of them are unscrupulous and uses the internet to propagate their criminal purposes (Brewer, Cale, Goldsmith, & Holt, 2018). The reason why the internet has become a good harbor for getting criminal victims is that there are many people using internet on a daily basis and some of them are innocent and naïve; they have limited understanding of cybersecurity. Therefore, educating the public will help sensitize them to be cautious and avoid being caught up by the tricks users by the cybercrime offenders (Jaishankar, 2018).

The address of the cybercrime threats can also be explored from the theoretic perspective. Various theories exist that explain why cybercrime exists; therefore, the international bodies associated with cyber criminology can apply the theories in developing reliable and ethical regulation and policy framework that prevents the penetration of the criminal act. For instance, the social learning theory and the routine activities theory among others are the commonly used ones in the explanation of the incidences of cybercrime; however, their applications have not been fully developed (Jaishankar, 2018). Additionally, the space transition theory explains the nature and behaviors of the individual engaging in the cybercrime. According to the space transition, people's behaviors vary from one person to another when they move from one space to another. However, it is important to note that not all people occupying a similar space behave similarly. There is a need to explore the concept of cyber criminology from the global perspective further to understand its scope of operation for easy development of appropriate measures to curb it(Jaishankar, 2018).

Internet use continues to grow daily, and it has become accessible due to its great importance(Brown, 2015). On the other hand, the combination of the increasing usage and

the global threat require that legal responses are developing to address the possible harms likely to be caused in the society (Brown, 2015). There is a need to identify both the criminal and their territorial competences to effectively fight the increasingly global threat. Identification of the internet offense perpetrators is still a major challenge in the current society, and this has made it difficult to fully impose the legal responses to the threat. The anonymity presented by the internet challenges both the police involved in the investigation and the judicial principles of the individual nature of the penalty. There is a need to develop adequate measures to counter cyber threats (Gillespie, 2015).

The cybercrimes go hand in hand with the political goals and demands; as a result, this poses a major challenge in addressing the issue fully. The liberal democracy is based on the fact that people have the freedom to debate their political views and the messages presented on the internet. The greatest challenge emerges when the states are incapable of reaching the agreement of the universal definition of the crime. The cybercrime is a concept that has been discussed widely with some scholars arguing that it should only be limited to the cyber-attack which are done by the terrorists. On the other hand, some scholars contend that it ought to involve all the use of the internet for terrorism only.

Theories Used in Guiding Global Legal Response to Cybercrime

Hacking, which originally had a positive connotation and was attributed to individuals with exceptional skills for being able to hack or find shortcuts, has been distorted. Social learning theory has been used frequently to analyze hacking. The measurements of hacking included items such as ; "tried to guess another password to get into his or her computer files or

account", "accessed others' computer account or files without his or her knowledge", and "wrote or used a program that would destroy someone's computerized data such as a virus, logic bomb or Trojan horse". Both differential association and differential reinforcement/punishment are both significant predictors of the aforementioned hacking behaviors (Brewer, Cale, Goldsmith, & Holt, 2018).

Besides the social learning theory, self-control theory has also been frequently used to study hacking; it is most widely used in criminology. While some hackers argue that being a hacker means having self-control, discipline, and commitment to learning systematically. However, previous studies have shown that there is no connection between self-control and hacking intentions. A group of researchers however strongly suggests that there is a strong connection between self-control and hacking in a significant way (Brewer, Cale, Goldsmith, & Holt, 2018).Apart from these two theories,parent-child relationship and depression enhance willingness to hack and risk propensity and rationality to hacking behavior. Also, introversion has been associated with hacking and related computer crime activities.

As the spread of technology and internet advances, more issues concerning cyber deviance are expected. Family, school, and neighborhood play different but significant roles in cyber deviance. According to Yar et al., 2005, hacking culture encourages more males to engage in the activity than females; For instance, his study found hacking to be overwhelming among males (8.29% versus 2.5% females). When it comes to downloading, gender distribution is more even -54.60% of males versus 42.24% of females. The biggest predictor for both was the easy access to computers at home; this suggests that affordability plays an important role. Computers at school get monitored easily and put more constraints on what should be downloaded,

furthermore download of illegal staffs can call for punishment or even expulsion from school.

Gender and grade are significant predictors of both downloading and hacking. For downloading, males were 1.46 times more likely perpetrators; however, when it comes to hacking, the difference was much more pronounced: up to 2.85 times more likely than females. Having a positive attitude towards violent behaviors was a significant predictor for downloading and hacking. Positive attitude toward violent behavior is linked to both physical and verbal violence.

Secondly, Parental attachment plays a significant role in cyber deviance; therefore, some of these social factors must also be considered in ensuring the effectiveness of the measures used to prevent cybercrime. Having a bad relationship with either mother or father have identical negative associations with downloading. In contrast, the odds ratio for getting along with mother was twice the size of the father regarding hacking. Parental control, such as knowing the respondents' friends is significant in knowing their deviant behavior. Furthermore, effective parenting has been shown to foster high levels of self-control which in turn can theoretically reduce the chance of downloading and hacking due to low self-control (Kostakos, 2018). In addition, school bonding is significantly and negatively associated with both downloading and hacking. Several studies have shown that increased attachment to school promotes conforming behavior, whereas lower school attachments have been associated with bullying, and later initiation to deviant behaviors such as drinking and smoking, delinquency and cyber victimization. School disorganization is also positively associated with downloading and hacking.

Lastly, neighborhood integration is significantly and negatively associated with downloading. The neighborhood disorganization relatively showed a less significance to the deviant behavior.

This statement seems awkward, however, if a neighborhood is described as well- off or organized, which should be the antithesis of social disorganization for instance, neighborhoods that have been associated with community problems in general, poverty and deviant behavior. This is possible that affordability and socioeconomic status are the factors to be considered. Middle-class children access the internet more often thus the prevalence connection between more frequent downloading, better neighborhoods and neighborhood attachments.

Government institutions all over the world are aware of the need to take legal actions and limit the progress of cybercrime; for example, President Barrack Obama declared the digital infrastructures in America as a national asset and developed the Cybercom, a unit that would regulate all the internet activities in the region. On the other hand, other nations still lack the capabilities to impose appropriate security measures to eliminate cyber threats. For example, the United Kingdom government leaders are not adequately prepared to foster security against cybercrimes and attacks. As a result, they announced the development and investment into measures and policies that would promote the defense of the National Cyber Security. Furthermore, the NATO has been raising awareness on the need to develop international laws applicable to the cyber warfare globally. As a result, it presents that cybercrime affects nearly all nations in the world and it is an issue in the global domain that must be addressed in time.

