The Indian Police Journal

Vol. LXII • No. 1 ISSN 0537-2429 January-March, 2015

The Indian Police Journal

Vol. LXII ● No. 1 ● January-March, 2015

The Indian Police Journal
January - March, 2015 • Vol. LXII • No. 1

EDITORIAL BOARD

CONTENTS

ON the occasion of 66th Republic Day, all the stake holders of internal security and the Indian Police in particular deserve to be congratulated for their dedication and commitment in providing Indian Republic and Democracy a secure and solid foundation. Despite various odds and the archaic laws hamstringing our police in executing its mandate, they have been persistently and actively participated in the nation building.

In this issue of the Indian Police Journal, we have dealt with the issues ranging from subaltern perspective of the criminal justice system and its reform, the role and need of public relations in policing, cyber policing, and gender policing.

Since long the problems of policing in the country are being discussed but steps have been taken to bring about reforms. But still we have to go a long way and much needs to be done. The shooting crime graph, plummeting conviction rate and overcrowded prisons-- all these underline the need of speedy implementation of the Criminal Justice Reform.

The views from field emerging out of various studies and reports also underline the urgency of the elusive reforms. The negative image and perception about the Criminal Justice System that has surfaced from the field studies tally with the bottlenecks afflicting the implementation of proposed reforms. The various studies and reports in general and that of subaltern ones in particular point to the fact that the police, prison, and judiciary have to undertake persistent and continuous steps to bring in reforms to usher in a positive perception in the mind of the people to whom they serve.

On the occasion of Republic Day, the police fraternity and all other stake holders must take pledge to reform from within. As one Police Administrator has rightly suggested that the Police should reform itself within the ambit of existing environ and resources. It seems to be more pragmatic as the 'top- down' approach has failed miserably in ushering reform in many countries of the world. The 'reform within' approach would not cost anything, except some commitments, honesty and dedication, of which there is no dearth among the Indian Police.

At the macro level, the Indian Police has earned many brownie points. The communitarian approach, more visible in the metropolitan policing and some State Police like Tamil Nadu, Kerala and others, is bringing it nearer to the people and the community. The disconnect between the police and the people is crumbling, and the faith and trust

of the society in police is being restored. Now Police is being viewed as 'much more accountable and responsible to public for their action.' This fact attests the democratic credo of the Indian Police in spite of being based on the traditional/colonial ethos, laws and the mind-set.

Other challenges faced by the Police range from **terrorism**, **left wing extremism**, **gender sensitive policing** and **cyber-crimes**. The law enforcement apparatus in India has managed to have a modicum of control over challenge posed by terrorists. With the establishment of National Investigation Agency (NIA) coupled with creation of the critical infrastructure by Govt. of India, support from intelligence apparatus of the country and close coordination with the state police forces, there has been significant achievement on this front.

The left wing extremism (LWE) too seems to have been subdued and under control with their spread has been checked by the police. This has led to demoralisation of the cadre resulting in their surrender in significant numbers. The synchronized campaign and the initiatives by MHA, Central forces and State police, backed with the development and social development agenda, have led to the positive results.

On Gender policing, the Police have shown gender sensitivity, particularly after the Nirbhaya case. The initiative taken by MHA in sensitizing the Police on the gender issues have paid some dividends. But we have a long way to go on this front. The induction of increased number of women in Police, continuous training on this front and bringing about a change in male attitude to treat women as equal partners would add to the efforts being made in this regard.

As far as Cyber Policing is concerned, it is technical, complicated and characterised with fluid situation consequent upon the fast changing nature of technology. Hence, the security apparatus faces a situation where in everyday technology changes and the criminals and anti-social elements migrate to the new technology to execute their nefarious designs. This has posed a veritable challenge for the policing. Lot more needs to be done on this front in terms of augmenting our capabilities to meet this challenge by setting up state of the art cyber forensic facilities, training police officers as how to collect and preserve cyber evidence, maintain chain of custody to preserve its admissibility as evidence. We also need to impart training to the judiciary so that they can appreciate the cyber evidence which often resides in virtual world.

We hope that coming years will see Indian Police and all the stakeholders of the internal security turning more professional and committed, earning the respect and trust of the society and the people they serve.

Jai Hind !

(Gopal K.N. Chowdhary)
Editor

The Indian Criminal Justice System: Voices from Field

Vijay Raghavan*

Keywords

Criminal Justice System, Legal Processing, Under Trial Prisoners, Reform Committees, Subaltern Perspective.

Abstract

This paper is based on a study of male youth arrested in crimes relating to extortion and gang related offences in Mumbai city. An attempt is made to understand the legal processing of youth involved in organised crime, their experiences with the criminal justice system and their perceptions emerging from the same. Most studies and analysis of the criminal justice system in India have a 'systemic' bias i.e. they attempt to study the bottlenecks and the failings that plague the system from the implementing agencies' point of view, rather than from the end user's view point. This paper attempts to highlight criminal justice reforms from the viewpoint of those arrested for committing serious gang-related offences.

Background

THE Criminal Justice System (CJS) in India is characterized by innumerable arrests, overcrowded jails and courts with lacs of pending cases. According to the Prison Statistics 2012 (India 2012), there are around 3.85 lac prisoners in the country with around 66 per cent being under trials.

Prison populations have remained at the margins of welfare and development, and have seldom been viewed as in need of or deserving of social services. With the development of criminology as a subject of enquiry, a gradual shift has taken place, whereby the individual

Author Intro:

* Associate Professor, Centre for Criminology & Justice, School of Social Works, TISS, Mumbai.

alone is no more held responsible for his/her norm or law breaking behaviour. This shift has led to law and policy changes advocating a moving away from torture and debilitating forms of punishment, favouring imprisonment as and not for punishment, more humane custodial conditions, protection of legal and human rights, and finally a focus on retraining, rehabilitation and social re-entry. In India, the system of prison welfare was established in the context of reformation and rehabilitation of the convicted prisoner, as prisons were originally meant to house those who had been convicted by the law for the offences they were charged with.

A minor focus of prisons was the housing of under trial prisoners – those awaiting trial and kept in judicial custody, till the completion of their cases in courts. However, one fact that the authorities and civil society did not take note of for a long time was the rising numbers of under trials in prisons. Owing to the rising number of arrests, the number of prisoners has expanded since the last century. Prison Statistics 2010 shows that 65.1 per cent prisoners were under trials.

The delays in trials in courts have also taken menacing dimensions, thus skewing the convict-under trial ratio in prisons. One of the main reasons for the huge pendency of cases in courts is the poor judge-population ration in the country. **The present judge strength in India is 14 per million population (TwoCircles.net, 2008)**. The Law Commission in its 120th Report recommended that the strength of judges per million population be increased to 50 judges. Hansaria (2005) says that India has one of the poorest judge-population ratios when compared to countries such as Australia (47 per million), UK (50 per million), Canada (75 per million) and USA (107 per million). This is despite the fact that the pendency of cases in the country is about 26.3 million in the subordinate courts and over 3 million in the High Courts in India (rtiIndia.org, 2007).

One is faced with a situation whereby the rights and facilities for custodialised populations enshrined in the system somehow elude those who are most in need. The major reason for this is that the lack of structures and investments required for implementing the court judgments and reform committee reports. There have been little or no investments made to increase trained humanpower to reduce overload on the system, ensure legal rights and create rehabilitation structures.

As per the Prison Statistics India 2012 (India, 2012), the total number of prisoners provided various types educational facilities is in India during 2012 was 118580 (about 33 per cent of total prison population). As far as vocational training is concerned, the figure for prisoners provided such facilities during 2012 stood at 52228 (about 13 per cent of the total prison population). The total number of cases provided financial assistance on release during the year 2012 stands at an insignificant 1631 prisoners. Similarly, the number of convicts rehabilitated during 2012 is 3776. Shockingly, as many as fourteen states and six union territories have reported the number of cases given financial assistance as zero and thirteen states and five union territories have reported the number of cases rehabilitated during the same period as zero (India, 2012).

As far as reforms in the CJS are concerned, important recommendations have been made from time to time by the reform committees and commissions. The National Police Commission's Report (1977-1981) made far reaching recommendations to improve policing and crime investigation. Among them was to separate the law and order function from the crime investigation role within policing to bring greater professionalism and specialization in policing. Setting up of a State Security Commission and fixing the tenures of police chiefs at police station, district and State level were also recommendations which the political class refuses to acknowledge as the need of the hour (India, 1981).

With regard to prison reforms, the government has set up working groups, committees and commissions to investigate the issue and offer solutions. The more important among them were the All India Jail Reforms Committee headed by Justice A.N. Mulla (1982-83) and the National Expert Committee on Women Prisoners headed by Justice Krishna Iyer (1986-87). These reports have, by far, given the most comprehensive accounts of what ails our prisons, and suggested a slew of measures. The latest Draft National Policy on Prison Reforms and Correctional Administration, 2007 (India 2007), includes welcome changes to the Prisons Act of 1894. These include the introduction of a provision to provide for aftercare and rehabilitation services and the appointment of officers to provide legal aid for prisoners. Also envisaged are the establishment of a Research and Development Wing, financial assistance to non-governmental organisations working for the rehabilitation of prisoners and community-based alternatives to imprisonment for offenders convicted for relatively minor offences.

In seeking to improve the deliverables of the criminal justice system, one has to first address the low personnel-population ratio compared to countries that have more effective justice delivery systems. The tendency of most state governments has been not to fill up vacancies and augment the staff strength across criminal justice wings.

The first attempt towards the reform of the entire CJS was undertaken by the government with the constitution of the Committee on Reforms of the Criminal Justice System, headed by Justice V.S. Malimath. The Committee submitted its report to the Ministry of Home Affairs, Government of India in 2003 (India, 2003). However, the Committee failed to take into account international human rights standards in its recommendations. Secondly, it has failed to address a vast range of important concerns about the current functioning of the CJS. The report fails to substantively address issues including the problems of access to justice; endemic corruption, discrimination and bias within institutions of the Criminal Justice System; and non-implementation of safeguards against police abuses, among others (Amnesty International, 2003).

As compared to the Mallimath Committee, the report of Draft National Policy on Criminal Justice 2007 (India, 2007) headed by Prof. Madhava Menon, presents a broader canvas of the CJS within the Indian context. It strongly recommends a modern and holistic approach to the issue of criminal justice reform within the Indian context. It states:

> *Rule of law, democracy, development and human rights are dependent on the degree of success that the governments are able to achieve on the criminal justice front. Even national security is now-a-days increasingly getting linked to the maintenance of internal security. Given its so critical importance for social defense and national integrity, the need for a coherent, co-ordinated, long-term policy on criminal justice is obvious and urgent (India, 2007).*

There is an urgent need today to introduce structural reforms in the criminal justice system to address the myriad issues and problems that plague an archaic system, originally meant to serve the interests of the colonial powers, and out of tune with the developmental goals of post-colonial India. The political economy of the country today, spurred by globalization and a neo-liberal agenda, is giving rise to extremist violence, terrorism, large-scale financial frauds and money laundering, cyber crimes, corporate and environmental crimes, human trafficking,

ethnic cleansing and crimes against weaker sections on a scale not witnessed before. All of these crimes have a strong link with or fall within the broader definition of organised crime, in terms of their scale, methodology, structure and networks. Since youth constitute a significant majority of persons involved in these crimes and therefore being processed by the CJS, it is obvious that that they get negatively impacted by it. It may not be wholly out of place to posit that one of the factors responsible for the criminalization of youth in our country is the way our criminal justice operates, particularly vis a vis the vulnerable and marginalized sections of society.

Voices from the Field

During the study[1] on which this paper is based, qualitative data was collected from male youth in the age group of 18 to 30 years, arrested in one or more offences relating to extortion and/or other gang-related offences. Most of the respondents in the study were in prison as under trials and had been arrested more than once at the time of data collection. A total of nineteen life histories were developed based on several hours of in-depth interviews with each of the nineteen respondents. The analysis of issues as they experienced the system and its contradictions present some unique insights about how criminal justice processing has impinged and impacted on their lives.

The Police

It emerged from the analysis of the narratives that by and large, the youth arrested in organised crime related offences had negative experiences with the police and therefore harboured negative perceptions about them.

The broad themes around which these narratives were woven are: violence inflicted during interrogation in the police lock-up, not allowing family members to meet the accused person in the lock-up, harassment of the family to get them to surrender (if they were 'absconding' after the case came to light) or to reveal facts or evidence related to the case; harassment of youth with a criminal record in terms of preventive arrests, calling them for questioning now and then, making demands of money or pressurising them to become informers; manipulation of facts to strengthen or weaken a case (due to bribery

1 Raghavan, Vijay (2010). Youth Arrested in Extortion Crimes in Mumbai City: Processes of Arrest and After, Ph.D. Thesis, Tata Institute of Social Sciences, Mumbai

or use of influence brought upon the police); threat of killing by fake 'encounters'; charging them with false cases or applying harsher sections of the law; and discrimination on account of their religious background.

Of the sixteen respondents who spoke about use of violence by the police, only three denied any use of violence by the police while they were in police custody. However, even in these cases, the fear of using violence palpably came across in their narratives. As one of respondents recalled, 'the police did not use any violence, but the fear of violence was sufficient to "force" me to confess my involvement in the crime'. The descriptions about violence used against the respondents ranged from 'rough treatment' to 'passing electric current' through their bodies.

Apart from violence, some of the other tactics used by the police to get the youth to confess to their involvement in crimes or to collect evidence related to their cases, or to get them to surrender before the police included keeping the accused in illegal detention for some days before officially producing them in court, harassment of family members (including threatening to or detaining a family member) and not allowing family members to meet the accused in police custody. There were allegations of violence being used owing to religious bias (belonging to the minority community) or as an act of revenge (in the case of a Muslim youth eloping with a Hindu girl).

Manipulation of facts relating to cases were alleged by at least eight of the youth, in terms of hiking up the amount of cash recovered from the accused, changing the location of the site of arrest, and falsely charging an accused in a case to strengthen the case. Harassment of youth due to past criminal record emerged as a recurring theme and included use of excessive violence, booking them under preventive sections of the law, forcing them to cough up money or pressurising them to become 'informers'. Venkatesh's (2008) study too brings out police using pressure on ex-gang members to turn informants and the danger this poses on the youth concerned.

At least four of the respondents spoke of the threat of fake 'encounters' as a strategy used by the police to deal with criminals; one of them related that one of his co-accused was killed in one such encounter. A senior member of a well known gang and a key informant echoed the views of respondents about role of police in the criminalization of youth offenders.

The overall content of the experiences of the youth vis a vis the police and their perceptions about the police can be termed as ranging from negative to very negative. One interesting highlight that emerged from the analysis was that use of violence was not so much a matter of contention for the youth; it was almost a given. Negative perceptions about the police emanated from whether and how the youth perceived the police using violence as a tool, against whom and in what circumstances. They connected this with concepts of justice and fair play. As one of the youth said, he was very angry about the fact that he had been severely tortured by the police, forcing him to confess in a 'false' case. 'If I was thrashed in a case where I was involved, it would have been justified'.

The respondents also felt very strongly about the use of money power to manipulate cases and the use of strong arm tactics to strengthen a case or to increase the culpability of an accused in a case. Many narratives contained descriptions highlighting false cases registered by the police against them by using these tactics. For example, one of the respondents said that out of twelve cases of robbery registered against him, three were false cases. Manipulation, double standards and dishonesty seem to emerge as the main grouse of the youth rather than the unconstitutionality of methods.

The Judiciary

One of the themes emerging from analysis of the narratives was the unresponsive, uncommunicative and insensitive attitude of the judiciary and the possibility of their being influenced or manipulated by extraneous factors. Six of the respondents spoke about these issues during their interviews. On the other hand, some of the youth had mixed experiences with the judiciary i.e. not entirely negative. They had a few good things to say about their judges. Four of them gave a mixed or a balanced picture about the judges. Overall, a slightly better picture emerged as far as experiences of the youth with the judiciary are concerned, compared to that of the police. Lack of responsiveness and sensitivity, and delays in trials emerged as the main criticisms against the judiciary.

The Prison

The broad themes emerging from the narratives about prison conditions were: shortcomings in basic facilities including food, hygiene, sanitation and heath care; space crunch and overcrowding; use of violence by

prison staff; corruption and availability of contraband items and drugs; sexual exploitation by convict warders; extra facilities given to those from gangs or with money or influence; and running of illegal rackets (extortion or gambling) by gangsters from inside.

The issue of lack of family support or legal aid and contact with habitual elements or gang members emerges as an important factor leading to criminalisation and prisonisation (Clemmer, 1940; cited in Fry, 1976, p. 126; Gillespie, 2003, p. 3) of youth offenders, first-timers and those arrested in petty crimes. The need for a positive environment through the provision of recreational, educational, library, vocational training and counselling facilities and the role that social workers and voluntary organisations can play to rehabilitate prisoners has been another recurring theme in the narratives. Watching TV and small talk about their lives and their cases seem to be the only avenues of 'passing time' in prison.

One of the respondents, also a gang member highlighted the issue of criminalisation by saying that that prison is a breeding ground for criminals. According to him, family support is critical to negate the criminalizing influences in prison. He elaborated on extortion and gambling rackets being run from inside the prison by gang members in collusion with corrupt prison staff, and about drugs being freely available inside. He added that the activities of NGOs have a temporary impact on prisoners. According to him, if a positive environment is to be created in prison, the focus has to be on keeping the prisoners' mind busy for the entire day with different activities like sports, reading, writing, music, art, etc. Prison time should be used to upgrade education levels, it should be made compulsory for all prisoners including under trials. The attitude of prisoners has to be changed from one of 'making money' to 'earning money'. Prison staff should avoid use of violence and make efforts to increase contact with families of prisoners, especially with mothers and/or wives.

Most respondents were critical about the conditions, especially about the food, medical facilities and overcrowding. They spoke about discrimination on the basis of religion, or about the insensitive and uncaring attitude of prison staff. They also highlighted issues of rampant corruption, availability of contraband items and drugs inside and the exploitation (including sexual) of small timers by the convict warders.

Violence did not emerge as a recurring theme in prison (as compared to police custody). Four of them said that violence was used by the staff

as a strategy to maintain discipline and their authority over prisoners. Instances of purported arrogance, indiscipline, 'misbehaviour', 'over-smartness', violent fights between prisoners, or the discovery of illegal rackets being run by prisoners (without the knowledge of the staff) were met with harsh treatment, whereby 'innocents' (those not involved) too would not be spared. As one respondent said, 'such incidents are used to send out a strong message to prisoners that the administration would not tolerate any nonsense'.

Interestingly, nine of the respondents were silent or refused to comment about the issue of prison conditions. This could mean that they either did not face problems relating to food, medical care or space in prison (a possibility with at least four of them considering that they had 'gang' connections and therefore could manage better facilities inside) or they were apprehensive of speaking about the same. It could also mean that decent living standards were not an issue as far as they were concerned or that they had come to accept poor living conditions in prison.

The youth who were part of organised gangs when they were in prison presented a rather rosy picture of the time they spent in prison. They seemed to be having a good time – sumptuous food brought by their families or from a fixed eatery (a restaurant or a caterer),[2] playing volleyball or carom, watching TV, chatting, 'visiting' hospital for a few days under the pretext of 'medical check-up' or even going out for a drink on the way back from court to prison. Gangs were able to corrupt everyone from the top to the bottom and gave an impression that the staff were at their beck and call.

The effects of prisonisation and presence of criminalizing influences emerged very clearly from the narratives of at least eight of the respondents. First-timers, those arrested in cases involving use of violence and petty offenders were sucked into the criminal nexus, especially in the absence of family support. Gang members often arranged for their legal aid; gave them money or coupons to buy cigarettes/*bidis* or eatables from the canteen; shared food with them; protected them from excesses committed by other prisoners or prison staff/convict warders and even gave emotional support in times of crisis. These youth felt obliged to these gang members and seemed agreeable to work for them once they were out of prison. As one of

2 The prison rules allowed under trial prisoners to eat home-cooked food. Some years back, this facility was stopped. It is now only allowed under court orders.

the respondents boasted, '…it is very easy to form a gang from inside by helping those without supports. Once they are released on bail (with the help of the gang), we can use them to carry out extortions; instructions can be given to them during prison *mulakats* and court visits'.

The entry of voluntary organisations and intervention of social workers assumes significance in this context. Some of the respondents said that the visits by NGOs helped them to stay positive and hopeful. They attended the sessions organised by religious groups and participated in vocational training course organised by NGOs.

Almost all the youth emphasised the need to improve living conditions in prison and create facilities which would foster rehabilitation. They made specific suggestions in terms of creating a positive environment through improvement in basic facilities, provision of legal aid and organising activities – educational, vocational training, library facilities, counseling sessions, moral and spiritual lectures and support in finding employment and shelter after release. Reading newspapers or magazines, watching TV and chatting with each other seemed to be only avenues for 'time-pass' in prison.

Most of the youth were in touch with their families while in prison. It emerged from the interviews that family support and the bond they shared with at least one member of the family had a crucial bearing on their rehabilitation chances; it created a positive impact on their minds. This could be gauged from their actions - advising their families not to bother to come to meet them time and again (every visit to prison or to court has financial and emotional implications); severing connections with the gang; feeling guilty about their actions and resolving to remain straight henceforth.

In cases where there was little or no family contact, the youth seemed to be very uncertain about their future. They were not sure if they would go back home after their release. This lack of contact seemed to be the outcome of a combination of factors – poverty and a consequent inability to come for *mulakat*, breakdown of relationships, self-pride and absence of a family. The absence of a catalyst to motivate the family to take interest also played a role in furthering this distance. This was proved in the case of one of the respondents, where the family came forward to get him out on bail, after an organisation which works in the prison intervened.