Various theories have been published to address the cybercrime at the global level; popular cybercrimes indicates that a lot of things are conducted differently by various people. Therefore, the theoretical framework to the analysis and regulation of the threat is embedded in the legal-political measures, innovation and the monetary talks among others. The legal-political framework requires that international

bodies investigate and develop standards that should apply to all nations globally.

Integrated Responses and International Conventions

The core mechanism concerning the responsibility and control over online services was the liability of both macroscopic and microscopic approaches in both central and local government. If officials were regarded as negligent when malicious conduct happened, they could equally face criminal or administrative punishments. The purpose of this regulation was to enhance state stability (Li, 2015). This is because many people than ever had started using the information networks to propagate their anti-revolutionary, liberalist, and separatist ideas made more complains and expressed more discontentment. Unlike China, other countries have exposed free information that is useful to commerce and technology, China's regulation on the internet was designed to eliminate harmful information while conserving useful information. While people from other countries worried that this regulation would have a negative impact on the protection of human rights and the development of the economy, which is just contrary to the internet spirit (Li, 2015).

Cybercrimes are mostly missed in the criminal justice area, and this oversight indicates the difficulties encountered in the criminal equity realization. The under-detailing of the cybercrimes is a major issue in fighting them at the global level. Fighting cybercrime can be described as the war that operates within the air as the media (Lee, & Sanchez, 2018). Therefore, the war against the cybercrimes requires a full understanding of the domain shape and exploring the principles of kinetic warfare (Hamin, & Rosli, 2018). The fight against cybercrimes is based on eight principles which include the dual use, the information as the environment of operation,

control of infrastructure, kinetic effects, and lack of physical limitation, stealth, inconsistency, and mutability (Udris, 2016).

The convention of cybercrime is the only binding multilateral treaty that has been used in combating the cybercrime. The convention was drafted in 2001, and it provides a good framework on the cooperation between the various parties, and it was open to ratification for the nations that are not members of the Council of Europe. This is an example of a substantive multilateral agreement that was mainly objectively developed to address the cybercrime threat (Lee, & Sanchez, 2018).

The convention attempts to cover the crimes of illegal access and criminal associated with the wrong use of the internet. Also, offense perpetrates by the use of computer systems such as the computer-related frauds the provision addresses transmission of immoral materials such as pornographic. As a result, the convention completely addresses some of the issues that were being left out by the scholars initially (Kostakos, 2018). The convention has a binding framework that addresses computer-related offenses, offenses against confidentiality such as infringing into the accounts of the companies or even national system to steal information and then criminal copyright infringement. According to article 23 of the convention, the arrangement on the legal framework is based on the development of standardized systems to promote integration among the global countries. As a result, the nations are expected to get into bilateral treaties (Gercke, 2012).

The Convention on Cybercrime of the Council of Europe remains one of the relevant international legal system governing the cybercrime and electronic evidence. Also, the level of cooperation among the members continues to increase as the treaty evolves to accommodate the new and emerging tactics used in the cybercrime field (The Budapest Convention on

Cybercrime: a framework for capacity building, 2016). The conventional operation and formula of success are based on the dynamic triangle. Its operation is guided by the need for strengthening the security and confidence in the IT sector and reinforcing the rules and laws protecting the human right from cybercrime (Keyser, 2017). The convention provides the common standards to be undertaken when investigating cybercrime and the international police and judicial cooperation. Also, the criminalization of the cybercrime victims is based on the treaty. Also, the convention leads to the formation of other international bodies such as the Global Cyber Space Conference which protects nations from Europe, America and some of the African nations.

The international integration is important in ensuring a successful fight against cybercrime threats globally. The development of the international standard as evident in the NATO conference is the key to ensuring that all nations read from the same page when it comes to addressing computer-related crimes. Considering that cybercrime occurs in a virtual environment with no physical boundary, the national regulatory measures may not be successful since people can still perpetuate the crime from any part of the world. Developing the global legal framework is the key and important in the realization of safe internet use (Miquelon-Weismann, 2017). As the use of internet continues, so does the need to develop international legal frameworks emerge. Technology presents a lot of advantages to the users, and this means that people cannot be banned from using the internet; however, policies must be developed to control the content posted on the sites as well as internet activities that may have harmful effects to the online users. However, as nations develop the integrated cybersecurity measures, it is important that guidelines are developed to handle the hearing and prosecution of the cybercriminals. For example, in case a person commits the crime in

a nation by operating from a different nation, where will that person be prosecuted? The integration will make it easy for the offenders to be caught and legal actions were taken against them; however, there are some aspects in the global legal framework dealing with cybercrime that must be addressed. Cyberstalking is mainly caused by the victims; therefore, it is also within the responsibility of each internet user to ensure that they uphold appropriate security measures. The implementation of the measures developed by the international bodies can only be a success if internet users are willing to adhere to them.

Furthermore, tight legal and regulatory frameworks have been gradually introduced through the cyber police who are mandated with surveillance and monitoring of the activities undertaken by the internet users. Therefore, even as the issue of the legal framework in addressing cybercrime from the global perspective gets a significant concern, it is important to explore the future of cybercrimes considering that technological advancements continue to occur. The intensity of cybercrimes increases with technological developments.

According to Mittal & Sharma (2017), the transnational aspect of the cybercrime came along with various issues of sovereignty and jurisdictions which must be addressed for effective cooperation. As a result, there is a need for the transnational conventions to unite all the nations and enhance the cohesion among the nations as they fight against cybercrime. For example, the Council of Europe Convention on Cybercrime is the only effective international body dealing with cybercrime, the body alone cannot eradicate the crime; as a result, there is a need to form other conventions to support the agenda of the Council of Europe Convention on Cybercrime. Also, the non-member states of the international bodies should join to echo a common voice against cybercrime.

Conclusion

In as much as various measures have been developed to address the increasing incidences of cybercrime at the global level, the enactment of the global legal measures still receive various challenges. Some of the challenges include definition of the cybercrime and the acts defining the crime. In addition, the boundaries between cybercrime and the traditional crimes continue to increase. The development of international conventions were meant to help address the cybercrime incidences; the international integration in cyber criminology presents a good solution in the future considering that they are dynamic and changes with time to address comprehensively the changing nature of cybercrime.

References

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents. *International Journal of Cyber Criminology,* 12(1).

Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology,* 9(1), 55.

Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship*, 5(1), 11.

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop?. *Crime Science*, 7(1), 8.

Gercke, M. (2012). *Understanding Cybercrimes: Phenomena, Challenges, and Legal Response.* International Telecommunication Union.

Gillespie, A. A. (2015). *Cybercrime: key issues and debates*. Routledge.

Hamin, Z., & Rosli, W. R. W. (2018). Cloaked By Cyber Space: A Legal Response to the Risks of Cyber Stalking in Malaysia. *International Journal of Cyber Criminology,* 12(1).