Legal Aid or Counsel

Most of the youth interviewed had private lawyers. However, very few of them reposed faith on them. They had complaints against lawyers in terms of the high fees charged by them, not communicating with them, not being regular in attending court, etc. An effective legal aid system emerged as crucial towards making access to justice a reality. The absence of effective legal aid can lead the unsupported prisoner to take the help of habitual offenders and gang members, thus drawing them into the criminal nexus.

Summing Up

The subaltern view emerging from the study presents a rather negative picture of the criminal justice system, leading to negative perceptions about the system. On a comparative scale, the police came across as the most negative followed by the prison. The image of the judiciary too was negative but more of a mixed picture. As one of the respondents very aptly put it,

> *"The criminal justice system is biased towards the powerful and influential. The fact that I was a gang member (and a senior member at that) actually helped me to get away without a conviction. I could get the police to frame weak cases against me and got support from politicians, who influenced the police to weaken my cases."*

The need to bring reforms in the system emerged clearly through this study. Some of the areas for improvement which have emerged from the narratives include desisting the excessive use of violence as a method to 'solve' cases by the police, the need to strengthen legal aid and family contact to counter the criminalizing influences in police and judicial custody; expediting the trial process, introducing alternatives to the financial system of bail, improving living conditions in custody; provision of educational, vocational, recreational, spiritual and counselling facilities in prison, introducing social services and the role of social workers, and setting up of after care facilities in terms of employment and temporary shelter.

References

Books and Journal Articles

Fry, L.J. (1976). The impact of formal inmate structure on opposition to staff and treatment goals.In *The British Journal of Criminology*, Vol. 16, No. 2, April 1976, pp. 126-141.

Gillespie, W. (2003).Prisonisation: Individual and institutional factors affecting inmate conduct. New York: LFB Scholarly Publishing LLC. Venkatesh, S. (2008).*Gang leader for a day*.London: Allen Lane.

Schlosser, J.A. (December, 2008). Issues in interviewing inmates: Navigating the methodological landmines of prison research. *Qualitative Inquiry,* Vol. 14, No. 8, 1500-1525.

Internet Sources

Amnesty International. (2003). Report of the Mallimath Committee on reforms of the criminal justice system; Some observations. Retrieved from on March 09, 2012, from http://www.amnesty.org/en/library/asset/ASA20/025/2003/en/2c963c9b-d694-11dd-ab95-a13b602c0642/asa200252003en.html

Hansaria, V. (2005). Welcome address on law day. Supreme Court Cases, (2005) 2 SCC Jour 19. Retrieved on June 12, 2009, from http://www.ebc-india.com/lawyer/articles/2005_2_19.htm

India. (1981). National Police Commission reports. Retrieved on October 10, 2009, from http://www.bprd.gov.in/index1.asp?linkid=281

India. (2003). Committee on reforms of criminal justice system. Retrieved on October 10, 2009, from http://www.mha.nic.in/pdfs/criminal_justice_system.pdf

India. (2012). Prison statistics 2012. Retrieved on June 12, 2014, from http://ncrb.nic.in/PSI2006/prison2006.htm

India. (2007). Draft national policy on prison reform and correctional administration. Retrieved on October 10, 2009, from http://www.bprd.gov.in/writereaddata/mainlinkfile/File1572.pdf

India. (2007). Report of the committee on draft national policy on criminal justice. Retrieved on October 10, 2009, from http://www.mha.nic.in/pdfs/DraftPolicyPaperAug.pdf

rtiIndia.org. (December 29, 2007).Nearly 30 million cases pending in courts. Retrieved on June 13, 2009, from http://www.rtiindia.org/forum/2385-nearly-30-million-cases-pending-courts.html

Two Circles.net. (May 6, 2008). Judge population ratio. Retrieved on June 12, 2008, from http://twocircles.net/data_bank/judge_population_ratio.html

Role and Need of Modern Public Relation Practices in Policing: Mapping a Pathway

Dr. Deepak Sharma* & Anshul Bhatia**

Keywords

Policing, Public Police Interface, Governance, Public Relation Practices.

Abstract

In a democratic society like India where various stakeholders viz. good governance, civil society, non-government institutions, accountability, need for internal security through effective policing, role of media, etc have come into the significant stream (Sharma & Marwah[1]). The need of effective public police interface is considered principal solution in establishing mutual coherence in making of a smooth society. The study finds that practice of public police interface is considered panacea but there are gaps that exist between the successful public and police connects. On basis of analyzing literature available on public police interface, we have deduced that police have failed to connect successfully with the different strata of society. The present study analyzes and evaluates the various dimensions of public police interface, its significance, challenges and brings forth the prospects of public relation tools and practices in ushering effective public police interface.

Introduction

IN a developing nation like India, government plays an important role in managing public affairs and to keep the growth of country on track. Modern day government is not only the provider of services but also the agent of social change. Government is not a standalone term these days but its nomenclature is replaced by a modern term

Author Intro:

* Senior Research Fellow (UGC) and Resource Person of Public Administration at PGGCG-42, Chandigarh.

** Research Scholar, Department of Public Administration, Punjab University.

'Governance'. Governance is a different term from government i.e. former is a qualitative concept whereas latter one is a physical entity[2]. Generally governance refers to the decision making and implementation processes in the administration of a country, state or organization. Governance refers to the 'governability' of a polity or, in other words, the capacity of a political system to govern efficiently and to provide necessary political conditions for socio economic development[3]. So, governance is government in action or government carrying out its functions to manage public affairs. Governance being a neutral term focuses only on functioning of government.

With the advent of liberalization, globalization and privatization reforms in India in 1991 many international agencies recognize absence of effective governance as a serious barrier to overall development. This was the time when a new modified term of governance emerged i.e. 'Good Governance'. Good governance is a term that connotes value assumptions. Authors define good governance as unambiguously identifying the basic values of society and pursuing these[4]. It is accompanied by certain values which installs positive virtues of administration and elimination of vices of dysfunctionalties. Good governance is attached with effective and efficient public administration in a democratic set up. Pai Panandiker sees good governance as it pertains to a nation which handles its people to lead peaceful, orderly, reasonable, prosperous, participatory lives[5]. It refers to the adoption of new values of government to establish greater efficiency, legitimacy and credibility of the system.

Good governance is a wider term which covers into its ambit various elements like rule of law, accountability, decentralization, honesty and independence of judiciary, human rights, people's participation, equality and absence of discrimination. So, good governance is an uphill task in which various stakeholders play their respective roles.

Government being the dominant actor plays an important role in formulating and implementing public policies which aim at achieving objectives of good governance. Government has multiple functions and multifarious agencies which perform their respective functions. As Weber remarks that state is a multifaceted entity[6].

In modern day governance, law and order is an important function for any government, but at the same time it poses a big challenge also. Law and order function is associated with police organization

of government. Effective law and order demands the application of rule of law. Rule of law is one of the fundamental characteristics of good governance. It entails certain principles which lay the foundation for working of every police organization; some of these principles are absence of arbitrary power, equality before law and primacy of rights of individuals. So, police being protector of citizen's life should maintain the principles of rule of law. Undoubtly effective police reforms can certainly help to strengthen confidence in the rule of law[7].

Rationale of Public-Police Interface

In a democratic polity maintenance of law and order is heart of governance. Increasing crime rates in any society reflects its negative image. Accordingly, it becomes the duty of police to curb evil practices in society and set an example of effective law and order. But in a country like India, police has a poor image in public. It is viewed as an oppressive tool in the hands of political masters. Whatever policies are formulated by government regarding law and order are implemented by police as line agencies. The police are the edge, the most visible and, according to many citizens, the most approachable of these criminal justices practioners[8]. The activities performed by police directly affects the behaviour of public. The general trend of opinion is that the public hates police and that police act harshly and oppressively towards the public. This portrays negative image of police in minds of the citizens. In this backdrop, it is imperative to have an effective and strong public police interface which will help to improve the relation between the two. In a democracy aiming at welfare state, it is essential that members of this vital service of police should cultivate harmonious relations with the public and should help the people in distress and trouble[9].

Another dimension of public police interface is community policing. Community policing draws its genesis from 'communitarianism' approach given by Amitai Etzioni[10]. In this approach aim is to make community participate in local level governance. They join hands with government agencies to solve local level problems and to achieve objectives of grass root governance. On the same lines community policing aims at improving the relationship between the service provider i.e. police and its beneficiaries i.e. public. A good example would be that of a Neighbourhood Watch Scheme designed to involve the community and police in policing their surroundings[11].

Literature Review

Several academicians and practitioners have advocated and facilitated the public police interface and community policing. Police is recognised as coercive arm of government to control crime, but there are frequent debates like extending human relations training of officers, developing programme to educate the public about the functioning of police and creating community relation units within departments, all these practices aim at changing role of police in society[12]. At the same time the police officer should be philosopher, guide and friend or that the police officer should be a helper. Line officers should be concerned with the preservation of peace, protection of life and property, enforcement of laws and detection of law breakers[13].

Theoretically it is easy to talk about friendly public police interface or involvement of public in policing, but some examinations are being carried out regarding nature of public police support in normal and some extra ordinary situations like in strikes, riots and such other instances of social disorder, natural calamities and communal tensions. It was deduced that in these situations complete dependence is on police machinery[14]. No doubt primary role of police is prevention of crime and maintenance of law and order, but this role should be played with deference to the satisfaction of the people as police is not supposed to rule but to serve[15]. Even in the ancient times police administration in the villages was collective responsibility of every resident in order to help police in uniform patrolling, crime investigation and prevention of crime. Such administration was based on principle of local responsibility and mutual cooperation[16]. Such mutual cooperation and collective responsibility is missing in present scenario due to lack of effective public police relations practices. Image of police is tarnished in the minds of public. There is a need to lay stress on police public relations which aims at developing favourable attitude of public towards police[17]. Such absence of public relation with police can be drawn from colonial past where police aimed at serving less. Since independence situation has not improved due to lack of public participation. Therefore public police interface has failed to ripe expected results[18]. Effective and strong public police interface can be devised by evaluating citizen's attitude towards policing. In this backdrop, a study was conducted in which special attention was given to role of media and direct contact with service providers[19]. With the passage of time expectations of public are changing regarding police.

In order to meet these complex expectations, community Policing practices would be an effective tool. It can help to change the attitude of citizens regarding police[20]. It is vivid that community policing is an imperative tool, but it cannot be implemented until and unless it is defined conceptually. A study was carried out, in which complex interactions in community policing, role conflicts, impact of media and evolution of police community relation was mapped[21]. Lastly community policing requires a benchmark leadership. Leaders and youngsters always play a positive role in shaping minds of society. So strategies should be devised to figure out young local youngsters and to keep them away from drug abuse and negative evils. Such strategies can be helpful in mobilizing local talent and to get information regarding local criminal activities[22].

Need of Effective Public Police Interface

The public police interface is an organizational philosophy which stands on effective communication and interaction with various strata of society. Police organization is a not a standalone entity, it is the form of integral part of society. Society can be termed as system in which various interdependent parts play their respective roles and give shape to a major role played by a system. In this backdrop we can deduce that society is a system in which public and police are interdependent parts which performs their respective roles. In modern day governance connectivity of police with public is pivotal. The following points depict the importance of public police interface in making a balanced society:

- **Meeting the Needs of Society:** The primary function of police is maintenance of law and order. But with the change of time, functions of police have also become complex and diverse. In order to cater to the needs of citizens, it becomes important to figure out and meet the expectations. Such needs must be understood by the police then it can direct its efforts towards the expected performance and efficient policing.

- **Positive Image Building:** Generally police has a poor public image. It is viewed as an oppressive force in society. Malfunctioning and corruption in policing have portrayed negative image of police amongst citizens. In order to overcome this daunting situation, it is imperative that police should devise some plans through which its image can be improved. Rigorous promotions, campaigns

and highlighting positive works can contribute to the positive outcomes.

- **Effective Feedback Mechanisms:** Feedback is a crucial tool through which connectivity can be built between two ends. It will also lessen the gap between public and police which will lead to better understanding and winning trust amongst the public. In order to have strong public police interface it is important that police should ask people for feedback of their performance. For ensuring this, periodic surveys and interviews must be conducted as collected information will help police to analyze its performance and also to set the further higher standards for delivering services to the citizens.
- **Participation in Police Governance:** In a democratic setup, it is important for police organization to educate people regarding the participative governance. Police public participation in crime prevention is a new dimension in police governance. Such collaboration will help both the parties in understanding each other and also to cooperate in crisis situation. As people will participate in policing, they will get a chance to learn safety techniques and also how to react in crisis situations.

Challenges of Effective Public Police Interface

Public police interface aims at philosophy, managerial style and organizational plan that promote better public police partnership and more proactive problem solving approach towards the community. It helps in providing solution to wide range of problems and issues involving crime control, crime prevention and the fear of crime. Public police interface is based on collaboration between police and citizens in an amiable and cooperative spirit.

It is not that easy to achieve effective collaboration of public police interface in practice. There are various hurdles which pose danger in the way. The image of police is harsh amongst the society. People find police oppressive and often hesitate to have any form of communication with them. The behaviour of police is rude and practices like maltreatment and corruption are often highlighted in media. Another grave concern is lack of soft skills and human relations approach in policing which arouse fear in society defeating the very purpose of public police interface. Besides this, police hesitate or ignore to keep in touch with public. These omissions and commissions

betray the poor training practices. Police is not trained in respect of public relation approach which is a dominant feature of modern day police governance. Above all there is absence of the marketisation of police service. Here marketing emphasizes a management process which indentifies and satisfy citizens requirement efficiently.

In order to overcome all these issues, the following section projects the implementation of modern day public relation tools and practices to usher effective public police interface. With the advent of these tools and managerial practices police personnel are supposed to be public managers who along with curbing crime also promote themselves as efficient public servants, tackling the crisis situations without breaching the ethical conduct and public good.

Role of Public Relations in effective Public Police Interface

Improving police department's image in the community takes more than just a concern or wishful thinking. The police department must establish an effective partnership with the community as a whole, the foundation of which is mutual trust and understanding. Police organizations must realize that they have the ability to alter their own image within the community.

Here the role of modern day public relation practices becomes important in making police reach at the doorsteps of people. Generally, public relation practices are considered as collection of communication techniques used by individuals or organizations to convey the public or media about the merits of an organization, programme or a policy. The matter of maintaining good relations with the public involves much more than trying to please an indistinguishable mass of people[23]. It involves trying to satisfy all those elements of divergent likes and dislikes in the society[24]. It is in this backdrop that the role of public relations in modern day public police interface is eminent. Effective public relation practices are the collection of creative techniques used for image building, enhancing internal and as well external coordination, handling and yielding media benefits for dissemination of knowledge[25]. All these techniques play a significant role as these tools can change the image of police which in turn reflects the degree of public confidence and respect for policing. So, here role of modern day public relation practices becomes important to shun the negative image of police from minds of people through effective public relation practices. Police can build stronger connectivity with public by

ushering in the community policing and improving the public police interface. The following public relation practices depict importance in different dimensions which are as follows:

- Through public relations practices like feed-back, surveys, harnessing coordinated campaigns, focussed group discussions police can highlight its vision and mission amongst citizen's thereby building trust. Such practices will bridge the gap and bring community more closer to the police.
- Holding meetings with resident welfare associations and briefing them about emerging trends of crimes will provide a platform to public to participate in public governance. Such meeting will yield suggestions for police to strengthen the policing gaps.
- Distributing printed material like brochures, verification forms and helpline numbers will raise the inquisitiveness of citizens to participate in community policing projects. There is need to have a complete Public relation unit in police department which must research the trends of crime and thereby designing the nature of activities. All the activities of community policing must be well advertised in various modes e.g. public service advertisements, flex advertisements, moving advertisements on public transport .These tools of persuasive communication will enhance the mutual understanding.
- With the advent of public relation and management practices, marketing the police would appear a practical exercise to undertake, and putting the citizen at the centre of police planning and activities may provide answers to many problems the police facing today. Marketing can be conducted through two processes[26]:

a) **Internal marketing:** In order to build strong public police relations, there is need to inculcate citizen centric policing among policemen. It can be done through internal marketing which aims at communicating with policemen at all the levels of police hierarchy and involving them in new initiatives and strategies. It helps to create spirit de corps and sense of team work among policemen. The following table describe the desired organizational and structural transformation which is needed for implementing the citizen centric policing.

Organizational and structural transformation aims to achieve desired goals. Changes in structure involve organizational and policy matter designing in recruitment, training, rewards, promotion and the establishment of specialized police units. As far structure is concerned, effective participative policing involves the shift as described in table below:

Traditional Policing	Citizen Centric Policing
a centralized structure	a decentralised structure (the aim is to bring the police closer to the community)
excessive specialization	a balance between versatility and specialization
standardization and uniformity	flexibility and diversity
an autocratic "command and control" style of management	a participative and consultative style of management
operational management of status quo	strategic leadership of change
a focus on short term strategies	a focus on the long term impact of strategies
a narrow definition of the duties of a patrol officer - their role is limited to attending to complaints and they must always act according to the "book"	an extension of the duties of the patrol officer - the patrol officer becomes a generalist responsible for attending complaints, solving problems, activating the community, preventing crime, and undertaking preliminary crime investigations. The discretionary powers of the patrol officer are recognized and developed.
narrow training emphasis on fitness, self-defense and knowledge of the law	a broader training focus which, in addition to fitness, self-defense and knowledge of the law, include knowledge of crime prevention, conflict resolution, problem-solving, and community participation
Head Office as a source of orders, rules and regulations	Head Office as a source of support, direction, norms and values
the measurement of performance based on "quantitative" criteria such as the number of arrests	the measurement of performance based on "qualitative" criteria such as the achievement of community goals or the solution of problems
heavy dependence on rules and regulations	a value driven approach based on the policing vision

***Source: Manual on Community Policing Policy, Framework and Guidelines (South Africa), Retrieved from* www.thecpf.co.za/request.php**

Such transformation is not possible overnight, role of effective public relation practices play a worthy role in shaping the organizational culture which can be carried out by continuous effective leadership and sensitization of police personnel at every level.

It can be depicted from the table that the traditional role of police no longer exists. These days more emphasis is on citizen centric policing in which citizen is considered sovereign. Modern policing requires decentralized structure which can shatter the barriers of old centralized policing with more scope of police participation. Moreover, role and duties of police has also undergone a change, increasing ambit of police functioning with more versatility and specialisation. More emphasis is given on educating police personnel about importance of fitness, crime prevention, knowledge of law and community participation. Performance of police has always been under scanner of citizens, so modern policing aims at quality rather quantity in achieving the goals of community. Police ultimately deals with public who have certain values which sometimes cannot be in consonance with rigid rules and regulations devised to control citizens. Here focus should be on a value driven approach in which citizen should be at centre. This transformation calls for strong public relation practices which can help in knitting strong public police interface. Some of these techniques can be advertising of the police work. The advertising is generally a mass communication technique through which a target group is sent a message. In policing, advertising can play an effective role in connecting with public. Through advertising police can create awareness regarding effective police functioning, new strategies for maintenance of law and order and in receiving feedback from citizens which will help police to understand the public perception. Secondly, a public relations department can be established in all police departments which will be involved in conducting rigorous public relation practices and thereby connecting police with community. For this, police personnel should be given a formal training in which they can be taught soft skills as how to connect with people. Such practices will help to provide a pragmatic shape to this sound idea of community policing.

b) **Interactive marketing:** Interactive marketing aims at forming a communication channel through which police can interact with public. A police officer should see public as a client with aim to provide service. Such interactive marketing will help police to create awareness among public regarding new police activities and

plans devised for public care. In return, public can also provide feedback regarding service delivery performance of police. It aims at highlighting good work of police, and change public perception about the police. But here attitude and behaviour of each police officer is crucial. So, police personnel should be given training regarding interaction skills and attitude.

Apart from aforementioned techniques, role of media is also imperative in strengthening the public police relations. Media is an important democratic resource and plays a pivotal role in developing the understanding between police and public. They have, therefore, a strong potential to serve as a positive force towards improving the system of public police relations. Media helps to generate awareness and disseminate information among public regarding police activities. It also plays a crucial role in the development of citizens to be active in police governance[27]. Generally media highlights malpractices in police governance. So role of media should be to portray positive image of police in society and appreciate the activities conducted by police for public safety. The role of effective spokesperson is of utmost importance for repairing the tarnished image through rebuttal, rejoinders and media conferences.

Conclusion

Presently, police administration has undergone a change in comparison with traditional one. Now police is much more accountable and responsible to public for their actions. Police functions have increased in consonance with public awareness, so having good relations with public is the need of hour. On basis of above discussion we can deduce that upgrading modern public relation practices have become a prospective area of concern for police to knit strong public police interface and connect the values of police and public.

Endnotes

1. Deepak Sharma & Jyoti Marwah (2013), An Appraisal of Community Policing Practices: A Case Study of Chandigarh, India, Journal of Administration and Governance, Vol. 8, No.1, pp. 39-51.

2. B.L. Fadia & Kuldeep Fadia (2013), Public Administration, Agra: Sahitya Bhavan, p. 949.

3. R.K. Sapru (2011), Administrative Theories and management Thought, Delhi: PHI, p. 507.

4. Subhash C. Kashyap (1997), Crime Corruption and Good Governance, New Delhi: Uppal Publishers, p. 113.

5. Bhabani Sen Gupta (1996), India: The Problems of Governance, Delhi: Konark, p. 12.

6. Francis Abraham & John Henry Morgan (2011), Sociological Thought, Chennai: Macmillian Publishers India Limited. 185.

7. Ramesh K. Arora & Rajni Goyal (2013), Indian Public Administration, New Delhi: International Limited Publishers, p. 844.

8. Thomas, Pamela & Ronald, Police – Community Relations and the Administration of Justice, New Jersey: Prentice Hall, 2008, p. 350

9. T.N. Chaturvedi, 'Police - Public Relations (1998)' Indian Journal of Public Administration, Vol. 24, pp. 274-280.

10. Amitai Etzioni (1993), The Spirit of Community, New York: Crown Publishers, p. 78.

11. R.K. Sapru(2011), Public Policy, New Delhi: PHI Learning Private Limited, p. 270.

12. Paul M. Whisen, James L. Cline & Harrge T. Felkenes (1973), Police-Community Relations, California: Good Year, Publishing, pp. 1-10

13. Richard E. Former & Victor A. Kowaleroski (1976), Law Enforcement and Community Relations, Virquonia: Restore Publishing Company, pp. 1-5.

14. P.J. Alexander (1980), 'The Electoral Process and Police Behaviour: A Case Study of Bye Election in a State' Indian Journal of Public Administration, Vol. 16(2), pp. 278-297.

15. S.C. Mishra (1981), 'Police Performance: Some Parameters of Appraisal' Indian Journal of Public Administration, Vol. 28(2), p. 45.

16. K.K. Mishra (1987), Police Administration in Ancient India, Delhi: Mittal Publications, pp. 1-5.

17. R.D. Sharma (1990), District Administration in India, New Delhi: H.K. Publishers, pp. 1-30.

18. P.S. Bawa (2000), 'Police Public Interface' The Indian Police Journal, pp. 11-15.

19. A.K. Donahue & J.M. Miller (2005), 'Citizens Preferences and Paying for Police' Journal of Urban Affairs, Vol. 27(4), pp. 419- 435.

20. Anand Kumar Tiwari (2007), 'Changing Public Expectation and Community Policing' The Indian police Journal, Vol. 54(3), pp. 73-80

21. Thomas, Pamela & Ronald, Police (2008)– Community Relations and the Administration of Justice, New Jersey: Prentice Hall, p. 351

22. Hiranmay Karlekar (2008), Inefficient Police & Flawed System, New Delhi: The Pioneer, 2008, p.23.

23. Raymond E. Clift, (1949) 'Police, Press and Public Relations' Journal of Criminal Law and Criminology, p. 669.

24. Ibid. p. 669.

25. Diwakar Sharma (2004), Public Relations, New Delhi: Deep & Deep Publications, p. 3.

26. Bushra Bano & Parvez Talib (2014), 'Public Perception About Indian Police: An Empirical Analysis' The Indian Police Journal, Vol. LXI, pp. 132-148.

27. Rohit Choudhary, 'Marketing the Police', The Tribune, 2012.

The Issues in Cyber-Defence and Cyber-Forensics of the SCADA Systems

Sandeep Mittal*, IPS

Keywords

Cyber Defence, Cyber Forensics, SCADA Systems, Malware, Cyber Missile.

Abstract

As the Supervisory Control and Data Acquisition (SCADA) system are deployed in infrastructures which are critical to the survival of a nation, they have emerged as a potential terrain for cyber-war, thus attracting the considered attention of 'nation-states'. The analysis of worms like 'stuxnet' 'flame' and 'duqu' reveals the hand of a 'nation-state' in their design and deployment. Hence, the necessity to understand various issues in the defence of SCADA systems arises. The forensics of the SCADA system provide deep insight into the design and deployment of the worm (the malware) once the system is attacked. This is precisely the scope of this essay.

Introduction

THE peace, prosperity and economic development of any Nation depends upon its critical infrastructure and how well-protected it is. These critical infrastructures are distributed physically and virtually in space and time. The Supervisory Control and Data Acquisition (SCADA) systems are an important component of the process to control and monitor industrial and infrastructure process. Initially, these SCADA systems were designed to run in an isolated environment. However, with sudden improvements in information and communication technology, SCADA systems have evolved and

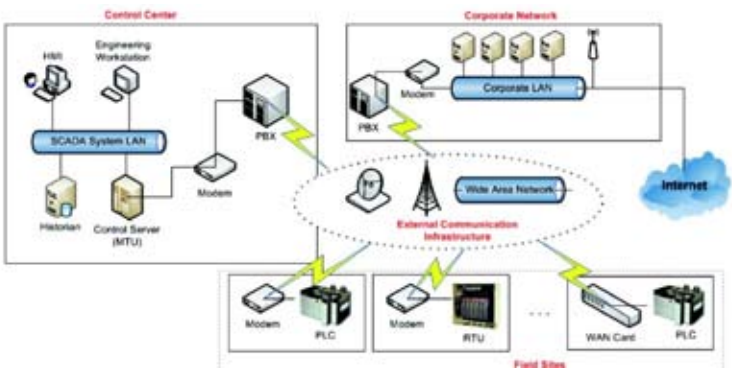
Author Intro:

* Deputy Inspector General of Police, LNJN National Institute of Criminology and Forensic Science (Ministry of Home Affairs: Government of India), Delhi-110 085, INDIA, E-mail ID: mittals.ips@gmail.com

adopted latest technologies like wireline IP communication, and communicate over public IP network on one hand making the SCADA system vulnerable to attacks (Bailey & Wright, 2003) and malware infections from the much wider networks. The discovery of ' stuxnet', 'flame' and 'duqu' in the recent past has opened a 'can of worms' which was unimaginable till recently. While 'stuxnet' could be termed as 'an essentially a precision military-grade, cyber-missile' which, once deployed, would not require any human intervention thus heralding the beginning of digital attacks on physical targets by hunting them globally (Chen and Abu-Nimes 2011), the other two are more improved malware to gather intelligence about critical infrastructure worldwide. The developers and the critical infrastructure stakeholders are realizing these increasing threats and have started taking measures to address these (Brandle & Naedele, 2008; Ahmed et.al, 2012).

The Components of SCADA System

A typical architecture of a SCADA system controlling a typical critical infrastructure would mostly comprise of a 'control-centre' and 'field-sites'. The 'field-sites' are equipped with devices like 'Programmable Logic Controllers' (PLCs) Remote Terminal Units (RTUs) which send information by different communication media (e.g. satellite, wide area networks or radio/cellular/microwave networks) about the state of Filed-equipment to Control-centre. The major components of a control centre are Human Machine interface (HMI), data base management system (Historian) and Server or Master Terminal Unit (MTU) Components. All the communications with the field sites are initiated by MTU and it receives back the data from field-devices, pre-processing this data, if necessary, and sending to historian for archiving. The HMI provides the interface to the human operator. The typical architecture is shown in the following figure (Ahmed et.al, 2012).



The Defence Issues in the SCADA System

The discovery of complex, complicated and deceptive worms e.g. 'stuxnet', 'flame' 'duqu' and 'careto or mask' in recent past points to the fact that the SCADA System are rapidly becoming the targets of 'nation-states' who are ever-eager to deploy such cyber weapons to strike at will in the enemy territory. Therefore, the defence approach for securing SCADA systems has to be comprehensive and multi-pronged. These strategies can be broadly divided in to 3 broad categories (after Nazario, 2004)

a) ***Host based defence measures provide a deeper entrenchment of the defence for any single system. Therefore, multiple defences at host level make things difficult for the malware attack to exploit the system. However, these defences may fail due to misconfiguration and may be bypassed. This strategy has the following components:***

- Host based static or the dynamic firewalls are used as a complement to the network firewalls. However, the limitations to this strategy are that the host based firewalls are ineffective in stopping the worms following the already established link paths that are allowed via policy. Moreover, the worm itself may subvert these firewalls if sufficient right are obtained by the malicious executable. A worm on launch may issue a command to unload the firewall's rule set, completely neutralising the installed security monitor.
- Server side commercial antivirus software can be implemented. However, it requires regular and timely updates to the definitions as they rely on signature based definition, failing which defence becomes ineffective.
- Partitioned privileges - The service running on well-known ports (between 1 and 1024) have elevated rights and handle authentication and thus having super-user level access to system databases. However these access rights are not required through the life time of a program. Any system that does not need repealed can discard the elevated privileges, it began with, once the restricted operations are performed.
- Privileges Separation – In this method, two instances of the application run, one with few privileges (only sufficient to

handle user request) and second with system level privileges (required to handle services such as authentication) and the two process communicate via inter-process communication, with the child requesting the results of any operations that require any privileged access. Thus a small process run with system level access that has minimal exposure to external risks. Compromise, if any, occurs in the unprivileged process space (Provos, 2002).

- The other strategies include disabling the unneeded service and features, aggressively patching known holes, implementing the behaviour limits on hosts. The last of these is a promising area for computer security and can be applied to different level of networks. The behaviour of the host in normal circumstances is enforced in this method. However, this method may prove useful at the network level rather them at the host level.

However, this approach may not scale well to large SCADA networks, in addition to difficulties in maintaining and enforcements. But they would continue to be used in SCADA defence as malware spreads by attacking the host only.

b) Firewalls and Network Defences

Firewalls are used to enforce a network security policy which includes authorisation to establish communication between two end points, controlled by the port, applications and protocols in place. The firewalls evaluate the connection requests against its rule base and apply a decision to requested action (Ranum & Avolio, 1994; Wack, Cutler & Pole, 2001; Nazario, 2004). Network architects and administrators managing SCADA systems should deploy firewall technology to achieve several key objectives (Wack and Cranahan, 1994);

- Protection from malicious applications by controlling their entry and exit from a network.
- Control the destinations and sources of network communications.
- Concentrated security and enhanced privacy
- availability of logging statistics for internet activities.

Most of the firewalling devices are of two basic types. The first is a packet filter which performs policy enforcement at packet level and could be stateful or stateless. A stateful filter understands the context of a communication and can conditionally pass or reject packets that are part of the communication (or at least appear to be so), while, in contrast, the stateless firewall, only monitors single packet irrespective of the context of surrounding traffic. Here, filtering rules are applied on a packet level basis as opposed to a connection level basis (Chapman, 1992). Placing a firewall at the network perimeter, usually the place where two different policies exist at the end of a network. At the 'outside', policies are generally more liberal than on the 'inside' of the network, thus giving rise to the 'trusted internal network and 'untrusted external network'. This creates a protected network and exposed network. These exposed networks have services such as web servers and access given to the world at large. Each network is then protected with different policies to meet the differing security requirements. However, the perimeter firewalls presume that one security policy can adequately meet the requirements of entire network which is simply impossible and therefore inadequate.

Therefore, a set of firewalls on each submit of the network are deployed and tailored to meet the usage patterns of the different use of groups, and are an effective natural way to defend against an active worms who spread and mutate rapidly. Another strategy is to deploy reactive Intrusion Detection System (IDS). Typically, an IDS sensor passively listens to the traffic on the network and only sends an alert when it has observed suspicious traffic, but still allowing the communication to proceed. In contrast, reactive IDS can be configured to close the connection via forged packets. A second type of network firewall is the proxy server which provides their services by being an intermediate system for a network connection. Typically a listening agent on the proxy server receives a request for a network action, and fulfils the action on behalf of the client. At no point of time the client and the final destination make a direct contact. However, as the proxy act as an active peer in the communication, it may held the data temporarily before transfer to the client system. This allows compromise of the content including the details of malicious activity being removed (Ptacek & Newsham, 1998). However, as using the proxies induces communication stream latency resulting in time lag in communication of critical instructions, its use in SCADA systems is limited.

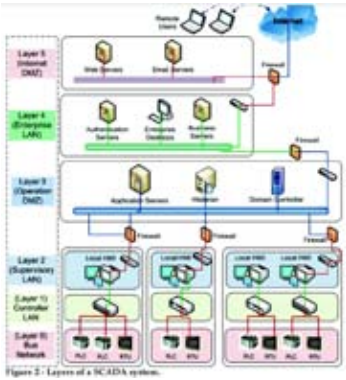
The most important thing to be kept in mind is that SCADA systems control the critical infrastructure which requires data transmission and decision implementation in real time failing which the critical networks may collapse. Therefore, any defense strategy to be used for SCADA system should have a judicious blend of security and usability in real time.

The Forensic issues in the SCADA Systems

The reliability of a SCADA system depends not only on safety, but also on security (Brandle & Naedele, 2008). A comprehensive guide on Industrial Control Systems (ICT) Security has been published by NIST (Stouffer et.al, 2011) and is very useful in implementing the security controls in SCADA systems deployed in critical infrastructure. A SCADA system is different than a conventional IT System i.e. criticality of timeliness and availability of its capability all the time, having terminal devices with limited computing capability and memory resources and last but not the least the direct impact of logical execution in the physical world. Additionally, the SCADA systems usually have a static topology, a presumably regular network traffic pattern and use simple protocols (Zhu & Sastry, 2010).

The Forensic examination of SCADA systems is important post-incident to understand the design, attack vector of malware and attribute responsibility if possible, to assist law enforcement in investigation.

From the perspective of digital forensics, a SCADA system can be viewed in different layers, as demonstrated in following figure (Ahmad et.al, 2012), based on the connectivity of the various SCADA components and their network connectivity with other networks such as Internet (Bailey & Wright, 2003),



The upper layers shown in above figure correspond to the enterprise IT networks environment wherein, the routine corporate desktops, servers dealing with enterprise business operate. However, it is the first 3 lower layers (layers 0, 1 & 2) where most of the forensic analysis in SCADA systems has to be performed as these layers contain the special SCADA components and are crucial for controlling the underlying industrial processes. However, the analysis may extend to further up the higher-layers if necessitated (Ahmed et.al; 2012). As 24/7 availability is a critical requirement of a SCADA system, a forensic investigator cannot turn it off for data acquisition and analysis, necessitating use of live forensics for data acquisition and subsequent offline analysis of the acquired data (Adelstein, 2006). However, live forensics data acquisition has a few challenges in capturing data viz;

- if the data is not acquired immediately, the volatile data would be lost.
- maintaining the integrity of volatile data and its admissibility in courts of law.
- inconsistent data image.

The SCADA systems typically have a primary system and a backup system. The investigator may put the SCADA system on the backup and conduct data acquisition on the primary affected system. But it is most likely that the malware which has infected the primary system would have affected the backup system also thus making the life difficult for a forensic investigator (Stouffer & Scarfone, 2011). Forensic investigators have to deal with the problems arising from the unique features of SCADA system which limits application of contemporary forensic tools and techniques to SCADA Systems (Ahmad et.al, 2012; Fabro and Cornelius, 2008):

- predefined rules in network traffic of SCADA system may allow communication between various components of SCADA system, but may not allow communication between forensic tool and SCADA components during data acquisition.
- customised operating system kernel of the SCADA components may not be compatible with the data acquisition tool.
- resource (e.g. memory, processing etc.)- constrained nature of SCADA components (e.g., RTUs & PLCs etc.) may limit data acquisition tools.
- log- records of SCADA systems are inadequate due to limited logging capability of SCADA systems.

- large amount of data generated by individual field-components (e.g. large number of sensors).
- vendor-dependency during analysis as the SCADA components (modern as well as legacy proprietry technology) are provided by multiple vendors some of the components being forensically compatible and some not as shown in following table. (after Fabro & Cornelius, 2008).

Table 2: Modern/Proprietary Technology and Forensics Compatibility (after Fabro & Cornelius, 2008)

Modern/Proprietary Technology	Effective Audit / Logging	Forensics Complaint	Reference Materials Available
Engineering Workstations, Databases, Historian	Unknown	Unknown	No
HMI, Data Acquisition, Application Server	Possibly Yes	Possibly Yes Most Likely No	No
Field Devices (PLC, RTU, IED), Modern/Remote Comms	Probably No	No	No

Table 3: Legacy/Proprietary Technology and Forensics Compatibility (after Fabro & Cornelius, 2008)

Legacy/Proprietary Technology	Effective Audit/ Logging	Forensics Complaint	Reference Materials Available
Engineering Workstations, Databases, Historian	No	No	No
HMI, Data Acquisition, Application Server	Most Likely No	No	No
Field Devices (PLC, RTU, IED), Modern/Remote Comms	No	No	No

At present the complex SCADA environment presents a number of challenges to forensic investigator, thus preventing him from applying contemporary forensic tools and techniques. The challenges are detailed in the following lines (Wu et.al, 2013):

- Live Forensics and Data Integrity – The live forensics is a dynamic environment and the live data acquisition would not be forensically sound as volatile memory cannot be verified and traditional hash algorithms, e.g., MDS cannot be used. However, baseline hashing algorithms of the ladder logic of field devices

can be taken and stored as read-only-access in a secure unit. In case of an incident a comparison of existing logic inside the field device would provide comparison to the baseline hash. The baseline hash of the ladder logic should be updated at regular interval to ensure device integrity.

- Lack of compatible forensic tools for field devices- The incidents like 'stuxnet- attack' on Iranian Nuclear Facilities clearly demonstrate that field components of SCADA (like PLCs in this case) can be compromised. These embedded devices have low memory and processing power, thereby limiting the data retention. However, the data on RAM and flash memory would be useful for forensic investigation.
- Lack of Forensically sound storage – OPC clients and Historians are typically the available devices for storage on SCADA systems. The data stored in these devices is for specific purposes, accessible from external environments and therefore forensically unsound.
- Identification of Data Sources on a SCADA system is very difficult. The several layers of connectivity, as discussed earlier, having complex architecture makes the task inherently difficult.

Another important issue is a sound "SCADA Forensic Process Model" for preservation, identification, extraction and documentation of digital evidence so that it is admissible in courts of law from procedural proprietary of process, law and science. SCADA Forensics Models have been proposed by researchers recently (Radvanovsky & Brodsky, 2013; Wu et.al; 2013). A SCADA Forensic process Model combining incidents-response and forensic-investigative models is illustrated in the following figure (Wu et.al; 2013).

However, it has to be borne in mind that due to complexity of SCADA components, architecture, and networking and also the sophistication of attacks now a day, one has to be careful in carrying out the various steps of the SCADA forensic model.

Conclusion

The complexity of SCADA systems in terms of technology, process and architecture throw a number of challenges to be experts securing the SCADA as also in collecting forensic evidence, one an incident is reported. The embedded technology, short memory, little processing power poses limitation in live forensics. Any defence strategy to be used for SCADA system should have a judicious blend of security and usability in real time. Any process of live forensic should meet the test of nonrepudiation on procedural aspect of process, technology, science and integrity of the data has to be assured, so that it is admissible in court of Law. The attacks on SCADA systems in future are not only going to increase but would be highly sophisticated, more particularly when SCADA systems would provide a potential terrain of war for the nation states. Only a judicious use of technology and common sense would help to keep the SCADA systems secure. More research is required in designing live forensic platforms that could be applicable to SCADA environment.

Note: The views expressed in this paper are of the author and do not necessarily reflect the views of the organizations where he worked in the past or is working presently. The author convey his thanks to Chevening TCS Cyber Policy Scholarship of UK Foreign and Commonwealth Office, who sponsored part of this study.

References

Adelstein, F. 2006, "Live forensics: diagnosing your system without killing it first. Accessed online on 10/05/2014 at: http://frank.notfrank.com/Papers/CACM06.pdf", *Communications of the ACM,* Vol. 49, no. 2, pp. 63-66.

Ahmed, I., Obermeier, S., Naedele, M. & Richard III, G.G. 2012, "SCADA systems: Challenges for forensic investigators. Accessed online on 11/05/2014 at: http://cs.uno.edu/~irfan/Publications/ieee_computer_2012.pdf", *Computer,* Vol. 45, no. 12, pp. 44-51.

Ancillotti, E., Bruno, R. & Conti, M. 2013, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges", *Computer Communications,* Vol. 36, no. 17-18, pp. 1665-1697.

Bailey, D. & Wright, E. 2003, *Practical SCADA for industry. Accessed online on 05/05/2014 at: http://books.google.co.in/books?hl=en&lr=&id=jLthOQfK-UAC&oi=fnd&pg=PR5&dq=Bailey+wright+scada&ots=Qmcsp2z0Ci&sig=S6GPM2XAUEZHXzag6Mo3dAuuny4#v=onepage&q=Bailey%20wright%20scada&f=false,* Newnes.

Brewer, R. 2012, "Protecting Critical Control Systems", *Network Security,* Vol. 2012, no. 3, pp. 7-10.

Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M. & Shenoi, S. 2007, "Security Strategies for Scada Networks" in *Critical Infrastructure Protection* Springer, pp. 117-131.

Chapman, D.B. 1992, "Network (in) security through IP packet filtering. Accedon 05/05/2014 online https://www.usenix.org/legacy/publications/library/proceedings/sec92/full_papers/chapman.pdf", *Proceedings of the Third UNIX Security Symposium*.

Choo, K.R. 2011, "The cyber threat landscape: Challenges and future research directions", *Computers & Security,* Vol. 30, no. 8, pp. 719-731.

Endicott-Popovsky, B., Frincke, D.A. & Taylor, C.A. 2007, "A Theoretical Framework for Organizational Network Forensic Readiness", *Journal of Computers,* Vol. 2, no. 3, pp. 1-11.

Fabro, M. & Cornelius, E. 2008, "Recommended practice: Creating Cyber Forensics Plans for Control Systems. Accessed online on 10/05/2014 at: http://www.inl.gov/technicalpublications/documents/4113665.pdf", *Department of Homeland Security*.

Genge, B. & Siaterlis, C. 2014, "Physical Process Resilience-aware Network Design for SCADA Systems",*Computers & Electrical Engineering,* Vol. 40, no. 1, pp. 142-157.

Hildick-Smith, A. 2005, "Security for Critical Infrastructure SCADA Systems", *SANS Reading Room, GSEC Practical Assignment, Version,* Vol. 1.

Igure, V.M., Laughter, S.A. & Williams, R.D. 2006, "Security Issues in SCADA Networks", *Computers & Security,* Vol. 25, no. 7, pp. 498-506.