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution, and Impact1. *International Journal of Cyber Criminology*, 12(1).

Jigar S. (2016). **A Study of Awareness About Cyber Laws for Indian Youth**. International Journal of Trend in Scientific Research and Development (ijtsrd), 2456-6470, 1-1.

Kerstens, J., & Veenstra, S. (2015). Cyberbullying in the Netherlands: A criminological perspective. *International Journal of Cyber Criminology,* 9(2), 144.

Keyser, M. (2017). The Council of Europe Convention on Cybercrime. In *Computer Crime* (pp. 131-170). Routledge.

Kostakos, P. (2018). Public Perceptions of Organised Crime, Mafia, and Terrorism: A Big Data Analysis based on Twitter and Google Trends. *International Journal of Cyber Criminology,* 12(1).

Lee, G., & Sanchez, M. (2018). Cyber Bullying Behaviors, Anonymity, and General Strain Theory: A Study of Undergraduate Students at a South Eastern University in the United States. *International Journal of Cyber Criminology,* 12(1).

Li, X. (2015). Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology,* 9(2).

Miquelon-Weismann, M. F. (2017). The convention on cybercrime: a harmonized implementation of international penal

law: what prospects for procedural due process?. In *Computer Crime* (pp. 171-204). Routledge.

Mittal, S., & Sharma, P. (2017). A Review of International Legal Framework to Combat Cybercrime.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Patney, V. (2017). *Asian defense review 2016*. New Delhi: KW Publishers Pvt Ltd in association with Centre for Air Power Studies.

Rana, R. (2018). Cybercrime in India: A study of legal response with special reference to Information Technology Act, 2000. *GLOBAL JOURNAL FOR RESEARCH ANALYSIS,* 6(5).

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends.

The Budapest Convention on Cybercrime: a framework for capacity building. (2016, December 7). Retrieved from https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime

Udris, R. (2016). Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study. *International Journal of Cyber Criminology*, 10(2).

Avoiding Self Inflicting Injuries- Sec. 65 B, IEA

The evolution of electronic evidence admissibility standards in Indian legal system

Dr. Mohit Kumar Garg, IPS[*]

Information Technology (IT) has revolutionized the lives of the people. With its advent, the public sector as well as the private sector, are betting high on e-governance. These governance initiatives have further enhanced the scope of IT and computers in our lives. This has not even spared the field of police investigation from its influence. Now, because of the pervasiveness of the IT gadgets, police officers have to deal with electronic evidence every now and then. Sometimes, because of the lack of clarity over the legal provisions regarding the admissibility of the electronic evidence, both because of varied judgments with conflicting opinions as well as because of lack of awareness among the police fraternity, police officers, many a time, tend to fail in their dealings with the electronic evidence. To prevent such failures, the prosecution must understand the evolution of the legal standards and the contemporary status in this regard. This is also the crux of the topic of discussion in our hand.

In this article, I want to discuss with the evolution of legal provisions related to the admissibility of electronic evidence. While discussing the evolution, we will start with the scenario prior to Information Technology Act, 2000 (henceforth IT Act, 2000), the change which IT Act, 2000 brought and its interpretations by the courts from time to time. At the end, we will summarize the current legal requirements for the admissibility of the electronic evidence in the court of law.

Legal environment prior to IT Act, 2000

Prior to the advent of IT Act, 2000, the judiciary was using the Indian Evidence Act (henceforth IEA) provisions of Sec. 61 to Sec. 65. Sec. 61 states

> *"Proof of content of documents – The contents of documents may be proved either by primary or by secondary evidence"*

So, earlier, the Indian legal position was that to prove the contents of the documents either primary evidence or secondary evidence needs to be produced. Sec 62, IEA states that

> *"Primary evidence: - Primary evidence means the document itself produced for the inspection of the Court. . . . . . ."*

This is self evident. For the evidence to be declared as primary, its original copy needs to be produced. The process of compelling the production of the document in court is called 'discovery'.

Section 63, IEA introduces the concept of secondary evidence. Sec. 63, IEA states that

Author Intro:

* Officer in Charge, Manipur Cyber Crime Police Station

"Secondary   evidence.—Secondary evidence means and includes—

(1)   *Certified copies given under the provisions hereinafter contained;*

(2)   *Copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies;*

(3)   *Copies made from or compared with the original;*

(4)   *Counterparts of documents as against the parties who did not execute them;*

(5)   *Oral accounts of the contents of a document given by some person who has himself seen it.....*"

As the original electronic evidence happens to be in the electronic form, the discovery of the electronic documents as primary evidence was not possible. So, for all practical purposes, the stored electronic data was treated as document and its secondary printed and signed form was introduced. Under certain circumstances, this type of signed evidence, called secondary evidence, is permissible. Sec. 65 states that

" Cases in which secondary evidence relating to documents may be given.- Secondary evidence may be given of the existence, condition, or contents of a document in the following cases:- When the original is of such a nature as not to be easily movable;. . . . . . ."

So, in India, before 2000, electronically stored information was treated as a document and secondary evidence of these electronic 'documents' was adduced through printed reproductions or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify her signature in the court and would be open to cross examination.

This simple procedure met the conditions of both sections 63 and 65 of the Evidence Act. (Acharya, Anvar v. Basheer and the New (Old) Law of Electronic Evidence, 2014)

In this way, prior to IT Act, the print outs or CDs were introduced to the court in the form of secondary evidence (as defined u/s 63, IEA) because of the inability to produce primary evidence (as per Sec. 65, IEA). Although, these sections were broad enough to cover the issues related to electronic evidence, broadly, but because of the special vulnerability of these types of evidence to tampering, hardware/ software malfunctioning etc., the need of having a special act was felt. To fulfil this need, following the examples of other countries, a special act was legislated.

Post IT Act Legal Scenario

As the volume of electronic transactions was increasing, the govt. thought it right to legislate a new IT Act. This act brought many changes with regard to the admissibility of the electronic evidence.

Amongst other things, it amended Section 3 and Section 59 of IEA The words 'electronic record' were introduced in section 3 (the definition of evidence) and section 59 (to exclude this from the ambit of oral evidence to prove its contents). It also, introduced Sec 22A, 45A, 65A and 65B to the IEA. With these changes, the act tried to bring clarity and specificity, so that law may come in sync with the technological evolution.

For the reference, the various changes, which have been brought by this act, have been reproduced here.

"65A. Special provisions as to evidence relating to electronic record.—the contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. Admissibility of electronic records.—

*(1) **Notwithstanding anything** contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) **shall be deemed to be also a document**, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and **shall be admissible in any proceedings,** without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.*

*(2) **The conditions** referred to in sub-section (1) in respect of a computer output shall be the following, namely:—*

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) ....

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,—

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human

intervention) by means of any appropriate equipment. Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process."

After the thorough reading, we may deduce the following principles.

Principle 1: *The omission of introduction of the words 'electronic records' to section 61 to 65 of IEA was intentional.*

We can see that the legislature has introduced the words 'electronic records' to sections (3) and (59) but has avoided such introduction to section 61 to 65 of IEA. Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. In this regard, the Apex Court in *Utkal Contractors and Joinery Pvt. Ltd. V. State of Orissa* held that

> " . . . *Parliament is also not expected express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for . . .*"

In the way, it's the cardinal principle of interpretation that if the legislature has omitted to use any word, the presumption is that the omission is intentional.(Arora, 2015) So, for the electronic records, these sections (sections 61 to 65 of IEA) will not be applicable. The legislature introduced section 65A and 65B for this very purpose.

Also, the same principle may be derived by reading the section 65(B) of IEA, which starts with the ' non obstante clause' of 'not withstanding anything' contained in this act'. It becomes amply clear that the legislatures wanted only sec 65(B) to be applicable for the electronic records admissibility (and not Sections 61 to 65).

Principle 2: *A certificate is a must to authenticate electronic record.*

Section 56(B)4 of IEA requires one certificate from the controller or administrator of the computer. This is to certify the authenticity of the document.

Principle 3:*The scope of the certificate, given u/s 65(B)4, extends till the best of person's knowledge and belief.*

The section specifically mentions that in the certificate it may be stated that the content of it is "to the best the knowledge and belief"of the person providing the certificate. This is very much required as the person is giving the certificate in good faith of what the person sees under the given situation. For instance, the content of the same website may change with the change of places, time and person. This is because many a time the content is user specific. For example, advertisement may differ with respect to the place. Another common example is Facebook page content. Facebook also, uses behavior analytics and shows user specific content on its wall. Considering this, the incorporation of this clause becomes important.

Principle 4: *Section 65B of IEA (in that sense sec 65 B (4) also) is concerned with only the 'admissibility' of the electronic evidence.*

Sometimes, some people wrongly infer that if the 65 B certificate is produced then it ensures the genuineness of the electronic record. They infer that there will be no cross examination. Their understanding is sometimes reinforced by the confusing judgments of the courts. Actually, it should be made clear that this certificate only authenticates the source and the content of the record. So, in a way, this ensures admissibility. After the admissibility stage is passed, to prove the genuineness, the court may take the refuge of section 45 A, IEA (read with section 22A, IEA) to validate its genuineness.

Principle 5: *Electronic record should be deemed to be a document (Sec 65 B (1).*

This implies that 'electronic record' should not be further classified as ' primary' or 'secondary' document. We will see in the later discussion as to how the Apex Court confused this aspect in Anvar vs Basheer Judgment. If at all, we want to understand electronic record in these terms, then, at best, it may be considered as secondary evidence, nothing else.(Acharya, Anvar v. Basheer and the New (Old) Law of Electronic Evidence, 2014)

Principle 6: *The 'Computer' for the purpose of Sec 65B, IEA, is the one from which the print out/ CD is directly taken.*

It must be noted that many people sometimes get confused that the Sec 65 B certificate will be given by the web server's administrator. But, to my understanding, this is a flawed and infeasible interpretation. The certificate will be given by the administrator/ lawful controller of that computer for which the print out or any other representative of electronic record, has been taken. For this interpretation, the following reasons may be cited:

a) This certificate, as we have already discussed, is only for the admissibility of the electronic record. This provides for the most basic level of security check to the court. The genuineness will be proved in the later course of the trial. So, the IO, after getting this certificate from the concerned person (administrator or controller of the said computer) will be certain that he would be able to introduce this evidence (electronic record) in the court of law. Then, in the later course of his investigation, IO may further drill into the evidence and may consult/enquire from the administrator of the web server or from his legal team to ascertain the genuineness of the electronic record. This is what police officers/ investigators normally do with the Facebook and other social media related cases.

b) There may be a case, for instance, in when a single bank account data may be a result of the compilation of the entries made by several different computers. In such scenario, getting the Sec 65 B certificate from all different computer administrators will be infeasible. In other words, if we are looking at the computer of the bank where the statement of account is compiled, it may involve multiple computers from which different data base elements are dynamically drawn to compile a viewable document. Also, there could be multiple owners of such computers including the owners of Internet routers through which the data passes through. (Na, 2016)

Principle 7: *Not all print outs of the electronic evidence need Sec 65 B certificate.*

Here, we need to differentiate between two situations. In one situation, we are using computer to print out the content which was originally not generated by us. For instance, the contents of the Facebook wall, the bank account statements, any website, etc. are not directly generated by the person who is viewing on his screen. If he/she gives the print out of such content, then he/she will have to provide Sec 65 B certificate. Only then will the electronic record be admissible in the court. But, in the second situation, we might be simply using computer as a type writer. To the best of my reasoning, in such scenarios, if the person, who has typed the content or who is the generator of the content, signs the printed out document, then, there will be no need for section 65 B certificate.(Na, 2016)

In this way, through these principles, which we have deduced from the understanding of certain important provision of IT Act, we have seen that this act was an attempt to specify the procedure so that all the courts may follow the same standards with regard to the electronic evidence. Unfortunately, Indian courts, especially the

lower ones, have been inconsistent in upholding the provisions of the law. In the following case, laws will prove this fact.

Afsan Guru Case [State (N.C.T. of Delhi) vsNavjotSandhu @ Afsan] Any 4, 2005

This case, which has been famously called as parliament Attack case, was one of the first cases, in which the two Judges Bench of the Apex Court had to deal with the conundrum of Sec 65 B certificate. The Honourable Court, while deciding upon the admissibility of the printouts of the computerized records of the calls (also known as CDR, Call Data record), held in Paragraph 150 as follows:

"150. According to Section 63, secondary evidence means and includes, among other things,

"Copies made from the original by mechanical processes which themselves ensure the accuracy of the copy, and copies compared with such copies". Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not a dispute that the information contained in the call record is stored in huge servers which cannot be easily moved and produced in the court. That is what the High Court has also observed at Para 276. Hence, printouts taken from the computers/ servers by mechanical process and certified by a responsible official of the service providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the provisions of the Evidence Act, namely, Section 63 and 65. It may be that the certificate containing the details in sub section (4) of section 65-B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if

the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, Section 63 and 65".