Malin, C.H., Casey, E. & Aquilina, J.M. 2012, "Introduction to Malware Forensics" in *Malware Forensic Field Guide for Windows Systems*, eds. C.H. Malin, E. Casey & J.M. Aquilina, Syngress, Boston, pp. xxiii-xxxviii.

Nai Fovino, I., Carcano, A., Masera, M. & Trombetta, A. 2009, "An Experimental Investigation of Malware Attacks on SCADA Systems", *International Journal of Critical Infrastructure Protection,* Vol. 2, no. 4, pp. 139-145.

Nai Fovino, I., Carcano, A., Masera, M. & Trombetta, A. 2009, "An Experimental Investigation of Malware Attacks on SCADA Systems", *International Journal of Critical Infrastructure Protection,* Vol. 2, no. 4, pp. 139-145.

Nazario, J. 2004, *Defense and detection strategies against Internet worms,* Artech House.

Provos, N., Friedl, M. & Honeyman, P. 2003, "Preventing Privilege Escalation", *Proceedings of the 12th USENIX Security Symposium* Washington DC, USA, pp. 231.

Ptacek, T.H. & Newsham, T.N. 1998, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Accessed on 05/05/2014 online http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA391565".

Radvanovsky, R. & Brodsky, J. 2013, *Handbook of SCADA Control Systems Security. Accessed online on 10/05/2014 at: http://books.google.co.in/books?hl=en&lr=&id=FMDTSr63co4C&oi=fnd&pg=PP1&dq=radvanovsky+SCADA+&ots=y7hUdArFpH&sig=_sKHqPrfbwA9mb8gvYDJOA2qn60#v=onepage&q=radvanovsky%20SCADA&f=false,*CRC Press.

Ranum, M.J. & Avolio, F.M. 1994, "A Toolkit and Methods for Internet Firewalls. Available at: https://www.usenix.org/legacy/publications/library/proceedings/bos94/full_papers/ranum.a", *USENIX Summer*, pp. 37.

Rrushi, J.L. 2011, "An Exploration of Defensive Deception in Industrial Communication Networks", *International Journal of Critical Infrastructure Protection,* Vol. 4, no. 2, pp. 66-75.

Slay, J. & Sitnikova, E. 2009,*The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems,* Springer.

Stouffer, K., Falco, J. & Scarfone, K. 2011, "Guide to Industrial Control Systems (ICS) Security. Accessed online on 05/05/2014 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.224.9549&rep=rep1&type=pdf", *NIST Special Publication,*, pp. 800-882.

Taveras, P. "SCADA Live Forensics: Real Time Data Acquisition Process to Detect, Prevent or Evaluate Critical Situations",.

Taylor, C., Endicott-Popovsky, B. & Frincke, D.A. 2007, "Specifying Digital Forensics: A Forensics Policy Approach", *Digital Investigation,* Vol. 4, Supplement, no. 0, pp. 101-104.

Wack, J.P., Carnahan, L.J. & Leibowitz, A. 1994, "Keeping Your Site Confortably Secure: An introduction to Internet Firewall. Accessed online on 05/05/2014. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=948AE719480319D3CE64A25B491BF80D?doi=10.1.1.40.2749&rep=rep1&type=pdf", .

Wack, J., Cutler, K. & Pole, J. 2002", *Guidelines on firewalls and firewall policy. Accessed on 10/05/2014 at*: http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA399879

Wright, C. 2013, "Forensics Management", *Handbook of SCADA Control Systems Security,* pp. 173.

Wu, T., Disso, J.F.P., Jones, K. & Campos, A. 2013, "Towards a SCADA Forensics Architecture. Accessed online on 10/05/2014 at: http://ewic.bcs.org/upload/pdf/ewic_icscsr13_paper2.pdf", *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, pp. 12.

Zhu, B. & Sastry, S. 2010, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy. Accessed online on 05/05/2014 at http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/zhu.pdf",*Proceedings of the 1st Workshop on Secure Control Systems (SCS).*

Cyber Crime: A Technological Threat to the Society

Dr. Shakeel Ahmad* & S.M. Uzair Iqbal**

Keywords

Computer, Internet, Cyber Crime, Network.

Abstract

Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. Internet has transformed the world into a Global Information Village. Internet made this world a virtual sleepless global market place. Internet is a global network of computer. It works in communication forms also likewise messaging, chatting, video conferencing etc.

The internet's roots can be traced from 1950's. The communication links were confined to military, defense contractors and university laboratories involved in defense related research. In this paper the authors try their best to explain the meaning, nature and importance of computer and internet, also highlights the issues pertaining to security.

Introduction

PRESENTLY in India as well as in the world the computers have become an integral part of the fast developing society. The computers are being used in various aspects such as in Banking, Manufacturing, health care, defense, insurance, scientific research, strategic policy making, law enforcement etc[1].

If we think presently about the society without the computer everything seems to be impossible for example Railway Ticketing system. Airline

1 Dr Gandhi; K.P.C; Introduction to computer: related crimes: CBI Bulletin 1996 p.6.

Author Intro:

* Assistant Professor, Department of Law, AMU, Aligarh 202002.

** Assistant Professor (Law), AMU, Murshidabad Centre (W.B.) 742223.

Ticketing as well as traffic control, Electricity bill, Telephone Bill office works etc., all seem to be impossible without the computer. Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The internet is like life in the real world being extended and carried on in another medium that cuts across the boundaries of space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. Every coin has two side likewise, internet having all benefits of anonymity, a liability, and convenience has become as appropriate place for persons interested in making use of the net for illegal gainful purpose, either monetary or otherwise[2].

Internet has transformed the world into a Global Information Village. Internet has also made this world a virtual sleeper's global market place. History is a witness to the most fact that all the technological inventions have been put to as much destructive use as constructive one. Information technologies are no different, while good people are using Information technology for finding better alternatives which can improve the quality of human life, while bad elements are using it for harming individuals, cheating others of their hard earned money, subverting and defrauding the business and to hide their crimes[3].

History and development of Internet

Internet has transformed the world into a Global Information Village. Internet made this world a virtual sleepless global market place. Internet is a global network of computer[4].

Internet and online services, sometimes called as "new media" services as in many respects similar to the traditional media as it also includes production oriented material such as music, audio, video, graphics, text and games. It works in communication forms also likewise messaging, chatting, video conferencing etc.

The Internet's roots can be traced from 1950's. In 1957 the Soviet Union launched the first Satellite, Sputnik I, triggering US president Dwight Eisenhower to creating the ARPA agency to arms race. So, the evolution of internet can be said to be started with the use of ARPANET sponsored by US military, which was set up in 1969[5].

2 Verma, S.K. & Mittal; Legal Dimensions of Cyberspace; ILI Publisher 2004, p. 228.

3 Cloniel Prasad, R.S; Cybercrime- An Introduction ed.1st 2004, ICFAI Publications; p-II.

4 Ibid; p-I

5 Dr. Chaubey, R.K; An Introduction to Cyber Crime& Cyber Law; Ed: 2009; p-57.

The first communication took place between research center at the University of California at Los Angles and the Stanford Research Institute. The ARPANET was as joint venture of Massachusetts Institute of Technology and the American Department of Defense Advance Research Project Administration as a source to establish continued communication between remote computer resources in the event of war. The communication links were confined to military, defense contractors and university laboratories involved in defense related research.

In early 1970's further innovations took place, such as electronic mail possibilities had grown. During this period other network equivalent to ARPANET being established such as the United Kingdom's Joint Academic Network (JANET) and the United States *National Science Foundation Network (NSENET)*[6].

In the year 1990 the US authorities released ARPANET and transferred it to National Science Foundation (NSFNET).

In the year 1993, Tim Berners is the person who developed the World Wide Web (www) in the European Laboratory for Particle Physics (CERN).

The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet explorer the preceding year. So, these browsers made Internet access possible from personal computers. From the mid 1990's various commercial Internet Services Providers (ISP) entered the market and offered the Internet connection through conventional telephone line[7].

On 24 October, 1955 Federal Networking Council (NFNC) unanimously passed a resolution defining the term Internet. This definition was developed in consultation with members of the Internet and Intellectual property Rights communities. The term Internet was defined as the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extension or follow-ons (ii) is able to support communications using the transmission control protocol/ Internet protocol (TCP/IP) suit or its subsequent extensions/follow ons, and or other IP compatible protocols and (iii) provides, uses or makes

6 Majid-Yar; Cybercrime & Society; p-7.

7 Ibid; pp-7-8

accessible either publicly or privately, high level service layered on the communications and related infrastructure described herein.[8]

Evolution: Nature and Scope of Cyber Crime

Cybercrime is the deadliest epidemic confronting our planet in this millennium. At present when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers cybercrime has assumed rather sinister implication[9]. It has raised its head as multi-headed hydra. Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. It has also scope for new age crime such as hacking, web defacement, cyber stalking, web jading etc.

Cyber crime is a twentieth century foetus of technological development, now which grown up like an epidemic and has become uncontrollable in the twenty-first century.[10]

The first cybercrime took place in the year 1820. Joseph-Maric Jacquard, a textile manufacturer in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquardi employee that their traditional employment and livelihood were being threatened. They committed the acts of sabotage to discharge Jacquard from further use of the new technology. So, this is the first-recorded cyber crime.[11]

Categories of Cyber Crime

There are different categories of cyber crimes, they are as follows-

i. Data Crime

a. Data Interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types

8 Adopted with the unanimous resolution by Federal Networking Council, on October 24, 1995 Available at http://www.livinginternet.com/how the internet works.htm accessed on 25th Jan 2011

9 Nagpal, Rohas; Cybercrime and Corporate Liability, CCH India, 2008 p. 166

10 Manupatra Newsline, Aug & Sep 2008.

11 Supra 9

of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream[12].

b. Data Modification

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer by tampering with data as it moves between sites[13].

In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000.

In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

c. Data Theft

Term is used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law[14].

12 CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

13 Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/network.101/ b10777/overview.htm, accessed on 28th Jan 2012.

14 Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/datathef.htm, accessed on 28th Jan 2012.

1. *Network Crime*

a. Network Interferences

Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.

b. Network Sabotage

'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things[15].

2. *Access Crime*

a. Unauthorized Access

"Unauthorized Access" is an insider's view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality[16].

b. Virus Dissemination

Malicious software that attaches itself to other software like virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim[17].

3. *Related Crimes*

a. Aiding and Abetting Cyber Crimes

There are three elements to the most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the

15 DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-, accessed on 28th Jan 2012.

16 IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, accessed on 28th Jan 2012.

17 Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, accessed on 28th Jan2012

commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact"[18].

b. Computer-Related Forgery and Fraud

Computer forgery and computer-related fraud constitute computer-related offenses.

c. Content-Related Crimes

Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.

The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of undeveloped or underdeveloped countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency[19]-

- Research study has found that one in five online consumers in the US have been victims of cyber crime in the last two years.
- RSA, the security division of EMC have released their Quarterly Security Statistics Review concerning identity theft online, phishing and malware, data breaches and data loss.
- The review found that 23 percent of people worldwide will fall for spear phishing attacks, while web pages are infected on average every 4.5 seconds.
- In Australia, cyber crime costs businesses more than $600 million a year, while in the US, one in five online consumers have been

18 Leagal Info (2009), Crime Overview Aiding and Abetting or Accessory, Available at:http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, accessed on 28th Jan 2012.

19 By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html, accessed on 28th Jan 2012.

victims of cyber crime in the last two years, equating to $8 billion.

- The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2009 Consumer Awareness Survey in the US found that 85 percent of respondents expressed concern about the safety of sending information over the Internet, while 59 percent expressed a need for improvement in the protection of the data they submit over websites.
- Reported cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims[20].
- One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites[21]. Additionally, the booming of call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained.
- The words of Prasun Sonwalkar[22] reflects the threat of cyber crime in India, India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams, claimed a study by researchers at the University of Brighton. Titled 'Crime Online: cyber crime and Illegal Innovation', the study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and that there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of call centers.

From Crime Desk of UK[23] said that online fraud is worth around £50 billion a year worldwide, with criminal gangs increasingly using the latest technology to commit crimes, provoking the Association of Police Officers to state in the FT that "the police are being left behind by sophisticated gangs".

20 PrasunSonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html, accessed on 10th Oct. 2009

21 India emerging as major cyber crimecentre (2009), Available at: http://wegathernews.com/203/india-emerging-as-major-cyber-crime-centre/, accessed on 10th Oct. 2009

22 PTI Contents (2009), India: A major hub for cyber crime, Available at: http://business.rediff.com/slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm, accessed on 28th Jan 2012.

23 Crime Desk (2009), Million Online Crimes in the Year: Cyber Crime Squad Established, Available at: http://www.thelondondailynews.com/million-online-crimes-year-cyber-crime-squad-established-p-3117.html, accessed on 12th Sept. 2011

Computer spam refers to unsolicited commercial advertisements distributed online via e-mail, which can sometimes carry viruses and other programs that harm computers. For the year to date, the UAB Spam Data Mine has reviewed millions of spam e-mails and successfully connected the hundreds of thousands of advertised Web sites in the spam to 69,117 unique hosting domains, Warner said. Of the total reviewed domains, 48,552 (70%), had Internet domains or addresses that ended in the Chinese country code ".cn". Additionally, 48,331 (70%) of the sites were hosted on Chinese computers[24].

Many of the African countries are in lack of the cyber policies and laws (many articles and news are available at[25] in this support). Due to this a cyber criminal may escape even when he is caught. Countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies.

The above text only quoated some of the examples related to US, Europe, Asia and Africa to show the horrible situation of cyber crimes. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over society with the future trends of cyber crimes are explained.

Classification of Cyber Crime:

Broadly speaking, the cyber crimes refer to all activities done with criminal intent in cyber space. They can be divided into three categories:-

1. Cyber Crime against person
2. Cyber Crime against property (against business and Non business organization)
3. Cyber Crime against Government.

1. Cyber Crime Against Person

The first category of cyber crimes committed against person include various, crimes like transmission of child-pornography, sexual

24 Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at http://www.newswise.com/articles/view/553655/, accessed on 10th Dec. 2010

25 Cyberlawtimes (2009), available at http://www.cyberlawtimes.com/forum/index.php?board=52.0, accessed on 13th Oct. 2009

harassment of anyone with the use of a computer and e-mail and cyber stalking. Any unwanted contact between two people that directly or indirectly communicates a threat or place the victim in fear can be considered stalking. The Trafficking, distribution, posting and dissemination of obscene material including pornography, indecent exposure and child pornography constitutes one of the most important cyber crimes known today. The potential harm of such a crime to humanity can hardly be over stated[26].

Similarly, the cyber harassment is a distinct Cyber crime, various kinds of harassment can and do occur in cyber space or through it. The Internet is a wonderful place to work, play and no less than a mirror of the real world and that means it also contains electronic versions of real life problems, stalking and harassment are some problems that may also occur on the Internet.

2. Cyber Crime against property

The second category of cyber crime is that of crimes against all types of property. These crimes include Hacking, unauthorized use of computer and network resources and cracking some breaks into someone else computer system often on a network or intentionally breaches the computer security. Virus is a computer programme that can reproduce itself causing destruction of data and contamination of the copyright protected creative or artistic works. You should only copy the copyrighted work with the copyright owner's permission. Infringement, impersonation or cyber fraud, cyber squatting is registering, trafficking in or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else etc. Among these Hacking and cracking are the gravest cyber crimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent has tampered with precious confidential data and information. Coupled with this, the reality is that no computer system in the world is hacking proof. So, it is unanimously agreed that any and every system in the world can be hacked.

3. Cyber Crime against Government

Cyber terrorism could be defined as the premeditated political attack against information system, computer programs, and data to deny

26 Dr. Patel, S. Banel; Cyber Crime: A burning problem: Reading Material; 3 day workshop cum conference, IT Laws and related Intellectual Property; p-184. Publication, Law centre 1. Delhi University.

service or acquire information with the intent to disrupt the political, social or physical infrastructure of a target resulting in violence against public[27].

During 1998, Liberation Tigers of Tamil Elam (LTTE) attacked a large number of Sri Lanka Embassy's computer system all over the world by releasing 800 e-mails to each embassy everyday, over a two week period with the messages, we are Internet black tigers and we are using this to disrupt your communications. This is first known attack by terrorists against a country's computer system.

Cyber Crime and Organized Crime

The internet revolution has transformed the society in general and the commercial world in particular[28]. While commercial dealing is rampant on the internet due to its reach worldwide in low cost. So organized crime also found the new opportunities and benefits on internet useful for furthering the criminal activities. The organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. Some traditional criminal groups are seeking the co-operation of e-criminals with the necessary technical skills, newer types of criminal networks operating in the area of e-crime have already emerged[29].

According to Phil Williams of University of Pittsburgh, the 'organized crime is primarily about the pursuit of profit and can be understood in Clausewitzean terms as a continuation of business by criminal means. The objective of organized crime is also to earn profits though businesses, but the only difference is that the business activity or means of contracting the business may be illegal[30].

Criminal organizations are constantly on the lookout for new opportunities as well as new ways of keeping themselves safe and away from the law enforcing authorities. Internet offers a number of services for the common man and criminals could abuse many of those services to their advantage. Internet is most inexpensible and

27 Prasad: Col. R.S.; Cyber Crime – an Introduction: p-8 ed. First 2004, Pub: ICFAI Univ. Press.

28 Ibid, p-15.

29 Dr. Tropina, Tatiama available at http://www. freedomfromfearmagazine.org. accessed on 2nd Aug. 2010.

30 Phi Williams, organized crime cybercrime Synergies Trends & Responses, 2003 available at http://www.crimeresearch.com accessed on 9th Dec. 2009.

realiable domain. These attributes attract the criminals as well as also help them in speeding up their activities. The structure of these criminal organization is different from traditional organized crime organization. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on "Stand alone" basis, as members rarely meet each other in person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organized cybercrimes groups from being detected and infiltrated by law enforcement.

Cyber Crime and Legislation of Nations

To meet the challenges posed by new kinds of crime made possible by computer technology including telecommunication, many of the countries largely industrialized and some of those which are moving towards industrialization have partly reviewed their respective domestic criminal laws from the point of adaptation, further development and supplementation so as to prevent computer related crime. A number of countries have already introduced more or less extensive amendments by adding new statutes in their substantive criminal law[31].

According to McConnell International, some countries laws are substantially or particularly updated, while some others have not updated the law. So, here in figure 1, Laws have been classified in two categories i.e. 1- updated law (Substantially or partially) 1 and 2- No updated laws.

List of Countries with Updated Laws (Partially or substantially) and no Updated Laws

S.No.	Updated Law (Substantially Partially)	S.No.	No. Updated Laws
1	Australia	1	Albania
2	Canada	2	Bulgaria
3	Estonia	3	Burundi
4	India	4	Cuba
5	Japan	5	Dominican Republic
6	Mauritius	6	Egypt
7	Peru	7	Ethiopia
8	Philippines	8	Fiji

31 Gurjeet Singh & Vidhy Sandher; Emerging of Cybercrime A challenge for new millennium; Aligarh Law Journal: Vol.-XIV & XV p – 33, year 1999-2000.

S.No.	Updated Law (Substantially Partially)	S.No.	No. Updated Laws
9	Tunkey	9	France
10	United States	10	Gambia
11	Brazil	11	Hungry
12	Chile	12	Iceland
13	Chines	13	Iran
14	Czech Republic	14	Italy
15	Denmark	15	Jordan
16	Malaysia	16	Kazakhstan
17	Poland	17	Latina
18	Spain	18	Lebanon
19	United Kingdom	19	Lesotho
		20	Malta
		21	Moldova
		22	Morocco
		23	New Zealand
		24	Microglia
		25	Nigeria
		26	Norway
		27	Romania
		28	South Africa
		29	Sudan
		30	Vietnam
		31	Yugoslavia
		32	Zambia
		33	Zimbabwe

Figure 1: List of the countries, that have updated their legislation for combating Cyber Crime. The list of countries as mentioned in figure 1 is the initiative of McConnell International that surveyed global network of information technology any Cyber Security Laws the around the world.

There is no uniformity in the legislation among the nations. So, it will be better to chart another figure which depicts which types of cyber crimes have been addressed through these updated legislations of the nation.

Australia: Has included offence related to computers in the Australian Crime Act. The penalty for damaging data in computers is imprisonment up to 10 yrs and for unlawful data in computers imprisonment from 6 months to 3 years.

Canada: Has named three Computer Crimes (a) Possession of devices

to obtain unauthorized telephone facilities; (b) unauthorized access to computer; (c) Committing mischief with data. The imprisonment varies from 2 years to upto 10 years depending the nature of the crime.

Germany: Classified Compute Crime like data spying, computer fraud, alternation of data and computer sabotage. The punishment varies from 2 to 5 years depending upon the nature of crime.

Singapore: Computer Misuse Act refers to unauthorized access to computer system with intent to commit or facilitate commission of offence, unauthorized modification of computer material etc. Punishment is Imprisonment from 2 to up to 5 yrs with fine.

Japan: Amended its penal code which, refer to activities as computer crime. Electronic record wrongfully made by a public servant's false entry in permit license or passport, interference with business by destruction or damage of computerized data, interference with computer and destruction of private and public documents.

United Kingdom: Computer Misuse Act includes unauthorized access to computer material or system and unauthorized access with intent to commit or facilitate commission of further offences as the computer crimes. The punishment is imprisonment from 6 months to upto 5 yrs.

United States: US has created a firm legal framework to deal with the peril of computer crime. Following are some of the top Internet–related laws that have been framed for this purpose: The Federal Fraud Abuse Act 1986, The Computer Misuse Act 1991, The Data Collection Improvement Act 1996, the Digital Signature Legislation 1996, The Electronic Fund Transfer Act 1996, the Federal Trade Marks Dilation Act 1996; The Intellectual Property Protection Act 1996, The National Information Infrastructure Protection Act 1996, The Telecommunication Act 1996.