Therefore, in a way, the judgment upheld the validity of alternative mechanisms other than 65(B) certificate in validating the admissibility of electronic records. The court specially mentions the importance of Section 63 and section 65 in this regard. Following this verdict, recently in 2010, in the case of Ratan Tata V. Union of Indian write petition (Civil) 398 of 2010, a Compact Disc (CD) containing intercepted telephone calls was introduced in the Supreme Court without following any of the procedure contained in the Evidence Act. (Acharya, Anvar v. Basheer and the New (Old) Law of Electronic Evidence, 2014)

But, we have already discussed that because of 'non obstante clause' in Section 65 B, Section 63 and section 65 cannot be applicable for electronic records. So, we may assume that the court wrongly interpreted the IT Act. (We will see further that the Apex Court would overrule this verdict in the judgment of Anvar vs Basheer Case in 2014.)

Anvar P.V. Vs P.K. Basheer and other Case (Supreme Court of India Appeal No. 4228 of 2012)

The three-member bench of the Apex Court consisting of Justices R.M Lodha, Kurian Joseph and RohintonFaliNariman, overruled the judgment of the Parliament Attack Case as far as the admissibility of the electronic record was concerned. Though, the case was related to an election issue, the judgment discussed in detail about the digital evidence aspect, also. While referring to the Navjot Sandhu case (Afsan Guru case) judgment the court laid down that :-

"Generaliaspecialibus non derogant, special law will always prevail over the general law. It appears, the court omitted to take note of sections 59A and 65 A dealing with the admissibility of

electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by sections 65A and 65B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this court in Navjot Sandhu case (supra), does not lay down the correct legal position. It requires to be overruled and we do so. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible."

So, the important inference which we may draw is that "being a special law, the general law under Section 63 and 65 has to yield." it simply means that for electronic records, IO will have to fulfill the conditions of Section 65B, without which the record can't be admissible. In this way, this judgment has established one unique procedure, upon which prosecution may relay.

But, at the same time, this judgment is also not without criticism. The following drawbacks in the judgment may be mentioned:

1. The judgment differentiated between primary electronic evidence and secondary electronic evidence. It held that secondary electronic evidence may be admissible only after fulfilling Sec 65 B condition, while primary electronic evidence may be admitted to the court even without Sec 65B certificate.

To quote:-

"An electronic record by way of secondary evidence shall not be admitted in evidence

unless the requirements under Section 65B are satisfied."

It continued to state

"in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible."

It also stated,

"The situation would have been different had the appellant adduced primary evidence, by making available inevidence, the CDs used for announcement and songs. Had those CDs used for objectionable song or announcements been duly got seized through the police or Election Commission and had the same been used as primary evidence, the High Court could have played the same in court to see whether the allegations were true."

In our initial discussions on the provisions of IT Act, under Principle 5, we have already dealt this point. The point which I want to make is we can't differentiate between primary electronic evidence and secondary electronic evidence. For all practical purposes, we may consider the electronic record to be a document of secondary evidence value. Moreover, to further substantiate my point, it may be mentioned that the videos even if original recorded (and not the copies of the original) and originally recovered from the scene of crime, would actually be in binary format of zeroes and ones. Human brain would only be able to see the video because of some intermediary software which would convert this into understandable videos. So, human/ witnesses would actually be able to testify only for the outer/cover/container of this binary data and not for this binary data, which is the actual content of the video. So in my opinion, for CDs to be admissible, the requirement of Sec. 65

(B) certificate should always be there. Contrary to this, for documents, on certain occasions, this requirement may be done away with (as explained in 'Principle 7').

2.   Supreme Court, in its judgment, introduced into the legislature some of the elements from nowhere. For instance, the court states that all the applicable conditions of Sec 65 B (2) must be specified in the certificate. No such language of applicability exists in the section. (Vaidialingam, 2015)

3.   Supreme Court has held that Sec. 65 B (4) certificate is the only door to make the electronic record admissible. But, for practical reasons, for instance, in the case of whistleblowers, there needs to be some alternative mechanism. As this case was an opportunity for the court to discuss all the relevant points in detail and plug all the loopholes, it missed this opportunity.

4.   Another major flaw with the judgment is regarding the requirement of contemporaneity in the production of the certificate. To quote,

> *"Thus, in the case of chips, etc, the same shall be accompanied by the certificate in terms of Sec. 65B obtained at the time of taking the document."*

This contemporaneity requirement is one of the reasons the electronic evidence in this case was not admitted. This clause of contemporaneity proves to be impractical and many a time acts as a road blocker; for instance, in whistleblower's case.

It must be mentioned that the Delhi HC in Ankur Chawla V CBI, recently applied the contemporaneity principle to declare the evidence inadmissible.

Paras Jain V State of Rajasthan

In 2015, another important event happened with regard to the evolution of the electronic evidence

jurisprudence. The Rajasthan High Court, in this case, had an opportunity to consider a situation, where contemporaneity clause stipulated by the SC in the Anvar Vs Basher Case was in question. In this case, the persecution had not produced the (right) certificate at the time of filing the charge sheet. They had produced the right version of the certificate during the course of trial.

The court dismissed the challenge against this delayed filing by the accused on the grounds that in Anvar "the question of stage at which such electronic record is to be produced was not before the Hon'ble Court."(Vaidialingam, 2015)

The HC explained this assertion on the basis of Sections 91, 173 (8), 231 and 311, CrPC.

Thus, it may be said that in all the cases where the police have not filed the certificate U/S 65 B IEA, the same can be filed by way of supplementary charge sheet U/S 173 (8) CrPC and this is no way even stops the police from generating the same electronic record as fresh and file in the court by way of charge sheet U/S 173 (8) CrPC.

So far, we have discussed the evolution of Indian legal position on the admissibility of electronic evidence in the court of law. We have seen that how the Indian jurisprudence evolved over the time. As the legal procedure has spread beyond the IT Act and because there have been many contradictory judgments, it would be better to summarise the contemporary rules about admissibility of electronic records-

1.   Procedure mentioned in Sec. 65 B is the sole procedure which needs to be followed to make the electronic record admissible in the court of law.

2.   If someone is the owner of the content, and he/she has reproduced it in the form of print out, then there is no need of Sec. 65 B certificate.

3. Sec. 65 B certificate will be given by the owner/legal controller/administrator of the computer, not of the server. The server administrator will give the certificate only in case when the electronic record is being taken from the server directly.

4. While giving the certificate, all the conditions stipulated under sec. 65 B, will not only have to be fulfilled, but also these will have to be mentioned in the certificate.

5. Prosecution may produce the certificate at any stage of trial.

These rules ought to be followed by every investigator. Not following these, is like a 'self inflicted injury' (term famously used by a US federal judge in Maryland in Larraine V.Merkel American Insurance Company Case), which may prove to be suicidal for the prosecution case. In all circumstances, we ought to avoid these self inflicted injuries.