The Electronic Communication Privacy Act 1997, The Electronic Theft Act 1997, The Child Online Protection Act 1998, The Internet Tax Freedom Act 1998, The U.S. Trademark Copyright Prevention Act, in Global and National Commerce Act (E-Sigh) 2000, The Uniform Computer Information Transaction Act 2000, and The Children Internet Protection Act 2001[32].

These acts classified computer crimes, as (a) willful unauthorized access of computer related to national defense or foreign relation

32 Aligarh Law Journal 1999-2000; P-34.

(b) intentional access of computer without authorization to obtain financial information, (c) unauthorized access of computer of a government department or an agency, (d) unauthorized access of federal computer, internet with intent to defraud, (e) knowingly causing transmission of data/programme to damage a computer network or deny use of computer, network etc, (f) Knowingly causing transmission of data/programme with risk that transmission will damage a computer network, data or program or without or dent use of computer, network etc. and (g) unauthorized access of computer with intent to defraud.[33]

Cyber Crime and Indian Position

The first cyber crime took place as early as in the year 1820. The crimes have, however, gained momentum in India only in the recent past. As an upshot, the Indian Parliament gave effect to a resolution of the General Assembly of the United Nations for adoption of a Model Law on Electronic Commerce. The consequence was the passing of Information Technology Act 2000. The Act aims to regulate and legalize E-Commerce and take cognizance of offences arising there from.

The Information Technology Act deals with the following cyber crimes along with others:

Tampering with Computer Source Documents

A person who knowingly or intentionally, conceals (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable.

For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file.

Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem

33 Ibid.

until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk.

Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by means is said to commit hacking.

Vinod Kaushik and Ors.v. Madhvika Joshi and Ors.[34]

The main issue in this case is whether accessing a husband's and father-in-law's email account without their permission amounts to 'unauthorized access'. In this case, the first respondent had accessed the email account of her husband and father-in-law, in order to acquire evidence in a dowry harassment case. The Adjudicating Officer held that accessing an e-mail account without authorization amounts to a contravention of section 43 of the Information Technology Act 2000. There was no compensation awarded to the complainant as the respondent had only submitted the information so obtained to the police and the court. The Adjudicating Officer, however ordered the first respondent to pay a fine of Rs. 100, as she was held to be in contravention of Section 66-C (identity theft and dishonest use of the password of any other person) of the IT Act 2000.

It is to be noted that there cannot be any defense of bonafide intention, in case of violation of privacy by accessing e-mail accounts without the consent of the user. It will be still construed as 'unauthorized access'. It is also interesting to note that the adjudicating officer relied on the reasoning that the information procured by the 'unauthorized access' was only disclosed to the Court and the police, therefore the respondent is not liable to pay any compensation to the complainant. However, Section 43 of the IT Act 2000 deals with the penalty and compensation for an 'unauthorized access' to any computer or computer system or computer network. It may be said there is a lacuna in the reasoning of the Adjudicating Officer. It also gives rise to the question whether a person is not liable to pay compensation under Section 43 if the

34 Before Sh. Rajesh Aggarwal, Adjudicating Officer, Information Technology Act, 2000, Government of Maharastra, At Mantralaya, Mumbai-400032, Complaint No. 2 of 2010. available at http://docs.google.com/open?id=0B8vVw0jzMxE0Y2EyM2I1ZTQtNmQ3Yy00MDhjLTgz... Visited on 23rd Jan. 2012

information obtained by 'unauthorized access' is only disclosed before competent authorities such as police or court. The 'unauthorized access' of an e-mail account by dishonest use of password of any other person also amounts to violation of privacy. It is covered under Section 66C of the IT Act 2000.

Publishing of information, which is obscene in electronic form

A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produced the effect of publishing), pornographic material in the electronic form.

Child Pornography

Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cyber crime. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cyber crime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start contacting children on their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object.

Accessing protected system

Any unauthorized person who secures access or attempts to secure access to a protected system is liable to be punished with imprisonment and may also be liable to fine.

Breach of confidentiality and privacy:

Any person who secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to be punished under the Information Technology Act.

K.L.D. Nagasree V. Government of India, represented by its Secretary, Ministry of Home Affairs and Ors.[35]

A writ petition was filed in the Andhra Pradesh High Court challenging the order of the respondent under Section 5(2) of the Indian Telegraph Act 1885. The respondent gave the order to intercept messages from the mobile phone of the petitioner. The Court examined the procedural safeguards that are in place in case with respect to an order of interception of communication. These safeguards are enshrined in Rule 419-A of the Indian Telegraph Rules 1951 pursuant to the guidelines laid down by the Supreme Court in the case of **PUCL v. Union of India**[36]. The Court, while considering the impugned order, decided that the order did not record the reasons for the interception. The Court also discovered that the Review Committee constituted under Rule 419-A (8) had without any reason delayed the review of the impugned order. The Court also laid down in this case that the procedural inconsistencies render any recorded evidence inadmissible in Court. The Court also observed that the enforcement agencies were not observing the correct procedure for interception of communications under Section 5(2) of the Indian Telegraph Act. It ordered that any such recording should be destroyed.

It is one of the few instances where the Court has gone on record to say that the enforcement agencies are not following the procedure established by law, with regard to giving out the orders for interception of communication under Section 5(2) of the India Telegraph Act 1885. Disregard to procedural safeguard by the enforcement agency amounts to a gross violation of right to privacy envisaged under Article 21 of the Constitution of India.

Rayala M. Bhuvaneswari v. Nagaphanender Rayala[37]

This case came up before the Andhra Pradesh High Court under a revision petition for a voice test of a tape recording. In this case, the

35 AIR 2007 AP 102, (Andhra Pradesh High Court)

36 AIR 2004 SC 1442

37 AIR 2008 AP 98 (Andhra Pradesh High Court)

Court discovered that the husband had tape-recorded a telephone conversation of his wife with her friends and parents, without her consent. Subsequently, he had been using this as evidence in the divorce case between the parties. The Court, at the very outset, held that there had been clear violation of privacy of the wife by her husband. It also cited the compilation of Federal Law on "Covertly Recording Telephone Conversation", which makes it unlawful to record telephone conversation except in one-party consent cases. One-party consent cases are those cases where the person can record their own telephone conversation without the consent or knowledge of the other party. But in this case no consent had been given by either party of the telephone conversation.

The Court held that the act of the husband was illegal and unconstitutional, and infringed upon the privacy of the wife. Even if the tapes were accurate, they could not be admissible as evidence.

This is one of cases where the Court has acknowledged that the protection of right to privacy under Article 21 of the Constitution of India is not only enforceable against the State but also against individuals. The Court also held that any recording which infringes upon the right to privacy of an innocent person cannot be admitted as evidence in a court of law.

Nirav Navin Bhai Shah and Ors. v. State of Gujarat and Another[38]

The appellants were accused of hacking into the computer system of the complainant and stealing important data. The main issue was whether criminal proceedings can be quashed on the ground that the parties have reached an amicable settlement. The Court decided that if the 'entire' dispute has been amicably settled, then the Court shall quash criminal proceeding to that effect.

In this case the appellants were charged under section 66 and 72 of the Information Technology Act 2000 along with other offences under the Indian Penal Code 1860. The complainant argued before the Court that the criminal proceeding should be quashed as the dispute is civil in nature. The Court rejected the contention, while stating that the offense cannot be viewed as a civil dispute because offenses under section 66 and 72 of the Information Technology Act 2000 are offenses against the society and cannot be condoned. The Court, however,

38 Criminal Misc. Application No. 10291 of 2006, Decided On: 28.09.2006 (Gujarat High Court)

quashed the FIR based on the reasoning that there was an amicable settlement of the 'entire dispute'. It also took into consideration that if criminal proceedings were continued, a miscarriage of justice would be the result.

The Gujarat High Court observed that violation of privacy and hacking are offenses against the society and cannot be condoned or treated as a civil dispute. However, if the parties agree to a settlement of the 'entire' dispute, then the Court may allow such settlement in the interest of justice.

Cyber crimes other than those mentioned under the IT Act

Cyber Stalking

Although there is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using Internet services. Stalking in general terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

Cybersquatting

Cybersquatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typosquatting (where one letter is different).

A trademark owner can prevail in a cybersquatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of -pocket expenses.

Data Diddling

This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed.

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

Cyber Defamation

Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Trojan Attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. It is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

Financial Crimes

This would include cheating, credit card frauds, money laundering etc. Such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

Internet Time Theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

Virus/worm Attack

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They

usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

E-mail Spoofing

It is a kind of e-mail that appears to originate from one source, although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends.

E-mail Bombing

E-mail bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of e-mail bombing can vary from individuals to companies and even the e-mail service provider.

Salami Attack

This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a programme whereby a meager sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all.

Web Jacking

This term has been taken from the word hijacking. Once a website is web jacked the owner of the site looses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site.

Crackers

These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

Hackers

These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting

to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

Pranksters

These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

Career Criminals

These individuals earn part or all of their income from crime, although they are Malcontents[39], addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture"[40].

Cyber Terrorists

There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal. Earlier when IT Act enacted in 2000, the punishment was silent but after amendment in 2008, the punishment has been prescribed.

Cyber Bulls

Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel e-mail messages are all ways of cyber bullying.

39 One who rebels against the established system.

40 Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/11/2012.

Salami Attackers

Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer.

Table 2: Various Offences under the IT Act, 2000 and their respective punishments

S. No.	Offence	Punishment	After amendment
1.	Tampering with computer source document	Imprisonment up to 3 years, Fine up to 2 lakh rupees.	
2.	Hacking with computer system	- DO –	
3.	Failure to comply with direction of the controller	- DO -	
4.	Breach of confidentiality or privacy	Imprisonment up to 2 years, Fine up to one lakh rupees.	
5.	Publishing false digital certificate	- DO –	
6.	Publishing digital certificate for fraudulent purposes	- DO -	
7.	Misrepresentation or suppression of material facts	- DO -	
8.	Failure to assist to decrypt information	Imprisonment up to 7 years	
9.	Securing access to protected systems	Imprisonment up to 10 years and fine	
10.	Publishing Information which is obscene	1st conviction – imprisonment up to 5 years and fine up to one lakh rupees. 2nd conviction – imprisonment up to 10 years and fine up to two lakh rupees.	1st conviction – imprisonment up to 3 years and fine up to five lakh rupees. 2nd or subsequent conviction – imprisonment up to 05 years and fine up to ten lakh rupees.

Challenges Posed by Cyber Crime

As the cyber law is growing, so are the new forms and manifestations of cyber crimes. Russia, China and Brazil are world leaders in cyber crime and India is fast emerging as a major hub of cyber crime in spite of enacting IT Act, 2000 to regulate and control cyber crimes. This situation raises apprehensions and concerns about the efficacy of our cyber law in dealing with cyber crimes.

It can not be disputed that Information Technology Act, 2000 though provides certain kinds of protections yet does not cover all the spheres of the I.T where the protection must be provided. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. It does not cove various kinds of cyber crimes and Internet related crimes. These Include Theft of Internet hours, Cyber theft, Cyber stalking, Cyber harassment, Cyber defamation, Cyber fraud, Misuse of credit card numbers, Chat room abuse. Even issues like cyber war against India or cyber terrorism against India have not been incorporated into the IT Act yet.

Copyright and trade mark violations do occur on the net but Copy Right Act 1976, or Trade Mark Act 1994 are silent on that which specifically deals with the issue. There is no enforcement machinery to ensure the protection of domain names on net. Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but does not hinder the violations caused in the cyberspace.

One of the important issues relating to taking legal action against cyber criminals is jurisdictional issue. The whole trouble with internet jurisdiction is the presence of multiple parties in various parts of the world who have only a virtual nexus with each other. Then if one party wants to sue the other, where can he sue? Traditional requirements generally encompass two areas—firstly, the place where the defendant resides, or secondly where the cause of action arises. In the context of Internet, both these are difficult to establish with any certainty. Issues of this nature have contributed to the complete confusion and contradictions that plague judicial decisions in the area of internet

jurisdiction. Further compounding the problem is the issue that a particular act in one national jurisdiction is legal and not barred by law, but the same activity may be considered as illegal and barred by law in another country. In such a case Governments can take action against cyber criminals only when there is a valid extradition treaty between the respective countries.

The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. When internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. A recent survey indicates that for every 500 cyber crime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cyber crime. The establishment of cyber crime cells in different parts of the country was expected to boost cyber crime reporting and prosecution. However, these cells have not quite kept up with expectations[41].

Even the basic 'e-mail tracking' procedures sometimes pose as a big challenge before the law enforcement agencies in India. It would be a 'dangerous trend' to follow to arrest or detain suspects on the basis of mere 'IP addresses' or 'e-mail addresses' as they are very easy to be spoofed and forged. It requires tremendous cyber forensics expertise to correctly trace the culprit. The recent incidents of wrongfully arresting innocent persons and imprisoning them for a considerable time on the basis of spoofed e-mail addresses is a glaring example of faulty and novice cyber forensics application in India. There is every need to strengthen cyber forensic systems to prevent the harassment of innocent people at the hands of overzealous police officers.

The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cyber crime. There has only been few cyber crime convictions in the whole country, which can be counted on the fingers. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries.

41 http://www.isrj.net/PublishArticles/289.aspx, accessed on 29th Sept 2012.

According to CID Detective, Inspector M.D. Sharath's study on cyber crimes, there is no tendency of the crimes slowing down. The 2011 research reports highlighted the new advanced threats and an increased sophistication in the attacks[42].

India is projected to be the third largest internet user base in the world in 2013 with over 120 million internet users in India. Electronic payments in India account for 35.3 per cent of the local transactions in terms of volume and 88.3 per cent in terms of value. India also has the world's second largest mobile phone user base with 894 million users as on December 2011. However, the NCRB Cyber Crime Statistics reveal that 1791 cyber crime cases are registered under the IT Act 2008. There is an increase of 85.4 per cent cases over 2010. As many as 422 cases are registered under IPC and 1184 persons have been arrested[43].

Cases filed under the Information Technology Act 2000

Radiological and Imaging Association v. Union of India[44]

A circular was issued by the District Magistrate of Kolhapur, requiring sonologists and radiologists to install silent observers (SIOB) in all sonography machines and to submit an online form F under the Pre-Conception and Pre-Natal Diagnostic Technique Rules 2003. The circular was challenged under Article 226 of the Constitution on the ground that it violates the right to privacy of the patients.

The Petitioner argued, inter alia, that there would be a violation Section 72 of the Information Technology Act 2000 if the impugned circular was implemented. The Court did not find any merit in this claim and clarified that Section 72 of the IT Act was not applicable in the case as it only deals with 'any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under'.

In this case the information was not considered to be obtained under the IT Act 2000 but under the Pre-Conception and Pre-Natal Diagnostic Technique Rules 2003. The Court also observed that the allegation of invasion of privacy due to the silent observer is far fetched as the images

42 http://thehackersmedia.blogspot.ro/2012/09/cyber-crime-biggest-challenge-to-cops.html, accessed on 28th Oct. 2012.

43 http://www.deccanherald.com/content/278754/cyber-crime-biggest-challenge-cops.html, accessed on 29th Sept. 2012.

44 2011 (113) BomLR3107 (Bombay High Court)

stored in the silent observer are not transmitted online to any server and stay stored in the sonography machine. There are also safeguards in place, including those requiring the removal of the silent observer device, and requiring the appropriate authority to enter a user name and password, which are under the control of Collector.

The Court held that right to privacy is not absolute and is subject to restrictions on the grounds of public interest. It also held that there are enough procedural safeguards to protect the privacy of the patients.

Shankara Shekhar Mishra v. Ajay Gupta[45]

The plaintiff bought a laptop for the purpose of web design and other functions. He also stored personal data on his laptop, including family photographs and bank details. The defendant, who was also involved in similar business of web design, barged into the premises of the plaintiff and snatched his laptop, which contained confidential and personal information. The plaintiff filed for a permanent injunction for the rendition of accounts, delivery of the infringing material and damages.

The Court took into consideration that there was ample amount of personal information on the laptop, which also contained vital financial data. The court asserted that the privacy of the plaintiff had already been invaded. The defendant had no right to transfer the information to any other person and the plaintiff was entitled to an injunction restraining the defendant to further transfer the information. The Court also noted that the plaintiff had gone though mental trauma and would be in constant fear that the data stored by him on the laptop may be misused by the defendant. The Court reiterated the value of privacy and stated that monetary compensation is widely recognized as the remedy to violation of right to privacy against State or individual. In its final order, the Court passed a permanent injunction restraining the defendant from infringing the copyright of the plaintiff in the "literary works" authored by the plaintiff, and restrained the defendant from disclosing the information of the defendant and his family stored on the laptop snatched to any person. In this case it is interesting to note that the Court also took into account the invasion of privacy along with the theft of laptop while deciding on the quantum of the compensation.

[45] 2011 VIIIAD (Delhi) 139 (Delhi High Court)

Interception of Communication

State of Maharashtra v. Bharat Shanti Lal Shah and Ors[46]

The legislative competence of the State to enact Sections 13-16 of the Maharashtra Control of Organized Crime Act 1999 (MCOCA) was challenged. The court, while deciding on the constitutional validity of the impugned sections, which deal with the interception of wireless, electronic or oral communication, observed that although the interception of communications is an invasion of an individual's right to privacy, the right to privacy is not absolute, thus the court must see that the procedure itself be fair, just, and reasonable[47]. It was also observed by the Court that MCOCA provides for sufficient procedural safeguards to avoid invasion of privacy, and hence the impugned sections are constitutionally valid and do not infringe upon right to privacy.

This case lays down the limits to the exercise of the right to privacy. It also reiterates that the State has the legislative competence to enact laws that may curtail the right to privacy of an individual. However, such laws should lay down fair, just and reasonable procedure with respect to the issuance and implementation of orders of interception of conversation or communication.

Amar Singh v. Union of India[48]

In this case the petitioner is a political leader of the opposition party. At the outset the petitioner had filed a writ petition before the Supreme Court under Article 32 of the Constitution, seeking to protect his right to privacy under Article 21. The petitioner in his petition mentioned that Respondent No. 7 (Indian National Congress) pressurized the Government of India and the Government of the National Capital Region of Delhi to monitor and record the phone conversations of the petitioner. The petitioner has also sued in Court asking it to direct telecom service providers to reveal the details as to the order of interception.

The Court dismissed the writ petition, on the ground that such a writ petition is frivolous, because of the change in the facts in the subsequent affidavits filed by the petitioner. In considering the facts of the case the Supreme Court said that it is the duty of the service provider to give

46 (2008) 13 SCC 5 (Supreme Court)

47 Para 60, (2008) 13 SCC 5

48 (2011) 7 SCC 69 (Supreme Court)

assistance to the law enforcement agencies, as and when required. Any violation of such a condition may lead to heavy imposition of penalty on the service provider. However, the Court observed that, "[i] n view of the public nature of the function of a service provider, it is inherent in its duty to act carefully and with a sense of responsibility." It further laid down that the service provider while acting on orders of interception should simultaneously verify the authenticity of the same from the author of the document.

In order to avoid forgery of orders of interception of communication, which may lead gross violation of privacy, the Supreme Court laid down the guidelines to be followed by the telecom service providers while assisting law enforcement agencies with intercepting communication.

Phishing

NASSCOM v. Ajay Sood[49]

The plaintiff filed the suit asking for a permanent injunction, restraining the defendants or any other person from acting under their authority to send and circulate fraudulent e-mails that appear to be sent by the plaintiff due to the use of the trademark 'NASSCOM' or any other mark which is confusingly similar.

It is the first judgment in India that recognized phishing. The Court observed that there is no law in India that deals with phishing. However, within the purview of the existing laws, it could be considered to be a form of misrepresentation, passing off and defamation.

Conclusion

Every coin has two sides so it will not be wrong to say that Technology is not an inherent evil, it is neutral; how we use it is the key. There is a lot more positive than negative that will be coming out of Internet, but we need to know how to use it and what we are getting into. The advent of computers and the Internet has been great boon to many, but at the same time it has created a number of problems for the law. On one side the Internet is a place of ideas and source of all kinds of information related with political, religious scientific and technological, but on the other side it is also full of different kind of pornographic material which are available in different format with just a click away. So it depends upon the user how he or she uses the Internet, either in positive way or in negative one.

49 2005 (30) PTC 437

Police Engagement Practices among Sub-Inspectors An Empirical Study

K. Sreekanth* & Dr. A.R. Aryasri**

Keywords

Employee Engagement, Police, Organization, Practice and Commissionerate.

Abstract

The objectives of this study include a) To identify the employee engagement practices among sub-inspectors in Hyderabad Police b) To investigate and analyze the prominent factors causing employee engagement and c) To identify issues related to engagement in Hyderabad Police commissionerate in Andhra Pradesh.

Data was collected from 102 Sub inspectors based on convenience and snow ball sampling from five zones of Hyderabad police located in Hyderabad police commissionerate. The hypotheses have been formulated and tested using SPSS software and the results have been arrived at.

The results from this empirical study indicate that fair treatment, salary and benefits, personal achievement, awareness of departmental policies and internal communication respectively are the factors that have been identified from the study that are believed to instil employee engagement in police sub inspectors irrespective of the experience.

It enables one to understand employee engagement practices in police department. Other Police Commissionerates which intend to introduce or improve employee engagement in the organization can consider these practices and thereby improve organizational culture.