Bibliography

Acharya, B. (n.d.). *http://cis-india. org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence.*

Acharya, B. (2014, September 30). *Anvar v. Basheer and the New (Old) Law of Electronic Evidence*. Retrieved May 29, 2017, from Centre for Internet and Society: http://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence

Arora, N. (2015, March 10). *Admissibility of Electronic Evidence : Challenges for Legal Fraternity.* Retrieved May 2017, from Neeraj Arora: http://www. neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/

Na, V. (2016, August 29). *Basheer Case Judgement and Section 65B of Indian Evidence Act...Cyber Jurisprudence develops.* Retrieved May 2017, from Naavi.org: http://www.naavi.org/wp/basheer-case-judgement-section-65b-indian-evidence-act-cyber-jurisprudence-develops/

Vaidialingam, A. (2015). Authenticating Electronic Evidence: S65B, Indian Evidence Act, 1872. *NUJS Law Review* (43), 43-66.

Improved Criminal Justice Delivery in NER: a pre-condition for "Act East"

Prasant N. Choudhury[1]

Jayanto N. Choudhury IPS (retd)[2]

Abstract

Militant violence has significantly dropped in the North-East region, especially Assam. To ensure investment and economic growth necessary to make "Act East" a reality, it is imperative to ensure a sense of security in the region. For this, it is necessary to increase the resources and upgrade the capacity of the police and engage communities in keeping peace. Long years of militancy in the region have slanted policing priorities towards anti-terrorist skills. The governance paradigm must now shift to development and civil policing. Parameters such as cases charge-sheeted and convicted are far below all-India levels in states like Assam and Manipur. This can be remedied only by addressing weaknesses in delivery of police services like investigation and prosecution capabilities of the criminal justice machinery. GoI has provided unstinting support to the states in effectively combating militancy. Now, similar innovative support is needed to "win the peace".

Keywords:

Security deficit – declining militant violence – delivery of policing services – secure north-east a pre-condition for 'Act East'

Introduction

Some years ago, one of India's largest corporate houses planned to set up a mega paper mill in an NER state, investing several thousand crores. Thousands of jobs would have been created by direct and indirect employment opportunities. Raw material, power, and water required for production were abundant; there were convenient road and rail links to markets for the finished product. The higher management had just one concern: the law and order situation – regular media reports of abduction of businessmen and executives, frequent and sudden 'bandh' calls enforced by violence, and a multiplicity of militant and 'socio-political' outfits that ran extortion rackets. Despite assurances from the highest political and administrative levels in the state, they finally took this investment to another part of India where these apprehensions were absent.

Is there a Security Deficit?

A modern state has multiple responsibilities to its citizens. Health, education, the right to livelihood and infrastructure are a few primary expectations. However, ensuring security of life and property of all citizens has been the historic *raison d'etre* of any state; assessing whether this

Author Intro:

[1]

[2]   Former DG, NSG & DGP, Assam

is being effectively delivered remains critical to any investment decision. It is the very keystone of "ease of doing business". Current demographic trends in NER, with a high youth bulge and disproportionate rural unemployment, require creation of adequate livelihood opportunities so as to avoid continuing public order issues and increasing crime trends. There may be other factors required for an eco-system that helps provide a sense of security–but an effective criminal justice machine is a *sine qua non* for good governance. NER has been plagued by multiple militant movements over the past half-century and major social agitations that have crippled normal working. This has led to a widely held perception of a security deficit in the region. In order to restore confidence, and to attract outside investment, the first step is to outline the current situation, diagnose deficiencies in the policing and criminal justice machinery, and identify possible remedies.

Changing security scenario

Militant movements have been an inescapable determinant of the law-and-order situation in the region since independence. Naga insurgency was the first in the 1950's followed by Mizoram, Manipur and Tripura in the 60's and the 70's, Assam from the late 80's and then Meghalaya, Arunachal Pradesh. Manipur continues to experience the highest incidence of violence today, mostly by valley-based militant groups, though violence levels are far lower than earlier. Fatalities in 2007 were 150 civilians, 40 SF personnel and 218 militants. In 2017, civilians and militants killed were 23 each and 9 SF personnel. The situation in Assam has changed even more dramatically; in 2000 over 400 civilians were killed by militants, 80 SF, and 330 militants also died. In 2017, 3 civilians were killed,5 SF and 18 militants.

This sharp drop in killings reflects the changed security environment in Assam over the past 30-40 years. In 1990, Brooke Bond Group had overnight evacuated its executives when faced with ULFA's extortion demands. The killing of Surendra Paul, the tea tycoon, abduction of tea estate managers and oil executives with several killed, murder of army-officers at Kamakhya temple, ambush of district SPs in broad daylight, and assassination of political leaders were the symptoms of the extreme breakdown of governance at that time. In the early years of this century, indiscriminate killing of tea-planters by NDFB, targeted killing of non-ethnic communities and indiscriminate acts of terrorism like the multiple bomb blasts in Guwahati (2008) had made life a nightmare for ordinary people. Worse, it led to a flight of capital and business skills from the state.

Criminal Justice delivery

Today, violence and militant influence are at far lower levels. Why then is there a continuing perception that the region is 'unfriendly' to investment needed for economic growth? Crime cannot be the reason: the incidence of reported crime in NER is just over 1.5 % of the annual 8 million cases reported countrywide, with most occurring in Assam (@100,000). This proportion roughly holds for most categories of serious crime like murder or property crimes. Only abductions and economic offences are higher – Assam records 10% of the 75,000 abduction cases registered all-India annually, and 5% of the 140,000 economic offences

The exceptionally high proportion of cases under special laws like UAPA(Manipur registered over 60% of UAPA cases across the country annually) and the high crime rate of offences relating to public order- at 16% double the all-India rate of 8%,gives a hint of sub-surface fault-lines(10% of all student agitations in the country are in Assam). NH-2 through Nagaland to Manipur has

been blocked by protesting groups for as many as 300 days in a year. At the same time, the Supreme Court set up an SIT in mid-2017 to probe into alleged 1500 plus extra-judicial killings in Manipur; the state that is also in the forefront of the movement to withdraw AFSPA. Moreover, the near absence of corruption cases registered despite a credible perception of widespread corruption, and negligible cases registered in this once heavily forested region under categories like the Forest Act, Wildlife Protection Act and Environment Act, are an indicator of weak enforcement of laws. This lacks engagement of communities in maintaining order is an aspect that may need to be carefully studied. NER is home to over 200 different ethnic communities and customary laws still play a role in several states. Even infrastructure initiatives intended to boost local development like highways or rail links, have been opposed by local communities who do not see any benefit since implementation is by mega construction firms from outside the region. In fact, many consider such infrastructure detrimental to the traditional way of life and only facilitating influx of outsiders.