***Originality/value:** Since the literature available on this topic is very scanty, this study has significant value and authenticity. Hence this study may serve as a point of reference for future studies in this area of concern.*

Author Intro:

* Research Scholar, School of Management Studies, JNTU Hyderabad, Kukatpally, Hyderabad-500085. Email: sreekanthjntuh@gmail.com

** Professor & Director, School of Management Studies, JNTU Hyderabad, Kukatpally, Hyderabad-500 085. E-mail: aryasri9@gmail.com

Introduction

IN India, the state of Andhra Pradesh enforces the law through the Andhra Pradesh Police. The Hyderabad city police the local law enforcement agency for the city of Hyderabad, Andhra Pradesh and is headed by the city Police Commissioner or the Kotwal. The Government of Andhra Pradesh controls the police through Department of Home Affairs. Hyderabad police commissionerate is bounded by its commitment to provide law enforcement in the city through its officers and men. It is also committed for building community partnerships, preventing crime, and protecting every residents of the city.

The Hyderabad police is committed to provide quality, productive, effective, and efficient policing. This includes developing stronger police-citizen relationships to foster stronger relations and develop community feeling to reduce crime. The department will continue to provide for the safety and enhancement of the quality of community life. The welfare of the community will always be on the foremost priority of the police. The department will ensure that proper rights of citizens are not compromised and that it continues to function in friendly manner. The transparency of the department will always be maintained in its entire affair.

History

1847-1948

The Nizam of Hyderabad used to appoint the Commissioners of Police who were officers of the Hyderabad Civil Service and they used to function during his pleasure. They were answerable to the Nizam directly on various matters of policing in Hyderabad city. However as far as administrative matters were concerned the Commissioner of Police used to correspond with the Home Department directly. The commissioner of Police was popularly called as "KOTWAL" and was responsible for maintenance of law and order, prevention and detection of crime etc.

Reorganization

Due to rapid increase in population, there has been a steady increase in crime. In view of the above in 1981 the City Police was re-organized; vide G.O. Ms. No. 341, Home (Pol. D) Department, dated: 1981-05-30. The following structure was instituted further:

- The disciplinary and administrative control of the force is held by the Commissioner of Police, having powers and functions of Additional District.
- The city was divided in to five zones: Hyderabad central, Hyderabad South, Hyderabad East, Hyderabad west & Hyderabad North. Each Zone is under the in charge of a Deputy Commissioner of Police (D.C.P.) of the rank of Superintendent Of Police for maintenance of Law and Order, Criminal Investigation and keeping up the morale of the force.
- Each Division is under the in charge of an Assistant Commissioner of Police (ACP) of the rank of Deputy Superintendent of Police, who works under the control of DCP. He is responsible for prevention and detection of crimes, maintenance of L&O and discipline of the force.
- Each Police station is under the in charge of Inspector of Police who is the Station House Officer (S.H.O) and performs all the duties and exercises all the powers of the S.H.O.
- The city crimes station was renamed as "Detective Department" which works under the D.C.P., assisted by ACPs and Inspectors.
- In 1992, the Government of Andhra Pradesh sanctioned 3 Joint Commissioner of Police posts in the rank of Deputy Inspector General (D.I.G.) to assist the Commissioner of Police for effective functioning and better administration of City Police each in-charge of Co-ordination, Crimes and Security.
- One Sub-Inspector of Police was to be placed in charge of Law and Order duties and another for Crime duties for each Police Station. A Divisional Detective inspector for each Division was provided for. In order to achieve this functional division it was proposed in the scheme to increases the number of posts of Sub-Inspectors and Head Constables and decreases the number of posts of Police Constables.

The main objective of this is paper to provide an insight into the Police department at Hyderabad and Police sub inspectors were invited to provide their feedback on a host of key organisation and workplace attributes such as its vision, leadership, communication, teamwork, the job itself, as well as respect and integrity within the organisation.

Employee Engagement Defined

Employee engagement refers to the level of connectedness an employee feels towards his or her organisation and the willingness to maximise his or her performance and discretionary effort as a result of that connectedness.

Engaged employees are vital to an organisation's success. Employers need employees who will go beyond just 'doing the job' – rather they need people who seek to solve problems, take the initiative, and help colleagues and customers when and where needed. Indeed, a considerable amount of research shows that engaged employees have a strong impact on important organisational outcomes like stakeholder and citizen satisfaction. Not surprisingly, engaging employees in the workplace has become a strategic priority for a great number of organisations.

Literature Review

Employee engagement is derived from studies of morale or a group's willingness to accomplish organizational objectives which began in the 1920s. The value of morale to organizations was matured by US Army researchers during WWII to predict unity of effort and attitudinal battle-readiness before combat. In the post-war mass production society that required unity of effort in execution, (group) morale scores were used as predictors of speed, quality and militancy. With the advent of the knowledge worker and emphasis on individual talent management (stars), a term was needed to describe an individual's emotional attachment to the organization, fellow associates and the job. Thus, the birth of the term "employee engagement" which is an individual emotional phenomenon whereas morale is a group emotional phenomenon of similar characteristics. In other words, employee engagement is the raw material of morale composed of 15 intrinsic and extrinsic attitudinal drivers. (E.g. Scarlett Surveys 2001).

Kahn (1990:694) defines employee engagement as "the harnessing of organization members' selves to their work roles; in engagement, people employ and express themselves physically, cognitively, and emotionally during role performances". The cognitive aspect of employee engagement concerns employees' beliefs about the organisation, its leaders and working conditions. The emotional aspect concerns how employees feel about each of those three

factors and whether they have positive or negative attitudes toward the organisation and its leaders. The physical aspect of employee engagement concerns the physical energies exerted by individuals to accomplish their roles. Thus, according to Kahn (1990), engagement means to be psychologically as well as physically present when occupying and performing an organisational role.

Most often employee engagement has been defined as emotional and intellectual commitment to the organisation (Baumruk 2004, Richman 2006 and Shaw 2005) or the amount of discretionary effort exhibited by employees in their job (Frank *et al* 2004). Although it is acknowledged and accepted that employee engagement is a multi-faceted construct, as previously suggested by Kahn (1990), Truss *et al* (2006) define employee engagement simply as 'passion for work', a psychological state which is seen to encompass the three dimensions of engagement discussed by Kahn (1990), and captures the common theme running through all these definitions.

Employee engagement has three related components: a cognitive, an emotional, and a behavioural aspect. The cognitive aspect of employee engagement concerns employees' beliefs about the organization, its leaders, and working conditions. The emotional aspect concerns how employees feel about each of those three factors and whether they have positive or negative attitudes toward the organization and its leaders. The behavioural aspect of employee engagement is the value-added component for the organization and consists of the discretionary effort engaged employees bring to their work in the form of extra time, brainpower and energy devoted to the task and the firm.

Research Design

Objectives of the study

- ❖ To study the employee engagement practices in police department with reference to Hyderabad police.
- ❖ To identify and analyze the factors which influence employee engagement practices in Hyderabad police.
- ❖ To identify and analyse specific employee engagement issues in Hyderabad police.
- ❖ To suggest certain measures to improve employee engagement to make Hyderabad city police a great place to work

Hypotheses

There is no significant association between experience and opinions about a) fair treatment of superiors towards them; b) superior behaviour at workplace; c) salary and benefits paid to police; d) degree of awareness of department policies; e) Team support; f) learning and career opportunities; g) performing challenging job; h) Informing about police activities regularly; i) feedback in police department; j) Contribution towards police department and k) existing compensation system.

Sources of the Data

As this is investigative study, the data comprises of both primary and secondary sources. The Primary data was collected through a structured questionnaire by distributing to Sub inspectors who are having three and more years experience working in different police stations which comes under Hyderabad. The secondary data was collected from journals, magazines, books and websites.

Sampling Method Used

Data was collected from 102 sub inspectors of Hyderabad police commissionerate, Andhra Pradesh based on convenience and snow ball sampling.

Statistical Tools Used

The hypotheses have been formulated and tested using SPSS software and the results have been arrived at.

Limitations of the study

- The study is limited to Hyderabad police commissionerate only.
- The sub inspectors who are having more than 3 and above years of experience in police department are only considered for relevant data collection.

Statistical Analysis

To test the reliability of data, the data collected was subjected to cronbach's alpha test. The results were:

Reliability

Reliability Statistics

Cronbach's Alpha	N of Items
.599	36

Scale Statistics

Mean	Variance	Std. Deviation	N of Items
108.27	34.300	5.857	36

Inference: Cronbach's alpha has been run for to check their reliability. The overall alpha for the all items is 0.599, which is very high and indicates strong internal consistency among the given items.

Factor Analysis

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.503
Bartlett's Test of Sphericity	Approx. Chi-Square	961.218
	df	630
	Sig.	.000

Factor Analysis is a data reduction technique. Before proceed for factor analysis first the researcher tested the eligibility of the data by checking KMO- Bartlett's test which is a measure of sampling adequacy (KMO test also tests for multivariate normality among the variables). The KMO value is .503 > 0.5 indicates multivariate normality among variables

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.841	10.669	10.669	3.841	10.669	10.669	2.761	7.669	7.669
2	2.637	7.324	17.994	2.637	7.324	17.994	2.190	6.084	13.753
3	2.433	6.759	24.752	2.433	6.759	24.752	1.931	5.365	19.118
4	1.984	5.511	30.263	1.984	5.511	30.263	1.798	4.994	24.112
5	1.857	5.157	35.421	1.857	5.157	35.421	1.764	4.899	29.012
6	1.755	4.874	40.295	1.755	4.874	40.295	1.730	4.805	33.816
7	1.520	4.222	44.518	1.520	4.222	44.518	1.724	4.790	38.607
8	1.487	4.131	48.649	1.487	4.131	48.649	1.698	4.716	43.323
9	1.365	3.791	52.440	1.365	3.791	52.440	1.599	4.442	47.764

Compo-nent	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
10	1.266	3.517	55.957	1.266	3.517	55.957	1.570	4.362	52.127
11	1.187	3.297	59.254	1.187	3.297	59.254	1.567	4.352	56.478
12	1.157	3.214	62.468	1.157	3.214	62.468	1.443	4.008	60.486
13	1.069	2.971	65.438	1.069	2.971	65.438	1.416	3.933	64.420
14	1.004	2.788	68.227	1.004	2.788	68.227	1.371	3.807	68.227
15	.947	2.631	70.857						
16	.913	2.537	73.394						
17	.862	2.394	75.788						
18	.813	2.259	78.047						
19	.776	2.156	80.204						
20	.750	2.083	82.287						
21	.664	1.843	84.131						
22	.647	1.798	85.928						
23	.590	1.638	87.566						
24	.569	1.580	89.146						
25	.533	1.482	90.628						
26	.486	1.350	91.978						
27	.445	1.235	93.213						
28	.401	1.113	94.326						
29	.372	1.032	95.358						
30	.343	.951	96.310						
31	.309	.859	97.169						
32	.283	.785	97.953						
33	.264	.734	98.688						
34	.212	.590	99.277						
35	.187	.519	99.796						
36	.073	.204	100.000						

Extraction Method: Principal Component Analysis.

Factor: The initial number of factors is the same as that of variables used in the factors analysis however not all 36 factors will be retained, in this example only the first 14 factors will be retained since their Eigen value is greater than 1.

Component Matrix[a]

	Component													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Vision	.051	-.033	.252	-.535	.227	-.045	-.102	-.051	-.009	-.071	-.050	-.477	.206	.150
Direction	.060	-.236	-.192	.098	.206	.516	.020	-.243	.114	-.201	.309	-.145	.125	-.136
Purpose	.229	.277	-.192	-.360	.318	-.056	.003	.075	-.231	.176	.377	-.155	.208	-.161
Open Commn	.195	-.288	.598	-.055	.168	.233	.044	.018	-.324	.032	.079	.125	-.005	.066
Informed	.152	.071	.059	.383	-.386	.213	-.254	.159	-.091	-.092	.324	.027	-.143	-.034
Objectives	-.291	-.473	-.020	.259	-.039	.163	.354	.197	.182	.270	.061	-.039	.009	-.240
Feedback	.061	-.024	-.130	.349	.423	-.096	-.035	.190	-.336	-.015	-.174	.099	.030	.125
Superior Behaviour	.645	-.402	.087	-.082	-.284	-.194	.200	.074	.160	.027	.109	-.214	-.074	.091
Treatment	.716	-.293	.134	-.071	-.309	-.150	.235	.100	.067	.012	.118	-.197	-.111	.117
Encouragement	.672	-.231	.061	-.149	-.044	-.020	.136	-.139	-.109	.067	-.077	.046	-.011	.098
Team Support	.395	.290	.007	-.115	.062	.180	-.105	.120	-.172	.207	-.170	.151	-.469	-.116
Job Role	-.023	.473	-.148	-.220	-.343	.184	.167	-.142	.215	.102	-.078	.206	.220	.052
Personal Achievement	.429	.430	.309	-.366	-.070	.184	.017	-.072	-.003	-.097	-.207	.165	.167	.101
Awareness	-.417	.251	.288	.080	.229	.010	.294	-.054	-.005	.207	.298	-.091	-.072	.404
Workstress	-.038	.192	.269	-.326	-.199	-.210	.164	.376	.053	-.132	.017	.157	-.060	-.262
Balance	.188	.097	.293	.148	-.040	.276	-.367	.313	.067	.070	.200	.151	.329	.253
Physical Work Environment	.348	.168	.172	-.202	.039	.279	-.173	-.246	.230	.103	.140	.235	-.277	-.035
Report	-.073	.249	.105	.010	.591	-.057	.009	-.174	.149	.225	-.088	.085	-.180	-.015

Tools	.183	.418	.096	.524	-.116	-.029	.128	-.036	-.200	-.068	-.185	-.254	-.050	.194
Knowledge	-.225	.338	.467	.065	-.002	.145	.460	.094	.085	-.069	.066	-.040	-.109	.088
Encouragement	.428	.500	-.176	.168	-.014	-.257	-.027	.260	-.060	.153	.232	-.049	-.059	-.114
Learning Oppur	.001	.121	.271	.143	.103	-.101	-.414	.463	.203	.044	-.307	-.375	.041	-.042
Training	.470	.299	-.140	.238	.101	-.060	.039	-.097	.324	-.083	.120	-.075	-.005	-.135
Special Rewards	.239	.278	.107	.455	-.104	.089	-.025	-.288	.123	.276	.101	-.116	.107	.118
Understand	-.007	.289	-.312	-.026	-.025	-.245	.234	.136	-.468	-.110	.263	.110	.039	-.043
Fair Assessment	.445	.006	-.235	.097	-.067	.397	.083	.027	-.296	.058	-.194	.032	.426	-.098
Performance Feedback	.457	.135	.284	.040	.249	-.010	.096	-.232	-.191	-.366	.001	-.210	-.090	-.220
Identification	.225	-.432	.040	.031	.252	-.407	.000	-.050	-.041	.097	.142	.303	.051	.293
Success	.180	-.286	.063	-.017	.285	.463	-.111	.207	-.093	.109	.090	-.109	-.219	-.131
Contribution	.254	-.163	.358	.157	.179	-.223	.053	.109	.145	.269	.051	.244	.297	-.272
Salary & Benefits	.418	.011	-.367	.193	.261	-.214	.059	-.282	.213	-.008	-.129	-.025	.043	-.077
Compensation System	.204	-.063	-.012	.178	.206	.286	.561	.280	.087	-.130	-.327	.114	.033	.031
Reward System	.209	-.186	.341	.284	-.081	-.216	-.266	-.217	-.054	-.336	-.065	.265	-.010	-.011
Challenging	-.011	.161	.099	.057	.338	-.045	.046	.251	.351	-.575	.231	.143	.098	.002
Public	.100	-.123	-.581	-.101	.045	.230	-.043	.176	.035	-.274	.046	.049	-.179	.338
Loyalty	.453	.041	-.401	-.153	.177	.004	-.059	.314	.267	.130	-.061	.069	-.028	.230
Extraction Method: Principal Component Analysis.														
A. 14 Components Extracted.														
Rotated Component Matrix[a]														

The first factor in the ROTATED COMPONENT MATRIX is heavily loaded with treatment. (Factor loading Value of 0.923 which is the highest for the first factor) the first factor represents treatment. The second factor is heavily loaded with Salary & benefits (0.657) hence factor 2 represents Salary & benefits and thus the subsequent factors can be interpreted based on their Eigen value. The final list of 14 factors which collectively account for 68% of the variance in the data is shown below:

S.No.	Factor Name	Factor Loading
1.	Treatment	0.923
2.	Salary & benefits	0.657
3.	Personal achievement	0.747
4.	Awareness	0.836
5.	Informed	0.755
6.	Feedback	0.628
7.	Direction	0.768
8.	Purpose	0.785
9.	Contribution	0.756
10.	Compensation system	0.805
11.	Team support	0.732
12.	Performance feedback	0.688
13.	Learning opportunities	0.860
14.	Challenging	0.822

Hypotheses

1. Treatment

Ho: There is no significant association between experience and their opinions on fair treatment of superiors towards them.

Crosstab							
			Treatment				Total
			Strongly Disagree	Disagree	Agree	Strongly Agree	
Experience	below 5 yrs	Count	1	13	9	14	37
		% within Experience	2.7%	35.1%	24.3%	37.8%	100.0%
	5-10 yrs	Count	0	18	14	9	41
		% within Experience	0.0%	43.9%	34.1%	22.0%	100.0%
	above 10 yrs	Count	0	6	12	6	24
		% within Experience	0.0%	25.0%	50.0%	25.0%	100.0%
Total		**Count**	**1**	**37**	**35**	**29**	**102**
		% within Experience	**1.0%**	**36.3%**	**34.3%**	**28.4%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.922[a]	6	.244
Likelihood Ratio	8.111	6	.230
Linear-by-Linear Association	.002	1	.966
N of Valid Cases	102		
a. 3 cells (25.0%) have expected count less than 5. The minimum expected count is .24.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on superior treats employees fairly.

2. Superior behaviour

Ho: There is no significant association between experience and their opinions on superior behaviour at workplace.

Crosstab							
			Superior Behaviour				Total
			Strongly Disagree	Disagree	Agree	Strongly Agree	
Experience	below 5 yrs	Count	1	8	14	14	37
		% within Experience	2.7%	21.6%	37.8%	37.8%	100.0%
	5-10 yrs	Count	0	15	17	9	41
		% within Experience	0.0%	36.6%	41.5%	22.0%	100.0%
	above 10 yrs	Count	0	6	11	7	24
		% within Experience	0.0%	25.0%	45.8%	29.2%	100.0%
Total		**Count**	**1**	**29**	**42**	**30**	**102**
		% within Experience	**1.0%**	**28.4%**	**41.2%**	**29.4%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.315[a]	6	.504
Likelihood Ratio	5.564	6	.474
Linear-by-Linear Association	.264	1	.607
N of Valid Cases	102		
a. 3 cells (25.0%) have expected count less than 5. The minimum expected count is .24.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on superior behaviour.

3. Salary & benefits

Ho: There is no significant association between experience and salary and benefits paid to police personnel as per qualification.

Crosstab						
			31.Salary & benefits			Total
			Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	2	10	25	37
		% within Experience	5.4%	27.0%	67.6%	100.0%
	5-10 yrs	Count	9	15	17	41
		% within Experience	22.0%	36.6%	41.5%	100.0%
	above 10 yrs	Count	7	6	11	24
		% within Experience	29.2%	25.0%	45.8%	100.0%
Total		**Count**	**18**	**31**	**53**	**102**
		% within Experience	**17.6%**	**30.4%**	**52.0%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.039[a]	4	.060
Likelihood Ratio	9.802	4	.044
Linear-by-Linear Association	6.099	1	.014
N of Valid Cases	102		
a. 1 cells (11.1%) have expected count less than 5. The minimum expected count is 4.24.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on salary and benefits are paid as per qualification.

4. Awareness

Ho: There is no significant association between experience and their opinions on awareness of department policies.

Crosstab						
			14.awareness			Total
			Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	4	29	4	37
		% within Experience	10.8%	78.4%	10.8%	100.0%
	5-10 yrs	Count	4	29	8	41
		% within Experience	9.8%	70.7%	19.5%	100.0%
	above 10 yrs	Count	5	15	4	24
		% within Experience	20.8%	62.5%	16.7%	100.0%
Total		**Count**	**13**	**73**	**16**	**102**
		% within Experience	**12.7%**	**71.6%**	**15.7%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.105[a]	4	.540
Likelihood Ratio	2.983	4	.561
Linear-by-Linear Association	.022	1	.881
N of Valid Cases	102		
a. 3 cells (33.3%) have expected count less than 5. The minimum expected count is 3.06.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on awareness of department policies.

5. Team support

Ho: There is no significant association between experience and their opinions on team support.

Crosstab						
			11.team support			Total
			Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	8	23	6	37
		% within Experience	21.6%	62.2%	16.2%	100.0%
	5-10 yrs	Count	13	14	14	41
		% within Experience	31.7%	34.1%	34.1%	100.0%
	above 10 yrs	Count	3	17	4	24
		% within Experience	12.5%	70.8%	16.7%	100.0%
Total		**Count**	**24**	**54**	**24**	**102**
		% within Experience	**23.5%**	**52.9%**	**23.5%**	**100.0%**

Chi-Square Tests			
	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	10.530[a]	4	.032
Likelihood Ratio	10.816	4	.029
Linear-by-Linear Association	.319	1	.572
N of Valid Cases	102		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.65.			

From the above table chi square is significant (sig. value is less than 0.05), reject null hypothesis. It means there is a significant association between experience and their opinions on team support.

6. Learning opportunities

Ho: There is no significant association between experience and their opinions on learning and career opportunities.

Crosstab						
			22.learning oppur			Total
			Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	18	18	1	37
		% within Experience	48.6%	48.6%	2.7%	100.0%
	5-10 yrs	Count	24	16	1	41
		% within Experience	58.5%	39.0%	2.4%	100.0%
	above 10 yrs	Count	10	14	0	24
		% within Experience	41.7%	58.3%	0.0%	100.0%
Total		**Count**	**52**	**48**	**2**	**102**
		% within Experience	**51.0%**	**47.1%**	**2.0%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.760[a]	4	.599
Likelihood Ratio	3.211	4	.523
Linear-by-Linear Association	.023	1	.880
N of Valid Cases	102		
a. 3 cells (33.3%) have expected count less than 5. The minimum expected count is .47.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on learning and career opportunities.

7. Challenging Job

Ho: There is no significant association between experience and their opinions on feeling happy to perform challenging job.

Crosstab						
			34.Challenging			Total
			Disagree	Agree	Strongly Agree	
Experience	below 5 yrs	Count	8	15	14	37
		% within Experience	21.6%	40.5%	37.8%	100.0%
	5-10 yrs	Count	7	10	24	41
		% within Experience	17.1%	24.4%	58.5%	100.0%
	above 10 yrs	Count	1	10	13	24
		% within Experience	4.2%	41.7%	54.2%	100.0%
Total		**Count**	**16**	**35**	**51**	**102**
		% within Experience	**15.7%**	**34.3%**	**50.0%**	**100.0%**

Chi-Sqwuare Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.660[a]	4	.155
Likelihood Ratio	7.571	4	.109
Linear-by-Linear Association	3.387	1	.066
N of Valid Cases	102		
a. 1 cells (11.1%) have expected count less than 5. The minimum expected count is 3.76.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on feeling happy to perform challenging job.

8. Informing activities

Ho: There is no significant association between experience and their opinions on informing about police activities regularly.

Crosstab						
			5.Informed			Total
			Disagree	Agree	Strongly Agree	
Experience	below 5 yrs	Count	14	16	7	37
		% within Experience	37.8%	43.2%	18.9%	100.0%
	5-10 yrs	Count	15	21	5	41
		% within Experience	36.6%	51.2%	12.2%	100.0%
	above 10 yrs	Count	10	7	7	24
		% within Experience	41.7%	29.2%	29.2%	100.0%
Total		**Count**	**39**	**44**	**19**	**102**
		% within Experience	**38.2%**	**43.1%**	**18.6%**	**100.0%**

Chi-Square Tests			
	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	4.155[a]	4	.385
Likelihood Ratio	4.174	4	.383
Linear-by-Linear Association	.066	1	.797
N of Valid Cases	102		

a. 1 cells (11.1%) have expected count less than 5. The minimum expected count is 4.47.

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on fell informed about police activities regularly.

9. Feedback

Ho: There is no significant association between experience and their opinions on police department encourages feedback.

Crosstab							
			7.Feedback				Total
			Strongly Disagree	Disagree	Agree	Strongly Agree	
Experience	below 5 yrs	Count	1	18	14	4	37
		% within Experience	2.7%	48.6%	37.8%	10.8%	100.0%
	5-10 yrs	Count	0	22	17	2	41
		% within Experience	0.0%	53.7%	41.5%	4.9%	100.0%
	above 10 yrs	Count	0	11	13	0	24
		% within Experience	0.0%	45.8%	54.2%	0.0%	100.0%
Total		**Count**	**1**	**51**	**44**	**6**	**102**
		% within Experience	**1.0%**	**50.0%**	**43.1%**	**5.9%**	**100.0%**

Chi-Square Tests			
	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	5.918[a]	6	.432
Likelihood Ratio	7.258	6	.298
Linear-by-Linear Association	.042	1	.837
N of Valid Cases	102		
a. 6 cells (50.0%) have expected count less than 5. The minimum expected count is .24.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on police department encourages feedback.

10. Contribution

Ho: There is no significant association between experience and their contribution towards police department is valued.

Crosstab							
			30.contribution				Total
			Strongly Disagree	Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	0	21	14	2	37
		% within Experience	0.0%	56.8%	37.8%	5.4%	100.0%
	5-10 yrs	Count	0	28	12	1	41
		% within Experience	0.0%	68.3%	29.3%	2.4%	100.0%
	above 10 yrs	Count	2	12	10	0	24
		% within Experience	8.3%	50.0%	41.7%	0.0%	100.0%
Total		**Count**	**2**	**61**	**36**	**3**	**102**
		% within Experience	**2.0%**	**59.8%**	**35.3%**	**2.9%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.708[a]	6	.138
Likelihood Ratio	9.562	6	.144
Linear-by-Linear Association	1.192	1	.275
N of Valid Cases	102		
a. 6 cells (50.0%) have expected count less than 5. The minimum expected count is .47.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis There is no significant association between experience and their contribution towards police department is valued.

11. Compensation system

Ho: There is no significant association between experience and their opinions on existing compensation system.

Crosstab							
			32.Compensation system				Total
			Strongly Disagree	Disagree	agree	Strongly agree	
Experience	below 5 yrs	Count	3	19	11	4	37
		% within Experience	8.1%	51.4%	29.7%	10.8%	100.0%
	5-10 yrs	Count	4	17	16	4	41
		% within Experience	9.8%	41.5%	39.0%	9.8%	100.0%
	above 10 yrs	Count	3	16	5	0	24
		% within Experience	12.5%	66.7%	20.8%	0.0%	100.0%
Total		**Count**	**10**	**52**	**32**	**8**	**102**
		% within Experience	**9.8%**	**51.0%**	**31.4%**	**7.8%**	**100.0%**

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.310[a]	6	.389
Likelihood Ratio	8.134	6	.228
Linear-by-Linear Association	2.385	1	.123
N of Valid Cases	102		
a. 6 cells (50.0%) have expected count less than 5. The minimum expected count is 1.88.			

From the above table chi square is not significant (sig. value is greater than 0.05), no evidence to reject null hypothesis. It means there is no significant association between experience and their opinions on present compensation system.

Conclusion

Through the empirical study conducted on sub-inspectors of Hyderabad police, it was observed that the factors which influence engagement are: fair treatment, salary and benefits, personal achievement, awareness of departmental policies and communication respectively.

The police can emerge as *high performing organisation* if it can focus on

- training its personnel on extending fair treatment to their superiors and subordinates
- Revise salary and perquisites more periodically to match the current inflation levels
- Recognise the personal achievements of the staff, motivate them for further achievements, and reward them wherever possible with financial and non-financial benefits
- Conduct more training programs to enhance the awareness o the departmental policies and procedures through appropriate documentation and creating systems in place
- Create an environment for involvement, openness, contemplation and reflection

The results of this comprehensive feedback exercise provide Hyderabad Police with a valuable opportunity to determine the types of actions needed to further engage their people and improve organisational functioning more generally.

References

1. Ms. Avanthika & Dr. A.K. Saxena , "A Study of Career Drivers of IPS Officer- Trainees" The Indian Police Journal, April - June 2012.
2. Andhra Pradesh Special Police Manual-1986, Andhra Pradesh Police Academy, Hyderabad.
3. Bates, S. (2004), "Getting engaged", *HR Magazine,* Vol. 49 No. 2, pp.44-51.
4. K. Sampath Kumar, Asst. Director, APPA, Police interface with Public – A Behavioural approach, Andhra Pradesh Police Academy, Hyderabad.
5. Kahn, W.A. (1990), "Psychological Conditions of Personal Engagement and Disengagement at Work", *Academy of Management Journal*, Vol. 33 pp.692-724.

6. May, D.R., Gilson, R.L., Harter, L.M. (2004), "The Psychological Conditions of Meaningfulness, Safety and Availability and the Engagement of the Human Spirit at Work", *Journal of Occupational & Organizational Psychology*, Vol. 77 pp.11-37.

7. Perryman Robinson and Hay day, The Drivers of Employee engagement, IES report 408, 2004.

8. Rao Purna Chandra, "Role of HRIS in improving Modern HR Operations", Vol2 (12), Advances in management, December 2009.

9. Richman, A. (2006), "Everyone wants an Engaged Workforce how can you create it?" *Workspan,* Vol. 49 pp.36-9.

10. Robinson, D., Perryman, S., Hayday, S. (2004), *The Drivers of Employee Engagement,* Institute for Employment Studies, Brighton.

11. Saks, A. (2006) 'Antecedents and Consequences of Engagement' Journal of Managerial Psychology 21(7) 600-19.

12. Schaufeli, W.B., Salanova, M., Gonzalez-Roma, V., Bakker, A.B. (2002), "The Measurement of Engagement and Burnout: a Two Sample Confirmatory Factor Analytic Approach", *Journal of Happiness Studies,* Vol. 3 pp.71-92.

13. Shaw, K. (2005), "An Engagement Strategy Process for Communicators", *Strategic Communication Management,* Vol. 9 No.3, pp.26-9.

14. Sharma Baldev R. and Raina Anupama, "Determinants of Employee Engagement in a Private Sector Organization" Vol2-3, Advances in Management, Oct 2010.

15. Hyderabad Police History and Structure, www.hyderabad police.gov.in

Ahead and Aftermath of Delhi Nirbhaya Rape Case: A Content Analysis of Sexual Assaults in Selected Newspaper in Tamilnadu

Dr. J. Sasikumar*, Ph.D and K. Madhan**

Keywords

Nirbhya, Rape, Verma, Prominence, Frequency, Placement.

Abstract

The Delhi Nirbhaya case made significant changes in political, social and legislative level in India. The media had a vital role in exposing the sensitive Delhi rape case. It gave much more importance to highlight the case and its follow-up. After the incident it had been reporting more views on sexual assaults through different ways such as articles, expert views, debate etc. The present study attempts to comparatively analyze the reporting of sexual assault cases before and aftermath of Delhi Nirbhaya rape case. The content analysis method was adopted for the present study. Two news papers namely The Hindu and The Times of India were selected for the study. 34 days papers were collected, 17 days papers were before the Delhi incident and another 17 days papers were on and after the Delhi incident. The study also covers frequency, prominence, space allotment, placement etc.

Introduction

EVEN though, the status of women has been enhanced for the last few decades, still they are vulnerable groups for attackers. According to the National Crime Records Bureau report 2013, the crimes against women are increasing year by year and it can be seen that there was no decline figure for the last few years. The total number of crimes against women in last five years (2008-2012)

Author Intro:

* Assistant Professor, Department of Criminology and Police Administration, JHA Agarsen College Madhavaram, Chennai-600060, Tamilnadu, India. Email: shasik.narco@gmail.com

** Student, Department of Criminology and Police Administration, JHA Agarsen College Madhavaram, Chennai - 600 060. Tamilnadu, India

was reported as 195856, 203804, 213585, 228650 and 244270 respectively (NCRB, 2013). The crime against women is various forms and it was categorized into crimes under Indian Penal Code and crimes under Special Laws. Some of the crimes are more cruelty in nature and considered as more sensitive and it may leave a way to make the changes in Criminal Justice System. In a way, the recent horrific Delhi's Nirbhaya case had more attention not only in India but across the world. On 26th December 2012, a 23 year old girl was raped by six member gang on a moving bus in the national capital of India and later she died in Singapore hospital. The trail of Delhi rape case was taken place in Delhi Fast track court and judgment was announced as juvenile sentenced to three years, and other four culprits sentenced to death. After this horrific incident, the protest against the incident was spread over the entire nation, the protestors wanted justice, more protection and they acted against all forms of crime against women.

Even a lot of sexual crimes are being reported in media every day, Nirbhaya case only had more attention from media, social, political and legal systems. The public reaction over the incidents was by various means like violent protests, human chain, silent march etc, the media also took this issues as special consideration and covered it for some more period of times. The various media such as daily newspapers, weekly and monthly magazines, televisions channels explored the issue in a line of attack by different ways like follow-up of the incident which included case details, victim's medical treatment, investigations, arrest of the accused, trial, public protests, public views, experts discussion and articles about the sexual crimes, women protection, loopholes of laws so on. The impact of Nirbhaya case also made some significant changes in Criminal Justice System. The government also took this as specific issue for discussion and appointed a committee headed by retired justice JJ Verma to find the real facts behind the incident and evaluate such crimes. The government also initiated some necessary steps to control such crimes in future. The political, social and legislative sectors placed some suggestions for policy makers for controlling such crucial crimes. The present paper attempts to analyze the coverage of the sexual crime news by the two selected newspaper in Tamilnadu. The present study mainly aims at compare and measure the reporting of issues of sexual assaults before and after the Delhi Nirbhaya case.

Review of Literature

The newspaper has a vital role in representation of news for the public. Newspapers, television stations and radios are among the most influential sources used by the public to develop opinions about crime and the Criminal Justice System (Chermak, 1995). In spite of informing the public about criminal activities going on in the society, studies have shown that the press over-reports violent crimes like homicide, assault, rape etc, and gives them more prominence in the layout in comparison with non-violent crime stories like property and environment crime (Cohen, 1972; Chiricos et al., 1997; Beckett & Sasson 2000; Reiner et al., 2000; Dubois, 2002).

Some of the studies further contend that such violent crimes are featured disproportionately compared to their incidence in official crime statistics or victim surveys, thereby contributing to concern over crime among the public (Davis, 1952; Sheley, & Ashkins, 1981; Marsh, 1991; Kirby et al., 1997; Westfeldt & Wicker 1998). The coverage of more sensitive issues in newspaper affects the attitude of its viewers. The importance of crime news to the readers is based on its representation. Some of the studies were conducted about coverage of the crime news which includes frequency of crime news, space allotment, prominence, placement, photos etc; Patel (2013) analyzed the cases of crimes against the elderly which were reported in Hindi newspapers, New Delhi, Uttar Pradesh and Uttarakhand editions. The paper analyses different variables such as sex of victim, crime rate of an area, and crime scene and victim-offender relationship through content analysis. Chan and Chan (2012) analyzed the newspaper report of crime influence public's perception, it included measurement of space and prominence given to crime, particularly sex and violent crime in three most circulated daily newspapers in Hong Kong.

Abodunrin et al. (2009) conducted a content analysis study on the presentation and representation of crime in Nigerian Media. They analyzed two newspapers and compare the report of the crime news coverage. Koomen et al. (2006) found that the fear of crime depend on the credibility of the news paper through the experimental study. Krouse (2005) studied school violence reported in news paper and found that 18.5% of the news was placed on front page. They also found that 20% of the information only related to offender and 21.5% of the information only related to victims. Chermak (1998)

analysed that how various crime, victim, and defendant characteristics affect the amount of space and attention provided to newspaper crime stories.

Yew (2013) addressed the women safety in India in respect of Delhi rape case. He critically evaluated the Delhi gang rape cases and the current status women in India. In his article he strongly pointed out redefining the laws against rape. Sharma (2013) made a content analysis study on representation of Delhi rape case in two newspaper namely Times of India and Hindustan Times. Their study found that the media gave extensive coverage to Delhi rape case. It also analyzed the content of editorial pages, placement, prominence, photographs and follow-up of the case. The present study attempts to differentiate the representation of sexual assault news before and aftermath Deli rape case. It also covers space allotment, placement, prominence and magnitude of the sexual assault issues.

Methodology

- To find out the frequency of sexual assault reports in selected newspaper.
- To compare the sexual assault issues before and aftermath of the Delhi Nirbhaya rape case.
- To analyze space allotment, placement, prominence of the news paper for reporting sexual assault issues.

Sampling and Coding

Content analysis method was adopted for the present study. For this study, two newspapers namely *The Hindu* and *Times of India* were selected. Convenience and purposive sampling method was adopted for the data collection. 68 papers were selected (34 each in *The Hindu* and *Times of India*). 184 issues were collected for the study. The data sources were collected by secondarily. A coding scheme containing lists of categories to look for in the papers was developed. After the collection of data from the newspapers, the frequency of occurrences of the items were taken and presented in tables. Statistical tools (mainly frequencies and percentages) were utilized in analyzing specific items gathered from the papers. Finally the data were presented in tabular form.

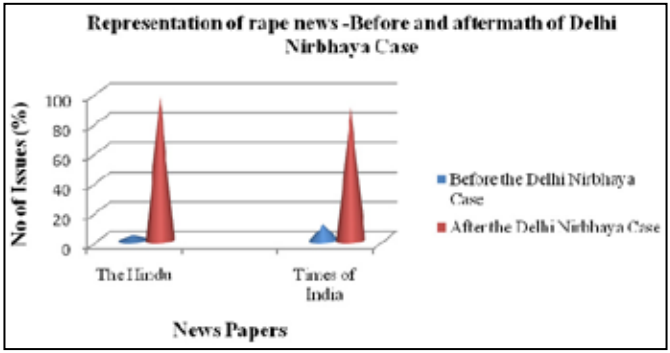
Result and Discussion

Table 1:
Representation of rape news-Before and after math of Nirbhaya's case

	The Hindu		Times of India	
Date of report	N	%	N	%
Before the incident (1st to 17th December 2013)	6[a]	3.3	10[c] (9 + 1art)	10.8
After the incident including the date where being reported the delhi rape case (18th December to 3rd January 2013)	85[b]	96.7	83[d]	89.2
Total	**91**	**100**	**93**	**100**

[a]5 Crimes news and 1 article
[b]37 Crime news and 48 article
[c]9 crime news and 1 article
[d]44 crime news and 39 article

The incident took place on 16th December, 2012 and it was reported in both media on 18th December, 2012. From the table (1), it can be seen that before the Delhi rape incident, the Hindu reported only 3.3% of crime news related to sexual assault, but after the incident the same newspaper reported 96.7% of sexual assault news which included new crime news, articles, protest against the Delhi rape etc in the same period of time. In Times of India, only 10.8% of issues were reported before Delhi rape case and after the incident 89.2% of the issues were reported. Both newspapers reported more sexual assault issues only after Delhi rape case (Figure 1).

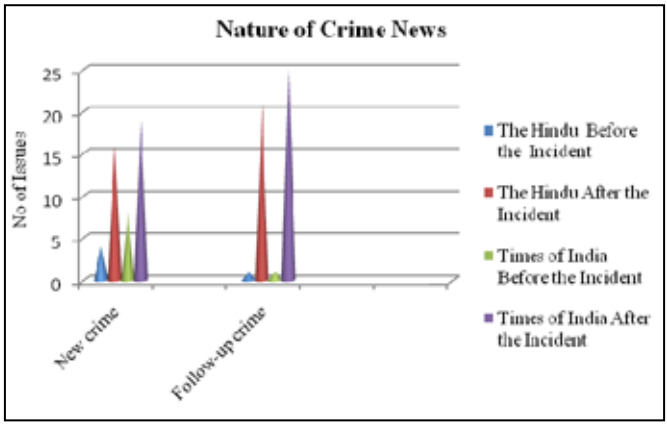


Once sensitive crimes such as terrorism, rape and murder is taken place, the media cover the issues in different aspects like follow-up, political, legislative, societal and public response on the incident. Including Delhi rape case, *The Hindu* placed 42 rape cases during the study period (1st December to 3rd January 2012). But the *Times of India* covered 53 rape cases in the same period. The same newspapers also focused more articles related to rape cases. Both news papers *The Hindu* and *Times of India* placed 49 and 40 articles respectively. It was found that totally 91 issues were covered in *The Hindu* and 93 issues were covered in *Times of India*.

The credibility of crime determines the allotment of space in the newspaper. The sensitive crimes occupied more space in the newspaper. This study found that before the Delhi rape case, *The Hindu* allotted only 387.1 cm for 6 cases (Average 64.5cm per case). The *Times of India* allotted 1145cm for 10 cases (Average 114.5cm per issue). But after the Delhi rape case, *The Hindu* allotted 36932.94cm for 85 issues (avg. 434.5cm per issue) and *Times of India* allotted 46740.88 cm for 83 issues (avg. 563cm per issue). After the Delhi rape cases space allotment for rape related news was six times higher than before the incident in both newspapers.

On basis of the locality of the crime occurrence, the news is placed in different portion of the newspaper. During the study period, it was found that *The Hindu* placed its 91 issues in various portion, mostly in *City* (27 issues), *Nation* (26 issues) and *Region* (21 issues), the rest of the issues were placed in *World* (8 issues), *Editorials* (09 issues). Meanwhile, *Times of India* placed 32 issues in *Nation*, 23 issues each in *Region* and *City* and 15 issues in *World*.

Usually sensitive cases were placed in front page of the newspaper in order to get more prominence. This study found that 18 issues were placed in front page in *The Hindu*. It is important to note that all 18 issues were placed in front page only after the Delhi's Nirbhaya case. Before that, none of issues were placed in front page during the study period and *Times of India* placed 15 issues in front page, 1 issue was placed before the Delhi rape case and 14 issues were placed in front page after the incident. *The Hindu* and *Times of India* placed the issues in other pages were 73 and 78 respectively. From the figure 1, it can be seen that 20 sexual assaults were newly reported in *The Hindu*,



among 20 cases, 4 cases were reported before the Delhi incident and 16 cases were reported after the incident. The rest of 22 issues (1 was before incident and 21 were after the incident) were found as follow-up like investigation, trial, punishment etc. In *Times of India*, totally 27 sexual assaults were reported, 8 cases were before the Delhi incident and 19 cases were after the incident. The rest of 26 issues (1 was before the incident, 25 were after the incident) were reported as follow-up.