An indicator of an effective modern justice system is the disposal of cases in the courts. All-India, the proportion of cases charge-sheeted by the police is 81%. In NER, Mizoram (91%) and Nagaland and Tripura (both 88%) exceed this, Meghalaya and Arunachal Pradesh average around 55%, Assam lags behind at 47% while Manipur is a dismal 13 %. All-India convictions rates are 46%., with Kerala securing over 80% conviction. In NER states, Mizoram maintains an impressive 93%, Nagaland an acceptable 70% while Manipur (44%), Meghalaya (37%), and Arunachal Pradesh (31%) are less than satisfactory. Assam at 12% is simply unacceptable. Of course, in quantum terms, trials of almost 30,000 cases are completed annually in Assam, as against less than 2000 in Mizoram and a mere 75 in Manipur. The sheer

volume of cases pending trial are swamping the judicial system. In Assam; almost 50,000 cases are added each year to a pending case load of almost 140,000. Yet trials are completed in only 30,000 cases annually.

Wanted: a different policing paradigm

Are weaknesses in policing and criminal justice systems in the region a result of inadequate resources, lack of capacity, or both? In order to tackle the multiple militant movements of the past, policing in the region was based primarily on deployment of large quantum of central forces while the State itself raised many armed battalions with some units specially trained in AT skills. For example, Assam has 29 state armed police battalions, Manipur 15, Tripura 12 and Nagaland 16 battalions. This lop-sided armed policing structure may need to continue for some more time, since conditions that generate militancy and ethnic violence have not completely disappeared. At the same time it is critical to increase strength of the civil police deployed in PSs, since it is this level that provides policing presence on the ground, and delivers policing services to citizens. It is the *thana* cops who ensure efficient prevention and investigation of crime and are the first-responders to law-and-order situations.

In Assam, just over 10,000 civil police personnel out of the total state police strength of about 60,000 are deployed in the 350 PSs spread over the over an area of 80,000 sq.kms. This works out to one PS covering about 250 sq. Kms with about 30-35 thana policemen for every 100,000 population. Policing of NHs and expanding rail network is grossly inadequate, affecting not just Assam but all the NE States. Tamil Nadu has 2½ times the population of Assam, has 5 times the number of PSs and almost 10 times the quantum of civil police. While research has shown that more policemen reduce crime, it is common-

sense that well-staffed PS, covering manageable jurisdictions will ensure more effective policing.

Certainty of punishment is as important as severity, and the dismal figure of convictions has to be improved. Perhaps dropping cases against militants as a condition for surrender may have affected the quality of investigation and prosecution. Compromises permitted as part of a counter-militant strategy included at times, turning a blind eye to extortion and intimidation by surrendered militants and arrangements like 'suspension of operations or 'cease-fire' whereby militants are paid a stipend and stay in camps (sometimes without surrendering weapons) pending a permanent resolution. This may have led to a collective consciousness even if subliminal, of condemnation of criminality. There are other factors like prolonged process of trials lasting a decade or more and a weak prosecution system that are beyond the purview of the police. What can be achieved to improve delivery of the policing services is better trained investigators which is why it is essential to upgrade training and forensics capabilities. At the same time a motivated police force is essential to better delivery of services; basic hygiene factors such as inadequate availability of housing, overwork and poor facilities need to be equally addressed.

Remedies

At the granular level, strengthening this system needs remedial measures aimed at weaknesses in both the investigative process and prosecution. Looking at only investigation is inadequate, since once the Final Form is submitted by the Investigation Officer (IO) before the competent court, it is the prosecution that follows up in court as laid down under provisions of Criminal Procedure, 1973 (as amended). Let us look at simple changes in the staffing and processes of the investigations and the architecture of

prosecutions that may make a difference. It's not rocket science; just simple and doable changes.

Investigation

Flaws in recording the FIR are a primary defect that weaken cases on trial. This is the first step in the investigative process and can be remedied if entrusted to a Literate Constable (LC) preferably with training in law who can record in precise form, the particulars of the crime. After being registered and endorsed to an IO, the same LC should be available to assist him through every stage of the investigation till preparation of the Final Form.

The existing Shrestha ASI at police stations needs to be trained and re-designated as Assistant Sub Inspector (Law). His role will remain oversight of General Diary entries and correcting of any lacunae, so that accurate facts along with seized evidence can withstand the rigours of examination-in- chief during trial.

The current Reader/Crime Inspector/Sub-Inspector at the district level needs to be strengthened and re-designated as Insp/SI (Law) and capacity developed to review case-diaries from all Police Stations/Police Outposts falling within the jurisdiction of a particular district SP. Flaws in procedure and inaccurately recording steps taken by the IO, during investigation are major reasons for the cases failing in court. An appropriate number of Inspectors (Law) with sufficient experience, are needed to monitor the progress of FIRs and investigation and give guidance should any lacunae be noticed.

It is imperative to build up capacity among field police officers to ensure greater knowledge of law and skill in investigation procedures. The prolonged militant scenario in the region placed a greater premium on militarized policing. Police officers posted against these law posts will need to be well versed in criminal jurisprudence

and criminal laws, procedure, and the Police Act with special expertise in maintenance of police diaries, all of which are required for effective prosecution of cases in both original and appellate courts. These Law Officers during the process of overseeing the cases at different stages of investigation upto final form, should separately keep accurate Note-Sheets of the Statement of Case at all stages. This will prove invaluable in case any of the accused approach the appropriate court for grant of anticipatory bail or should the accused flee to evade arrest, till such time as they can approach the competent court for their conditional surrender which may include a limited or no conditions of cooperation with the IO. These notes will be of immense assistance in resisting claims of the accused for the privilege of pre-arrest bail or a prayer of inter alia direction for a conditional surrender which may hamper the process of investigation .Further these notes would also be of tremendous help during prayer by the IO for extension of police custody, or forwarding to judicial custody with right to access the accused. This is also relevant because of the practice of many IOs to slap inappropriate sections of penal law, which unnecessarily invokes a judicial frown. That this is more so for specially constituted courts involving specified laws and special courts dealing with terrorism or corruption cases.

The growing tendency of imposing harsher sections than needed casts a shadow on investigation. Prime examples in courts across the country are against Lt. Col. Purohit in the Malegaon blast case, T. Raja (Former Telecom Minister) linked to the 2G scam, the Arushi murder and against Bhagya Kalita in the Karobi –Darobi murder case. A careful perusal of the judgment and orders passed in these cases reveals that lacunae in investigation were unable to support effective prosecution of these cases. Even the appellate courts endorsed the orders of the lower courts. These obviously reflect

an urgent need to upgrade capability of the investigators.

There is a common perception that poor quality of prosecutors and prolonged trials have affected the ability to deliver effective justice. There is also little doubt that the justice delivery system of NER needs to be revamped so as to provide speedier trials. However, the starting point for more effective delivery by the criminal justice system is better quality of investigation. The foundation for a strong case is the case dairy maintained for each crime investigated. It is essential to thoroughly document all stages of investigation to enable analysis at the time of framing of the charge, as to how each piece of evidence gathered during investigation supports prima facie material evidence. This will also make sure that on commencement of trial proceeding there is no wastage of valuable judicial time, and that the business of the court is not stalled due to some technical plea by the accused on points of law gleaned from materials supplied with the charge-sheet. These vulnerabilities in case records provide opportunities to disrupt the prosecution's calendar of trial and the need to conform to basic judicial principles, i.e. to prove all evidence "beyond reasonable doubt" and to complete the trial in the shortest possible time, since "justice delayed is justice denied".

Prosecution

The ruling maxim remains that "the Court is equally guilty if the accused is set free due to the poor prosecution". Technology can improve coordination between the IO and prosecution. The crime detail records can be posted online via a secure crime police record net connected to Director / Deputy Director of Prosecution (as provided for under Sec. 25 A CrPC) situated in the Police HQ/ H.Q of the Investigation Agency. Perhaps the existing CCTNS network can be extended to achieve this.

A critical requirement for an effective prosecution is the quality of PPs (Public Prosecutors). Those recruited through the UPSC may lack practical experience of appearing before courts. Incumbents are usually young lawyers who seek to gather experience before moving on to private practice. A critical contradiction is that the senior PPs representing a particular state agency get salaries from the Consolidated Fund of India and are technically employees of the state. Interestingly, the Bar Council of India's rule 49 restricts a salaried employee from practising as an advocate.

Similarly, section 2(c) of the Prevention of Corruption Act, 1988 defines 'public servant' as

(i) any person in the service or pay of the Government or remunerated by the Government by fees or commission for the performance of any public duty;

(ii) any person in the service or pay of a local authority;

(iii) any person in the service or pay of a corporation established by or under a Central, Provincial or State Act, or an authority or a body owned or controlled or aided by the Government or a Government company as defined in section 617 of the Companies Act, 1956 (1 of 1956);

Therefore fully employed public prosecutors are public servants technically violating the laws, and also contrary to provisions of Sec. 24 and 25Cr. P.C. Moreover, this practice has led to poorly prosecuted cases in view of the "Yes Sir" syndrome. On the other hand, practising advocates engaged as PP or Addl. P.P or Special P.P performs a public service without being public servants (Gujarat H.C Judgement dt. 16th June '17, Jalpa Pradeep Bhai Desai Vs. Bar Council of India &Ors, Supreme Court Judgement dtd.3rd Jan. 2001 Artish Kr. Sharma Vs. Bar Council of Himachal Pradesh).

Act East needs secure North-East

Policy makers stress a stable law & order environment as a pre-requisite for sustained development. That's because apart from physical infrastructure, access to finance and availability of suitable skills, a sense of security is indispensable for progress. UN Resolution 2151 states, "Good governance and the rule of law…are essential for sustained, inclusive and equitable economic growth, sustainable development and the eradication of poverty and hunger."Goal 16 of the UN's SDGs calls for strengthening relevant institutions, for building capacity at all levels to prevent violence and crime.

To move beyond aspirational rhetoric, the "Advantage Assam" initiative needs to first generate a sense of security. Better governance, an expanded civil policing system and an engaged community are potential game-changers toward making the region an attractive investment destination and a springboard to expanding economic links to South-East Asia. Not as a catalyst, but in partnership with other states like Nagaland and Manipur, Assam as a gateway to the region can work toward a 'secure north-east' conducive to economic growth that makes "Act East" a reality. In the past, the central government has been pragmatic in responding to security problems of the region, whether by creating 6th Schedule areas, engaging militant outfits in dialogue or framing and funding surrender policies. The generous support to raising India Reserve (IR)battalions and reimbursing SRE (security-related-expenditure) have all helped achieve today's improved security environment.

Now, Assam needs support to 'win the peace'. Av ital component is to strengthen the criminal justice system, including upgrading the capacity of civil policing services. A holistic not fragmented perspective is needed to achieve a better managed security environment. Recognizing the

need for a more broad-based approach, the 2nd Administrative Reforms Commission in its report on Public-Order (2007) made recommendations that include specialization of policing with law-and-order separated from investigation, greater investment in technology to support a scientific investigation, better training, and more "people-friendly" police.

Institutions like Niti Aayog that are looking at ways to improve governance could examine allocation of resources to policing required to achieve desired outcomes. At the same time, public representatives and opinion-makers in NER need to take up the baton to support building up of an appropriate policing system, using all available forums. The requirement to improve criminal justice delivery as an essential precursor to achieving declared economic objectives is "too important to neglect, too urgent to delay."

References

1. NCRB, MHA "Crime in India 2015"
2. BPR&D, MHA "Data on Police Organizations (as on Jan 1, 2017)
3. Address by Chief Minister Assam in the CM's conference on Internal Security, Vigyan Bhawan New Delhi June 5 2013
4. USI Strategic Review 2017. Jayanto N. Choudhury "Modernization of Police Forces for effective management of Internal Security Challenge

Note for Contribution

The Indian Police Journal (IPJ) is the oldest police journal of the country. It is being published since 1954. It is the flagship journal of Bureau of Police Research and Development (BPR&D), MHA, which is published every quarter of the year. It is circulated through hard copy as well as e-book format. It is circulated to Interpol countries and other parts of the world. IPJ is peer reviewed journal featuring various matters and subjects relating to policing, internal security and allied subjects. Over the years it has evolved as academic journal of the Indian Police providing critical inputs to the stakeholders of policing and internal security.

How to submit Article/Paper

The paper/article on crime, criminology, general policing, internal security, forensic science, forensic medicine, police organization, law and order, cyber crime, organized crime, white collar crime, crime against women, gender policing, juvenile delinquency, human resource development, police reforms, organizational restructuring, performance appraisal and service delivery, social defence, police family, police housing, police training, human rights, intelligence, corruption, terrorism and counter terrorism, community policing and allied subjects can be submitted.

The paper/article with keywords and abstract should be between 2000-4000 words. The paper/article should be original and have not been published in any journal. A brief detail about author should also be submitted. The paper can be submitted through email:editoripj@bprd.nic.in.

The paper/article can also be submitted via post with hard copy in duplicate and a CD on following address. **The Editor, The Indian Police Journal, BPRD, MHA, New Building, National Highway-8, Mahipalpur, New Delhi-110037**