In respect of representation of the victim's age, *The Hindu* represented victim's age in 27 cases among its 42 sexual assault cases. It did not represent about the age of victim in 15 issues. The study found that among 27 victims, 12 belonged to only 11-18 age group. 6 victims belonged to 19-26 age group, 4 victims each comes under 3-10 and above 32 age group. Whereas *Times of India* represented the victim's age in 21 rape cases among its 53 issues. It did not represent about age of the victim in 32 issues. The study found that among 21 victims, 10 victims belonged to 11-18 age group, 5 victims each coming under 3-10 and 19-26 age group. The consideration of representation of the place of occurrence, *The Hindu* reported that 7 victims were victimized at their home when they were at alone and *Times of India* reported the same as 5 victims. The study also found that some other places of crime occurrence such as isolated area (7 in *The Hindu*, 2 in *Times of India*), working place (3 in *The Hindu,* 5 in *Times of India)*, educational institutions (2 in *The Hindu*, 6 in *Times of India*), bus (including Delhi incident) (1 in *The Hindu,* 2 in *Times of India*). *The*

Hindu did not represent the place of occurrence for 22 issues and *Times of India* did not represent the same for 31 issues. The study also found that *The Hindu* and *Times of India* reported 3 crimes were committed while under the influence of alcohol. 6 issues were reported as kidnap and rape in *The Hindu* and it was reported as 5 issues in *Times of India*. *The Hindu* reported 9 sexual assaults committed by gang and it was reported as 7 assaults in *Times of India*. 24 issues in *The Hindu* and 38 issues in *Times of India* did not represent about the mode of crimes. The present study also analyzed victim- offender relationship. The study found that *The Hindu* reported 11 sexual assaults committed by the strangers, and it was reported as 10 in *Times of India*. The both news paper reported that father was identified as accused person in three cases. They sexually assaulted their own daughter under the influence of alcohol. *The Hindu* reported that teacher was identified as accused person in 1 case and it was reported as 5 cases in *Times of India*. Some other persons who involved in sexual assault were identified as doctor (1 case by Times of India), the higher officer to the victim in working places (1 case each by *The Hindu* and *Times of India*) and relative or well known person to the victim (5 cases by *The Hindu*, 1 case by *Times of India*). 21 issues in *The Hindu* and 32 issues in *Times of India* did not represent any relationship between the accused and victims.

After the Delhi rape incident, mostly all the crime news related to sexual assault were being reported. It shows that the people are getting more aware and confident about the justice and they step forward for reporting their harassment. Some of the rape cases might be in dark before the exploration of Nirbhaya's case. But after the Delhi incident, mostly all the sexual assault cases came to light. The public were more aggressive and raised voices against sexual harassment cases in all the parts of India. Obviously, Delhi rape case incident became a more sensitive and got more attention from the public, the media showed extra interest and concentrated more on highlighting the sexual harassment cases. The present study found that after the Nirbhaya case, the way of approach on sexual assaults is more sensitive. It spent more space and provided more prominent place to the sexual assault cases. It also covered articles, discussion, expert opinion, public perception etc which related to the sexual assaults. Obviously, the media deeply covered the sexual assault cases and it's follow-up.

Conclusion

The media would give more significance for reporting the crime news if the news is more credible and sensitive. The credibility of the news depend on the nature of the crime. As the Nirbhaya case was more credible and more sensitive among public, the media gave much more importance for covering the issue and reported it for some more period of times even after the incident. In addition to that, media took a vital role in making changes in the Criminal Justice System through covering the issues by various means.

References

Abodunrin, J.A., Amzat, J. & Okunola, A. (2009). *The presentation and representation of crime in Nigerian Media*. In K. Jaishankar, (Ed). International perspectives on crime and Justice, pp. (343-364), New Castle: Cambridge Scholars Publishing.

Beckett, K. and Sasson, T. (2000).*The Politics of Injustice*, Thousand Oaks: Pine Forge Press.

Chan, K.P and Chan, M.S. (2012). Public perception of crime and attitudes toward police: Examining the effects of media news. *Discovery-SS Student E-Journal,* 1: 215-237.

Chermak, S.M. (1998). Predicting crime story salience: The effects of crime victim and defendant characteristics, *Journal of Criminal Justice*, 26, 61-70.

Chermak, S.M. (1995). *Victims in the news: Crime in American news media*. Boulder: Westview.

Chiricos, T., Eschholz, S., &Gertz, N. (1997). Crime news and fear of crime: Towards an identification of audience effects. *Social Problems*, *44*(3), 342-357.

Cohen, S. (1972). *Folk Devils and Moral Panics*, London: Paladin.

Davis, J. (1952). Crime news in Colorado newspapers.*American Journal of Sociology, 52*, 325-330.

Dubois, J. (2002). *Media Coverage of Organized Crime: Impact on Public Opinion*. Ottawa: Universite du Quebec

Government ofIndia.(2013), *Crime in India*, National Crime Records Bureau, Ministry of Home Affairs.

Kirby, M., Kidd, W., Koubel, F., Barter, J., Hope, T., Kiton, A., Madry, N., Manning, P., and Triggs, K., (1997).*Sociology in Perspective*. Oxford: Heinemann Educational.

Koomen, Visser&Stapei.(2006). Credibility of news paper and fear of crime. *Journal of applied social psychology,* 30, 921-934.Retrieved on 24th September 2010 from www.interscience.wiley.com.

Krouse, M. (2005). Are you getting the whole picture? The Absence of Crime Data in Newspaper Reaportingof School Violence.*The Penn state McNair Journal,* 1, 53-71.

Marsh, H. L., (1991). A Comparative Analysis of Crime Coverage in Newspapers in the United States and Other Countries from 1960-1989. A Review of the Literature.*Journal of Criminal Justice*, 19(1), 67–80.

Patel, A.B. (2013). Effect of crime on the wellbeing of the elderly: A content analysis study of Indian elderly. *International Journal of Criminology and Sociological* Theory 6(2): 1138-1149.

Reiner, R., Livingstone, S., and Allen, J. (2000). Casino Culture: Media and Crime in a Winner-Loser Society. In K., Stenson and R., Sullivan (eds) *Crime, Risk and Justice,* 175-93, Cullompton: Willan

Sharma, B. (2013). *Media Activism and Public Participation: A Case Study of Delhi Gang Rape with focus on Indian Print Media*. Retrieved from rhttp://amic.org.sg/conference/AMIC2013/Full%20Papers/F4/Bindu%20Sharma.pdf on 13th November 2013.

Sheley, J., &Ashkins, C. (1981).Crime, Crime News and Crime views.*Public Opinion Quarterly*, *45*(4), 492-506.

Westfeldt, W., and Wicker, T. (1998).*Indictment: The News Media and the Criminal Justice Media*. In (1999) *Newswatch,* 03/12/1999.

Yew, L.K. (2013). The *Delhi gang rape: Addressing the women's Safety and public outrage*. School of Public Policy, National University of Singapore. Retrieved from http://lkyspp.nus.edu.sg/wp-content/uploads/2013/10/LKYSPP-Case-study_The-Delhi-Gang-Rape-Case.pdf on 13th November 2013.

Justice for Juvenile

Kumar Vivek Kant*

Keywords

Juvenile Justice, National Policy for Children, Juvenile Justice Act, Deliquency.

Abstract

Children constitute the most vulnerable section of society and are considered a supremely important asset of our nation. Protection and Development programmes for the specially disadvantaged children should ensure that every child has equal opportunities for optimum personal growth. Socio-economic circumstances of a family often result in family stress, disintegration and child destitution. Special programmes have been evolved as a response to the needs of such families "at risk". These services supplement or substitute parental care and supervision, to promote the overall well-being of vulnerable children; prevent neglect, abuse and exploitation of children and provide care and shelter for disadvantaged children.

Introduction

THE practice of child protection has undergone a significant change when seen from a historical perspective. The traditional approach of custodial care in an institution is being replaced because of a strong conviction that the Right to Family is one of the most basic rights of a child. Recognising this right of a child to a family, all interventions must try and ensure that the physical, social, emotional and educational needs of the child are met in a secure, nurturing family environment. The primary focus of social work intervention is the strengthening of the family, prevention of family

Author Intro:

* Research Scholar, Department of Sociology, BHU, Varanasi, U.P.

disintegration and abandonment of children. Traditionally in India, the child without parents was looked after by the joint extended family, but these systems slowly disintegrated and the problem of child destitution has been on the increase. While institutional care has been one of the alternatives, even the best of institutions cannot be a substitute for the individualised care that a family can provide.

The traditional approach of long-term institutional care resulted in the child being separated from his family environment. Research studies and experiences have shown that the negative and painful experiences in large, de-personalised institutions could result in an "Institutionalised Child Syndrome" accompanied by serious psychological problems. The predominance of institutional care may lead families to seek institutionalisation as an option for caring for their children, when faced with crisis. The cost of child care in an institution also far outweighs its advantages, and even the best of institutions cannot substitute for the care in a family. Hence it is better to provide support to the families in crisis through alternate family based and community oriented noninstitutional Services, so that the child can be looked after within his / her own family environment.

Importance of Child

The National Policy for Children adopted by the Government of India in 1974 declared that the nation's children are a supremely important asset and that their nurture and solicitude are the responsibility of the State. It shall be the policy of the State to provide adequate services to children, both before and after birth and through the period of growth, to ensure their full physical, mental, and social development. The state has undertaken to protect children against neglect, cruelty and exploitation.

The Supreme Court emphasising the importance of Child's welfare in L.K. Pandey, V. Union of India rightly remarked:

> *"The welfare of the entire community, its growth and development depends upon the health and well-being of its children. The great poet Milton put it admirably when he said: "Child shows the man as morning shows the day". Children need special protection because of their tender age and physique, mental immaturity and incapacity to look after themselves."*

The Preamble of the Declaration of the Rights of the Child, 1959 mandates that "the child, by reason of his physical and mental immaturity needs special safeguards and care including appropriate legal protection, before as well as after birth" and further it States that" mankind owes to the child the best it has to give."

World renowned Poet William Wordsworth (1770-1850) said that "Child is the father of the man". In one line the poet imagined that reality that children are the hopes and future of mankind.

So far the importance of the child in society.

2. Status of Child

UNICEF in its report says:

> *"Of the more than 100 million out of school youth, 60 million are girls. Between 60 million and 100 million women are missing from the world's population. Victims of gender-based infanticide, Foeticide, malnutrition and neglect. 90 percent of domestic workers, the largest group of child workers in the world, are girls between 12 and 17 years old. In some areas, HIV infection rates are five times higher for girls than for boys."*

Further in another report it is said that" an estimated 10 crore children, abandoned by their families, lived on the streets of the world's cities in the 1990s. Approximately 15.5 crore children were living in absolute poverty crore in urban areas and 11.5 crore in rural areas".

This report by UNICEF shows a very dismal condition of the children which requires immediate ameliorative measures. The Government of India mentioned "that there were 38 crore children below the age of 14 years. The literacy rate is 28.4 7 per cent for girls and 53.48 per cent for boys in the age group of 5-9 years. India has the largest number of working children in the world. The working conditions for child labourers are usually very harsh. For example, it was found that about 45000 children between the ages of 5 and 15 years work almost 12 hours a day in the match and fire works industries with hazardous chemicals in cramped environments with inadequate ventilation. In the bidi industry, children between 8-12 years of age, put in long hours and often contact chronic bronchitis and tuberculosis. Children from poor families are compelled to join the labour force because of the need to supplement the family income. Poverty, neglect ill-treatment,

and family discord are forcing an increasing number of children to run away from home and take shelter on the streets.

In such a dismal picture of children in India, the research scholar "makes a modest attempt to analyse the concept of Juvenile Justice in the context of legal frame work presented by Juvenile Justice (Care and Protection of Children) Act, 2000 in short 79 (C&P) Act, 2000.

Meaning and Definition of Juvenile

Juvenile or child is commonly known as person who has not completed eighteenth years of age. Recognition rests on our concept of adolescence (juvenile) as a status between childhood and adulthood. During childhood the individual is largely dependent upon parents or guardians for his material and social well-being, and during adulthood he is largely responsible for himself. But the adolescence is midway between the two in that he is still largely dependent on his parents for his material needs but has begun to acquire identify and social relationships apart from them and their social spheres.

The dictionary and statutory meaning of juvenile are given as:

Dictionary Meaning

Juvenile

As an adjective juvenile means pertaining to, characteristics of or suitable children and as a noun it is used in the sense of a young person.

(a) (i) Juvenile of pertaining to, characteristic of or suitable of or intended for young persons.

(ii) Young, youthful

(iii) Immature, childish, infant

(iv) Young persons

(b) Pertaining to, suitable for, or intended young persons, young

(c) (i) Young pertaining or suited to youth or young people.

(ii) Having or retaining characteristics of youth.

(iii) Childish

(d) "A persons below the legal age of responsibility and above a certain minimum age, who is held to be punishable for breaking

the law, or designating young offenders against the law or the offences committed by them esp. in juvenile delinquency, delinquent, also juvenile adult.

Delinquent

(a) "One who neglect a duty or one who commits a fault, a criminal"

(b) "Failing in or neglectful of a duty or obligation, guilty of a misdeed or offence" .

(c) "Failing in or neglectful of a duty or obligation, more generally, guilty of a misdeed or offence".

Delinquency

(d) "fault, offence, omission of duty

(e) (i) Failure in, or neglect of duty or obligation, fault, guilt

(ii) a shortcoming a misdeed or offence".

Thus, "juvenile delinquency" means behaviour of a child or youth that in marked by violation of law, persistent mischievousness, antisocial behaviour, disobedience, or intractability as to the ward correction by parents and to constitute a matter for action by the juvenile court and "juvenile delinquent" means a minor who cannot be controlled by parental authority and commits antisocial or criminal acts as vandalism or violence. A child or youth characterized by juvenile delinquency. However, the most common criteria employed is chronological age.

There are two concepts, named delinquent child and neglected child always overlapping to each other, and creating confusion in the mind, so the distinction between both concepts is necessary for understand the bare meaning of delinquent child. The New York State Law defers between both concepts as follows:

On the one hand the term "delinquent child" small means a child over seven and under sixteen years of age: (a) who violates any law of the United States or of this State or ordinance of the City of New York, or who commits any act which if committed by an adult would be a crime, except any child fifteen years of age who commits any act which if committed by an adult would be a crime punishable by death or life imprisonment, unless an order removing the action to

the children's court has been made and field pursuant to section three hundred twelve-c subdivision (c) and section three hundred twelve-f subdivision (a) and (b) of the Code of Criminal Procedure (b) who is incorrigible, ungovernable or habitually disobedient and beyond the control of his parents, guardian, custodian of other lawful authority; (c) who is habitually truant; (d) who, without just cause and without the consent of his parent, guardian or other custodian, deserts his home or place of abode; (e) who engages in any occupation which is in violation of law; (f) who begs or who solicits aims or money in public places; (g) who associates with immoral or vicious persons; (h) who frequents any place the maintenance of which is in violation of law; (i) who habitually uses obscene or profane language or (j) who so deports himself as wilfully to injure or endanger the morals or health of himself or others.

And the term "neglected child" shall mean a child under sixteen years of age (a) who is without proper guardianship (b) who has been abandoned or desecrated by either or both of its parents or by any other person or persons lawfully charged with its care and custody, (c) whose parent, guardian or person with whom the child lives, by reasons of cruelty, mental incapacity, immorality or depravity is unfit properly to care for such child; (d) whose parent or guardian has been sentenced to imprisonment for crime; (e) who is under lawful or improper supervision, care, custody or restraint by any person, (f) who wanders about without lawful occupation or restraint, or who is unlawfully kept out of school, (g) whose parent, guardian or custodian neglects or refuses, when able to do so, to provide necessary medical, surgical institutional hospital care for such child (h) who is found in any place the maintenance of which is in violation of law, (i) who is in such condition of want or suffering or is under such improper guardianship or control as to injure or endanger the morals or health of himself or others.

The Pennsylvania Statute defines a neglected child as:

- A child who is abandoned by his or her parent, guardian, custodian or legal representative.
- A child who lacks proper parental care by reasons of the fault or habits or his or her parent, guardian, custodian or legal representative.

- A child whose parent, guardian, custodian, or legal representative neglects or refuses to provide proper or necessary subsistence, education, medical or surgical care, or other care necessary for his or her health, morals or well being.

International Guidelines

United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)

As states began to establish their own juvenile justice systems, the need became apparent during the 1980's for an international coherent framework within which states would be able to operate their systems of juvenile justice. In 1985, the General Assembly adopted the United Nations Standard Minimum Rules for the Administration of Juvenile Justice known as the Beijing Rules which provide a model for states of a humane response to juveniles who may find themselves in conflict with the law. Some of the Rules have been incorporated into the Convention on the Rights of the Child. Hence the duty on states parties to establish a minimum age for criminal responsibility has been strengthened by virtue of being enshrined in article 40(3)(a) of the Convention.

The Convention on the Rights of the Child

States are also beginning to accept limitations placed on their discretion in both the use and the length of time for which children can be deprived of their liberty in comparison to adults children are even more 'highly vulnerable to abuse, victimization and the violation of their rights'. These limitations are found in article 37(a) and (b) of the Convention on the Rights of the Child and emphasize that the detention or imprisonment of children should only be as a measure of last resort and only for the shortest appropriate period of time. In addition states parties are prohibited from imposing life imprisonment without the possibility of release.

The United Nations Rules for the Protection of Juveniles Deprived of their liberty: Despite the provisions of the Convention, there still remained a paucity of detailed international law protecting the rights of children deprived of their liberty. In 1981 the British Section of Amnesty International produced draft rules for the protection of children deprived of their liberty and enlisted the willing support of

other non-governmental organizations in lobbying for their adoption by the international community. The initiative of the non-governmental organizations resulted in the United Nations Rules for the Protection of Juveniles Deprived of their liberty which set out a detailed code on the management and conditions of all forms of institutions, penal and otherwise, in which children are deprived of their liberty. Their drafting and subsequent adoption provided the Secretary-General of the United Nations with a legislative framework within which he was able to appoint a Special Rapporteur on the application of international standards concerning the human rights of detained juveniles.

The United Nations Guidelines for the Prevention of Juvenile Delinquency (the Riyadh Guidelines): States are also beginning to accept guidance on preventive policies which seek to prevent children coming into conflict with the law. As well as being an unusual area for international law to enter, it is a field fraught with hidden dangers. There is the risk that the aims of prevention could be abused and the wafer-thin line dividing prevention and indoctrination be crossed. These risks are enhanced by the lack of a commonly accepted precise meaning of the term 'delinquency'. The United Nations Guidelines for the Prevention of Juvenile Delinquency otherwise known as the Riyadh Guidelines aims at protecting those who are abandoned, neglected, abused or who live in marginal circumstances. The Guidelines focus on early protection and preventive intervention paying particular attention to children in situations of 'social risk.Together the Riyadh Rules, the Beijing Rules and the Deprivation of Liberty Rules form a triptych on which is sketched a coherent and humane approach to child justice

The International Umbrella Principles

- Juvenile justice legislation should apply to all those under the age of 18
- Juvenile justice is a part of the national development process of a State and as such should receive sufficient resources to enable juvenile justice to be organized in accordance with international principles;
- The principle of non-discrimination and equality is applicable to juvenile justice, and this includes a prohibition on discrimination on account of the child and the child's family (article 2 of the Convention on the Rights of the Child);

- The guiding principle for any policy or action concerning juvenile justice is that the best interests of the child is a paramount consideration (article 3, para. I, of the Convention);
- Delay in deciding matters relating to a child is prejudicial to the best interests of the child (article 37(d) and article 40, paras. 2(b)(ii) and 2(b)(iii), of the Convention) ;
- Every child shall be treated with humanity and with respect for the inherent dignity of the human person, taking into account the age of the child (article 37(c) of the Convention);
- At all stages, children should be treated in a manner that facilitates their reintegration into society and their assuming a constructive role in society (article 40, para. 1, of the Convention);
- Children are entitled to express their views freely in relation to criminal justice, and the views of the child should be given due weight in accordance with both the age and the maturity of the child (articles 12 and 13 of the Convention);
- Children have the right to seek, receive and impart information concerning the juvenile justice system in a form that is both accessible and appropriate to children (article 13 of the Convention and guideline 11 (b) of the Guidelines for Action on Children in the Criminal Justice System);
- Juvenile justice should be organized in a manner consistent with children's rights to privacy, family, home and correspondence (article 16 of the Convention);
- If children are deprived of their family environment they are entitled to special protection and assistance (article 20, para. I, of the Convention);
- No child shall be subject to torture or to other cruel, inhuman, degrading or harsh treatment or punishment (article 37 of the Convention and rule 87(a) of the United Nations Rules for the Protection of Juveniles Deprived of their Liberty);
- At any stage of the juvenile justice process, children should not be unlawfully or arbitrarily deprived of their liberty (article 37(b) of the Convention);
- The arrest, imprisonment or detention of children should only be used as a measure of last resort and for the shortest appropriate period of time (article 37(b) of the Convention);

- Parents are to be notified of any arrest detention, transfer, sickness, injury or death of their child (article 9, para. 9, of the Convention and rule 56 of the United Nations Rules for the Protection of Juveniles Deprived of their Liberty)

National Approach

The Constitution of India

Articles 14, 15, 15(3), 19(1) (a), 21, 21(a), 23(1),24, 39(e), 39(f) and 45 have a direct reference and impact on the welfare and development of the nation's children.

The National Policy For Children

Declared by the Government of India in 1974.

To ensure that programmes of children are incorporated in the National Plans for the development of Human Resources.

To ensure effective services for children in the areas of Health, Nutrition, Education and Recreation with special emphasis on the weaker sections of society.

Inorganising these services, efforts would be directed *to* strengthen family ties, so that full potentialities of growth of children are realised within the normal family and community environment"

National Plan of Action

Prepared by the Government of India under the title "A Commitment to the Child".

The NPA had particular significance for Children in Need of Care and Protection (CNCP) since it identified the various target groups of vulnerable children and called for improved protection of these children.

The Plan is an outcome of an Inter-Sector, Inter-Department co-ordination and covered areas of health, nutrition, water and sanitation, education, children in need of care and protection, girl child, adolescent girls, children and environment, women, advocacy and people's participation, resources, monitoring and evaluation

United Nations Convention on the Rights of the Child (CRe)

The Convention on the Rights of the Child (CRe) drafted by the UN Commission on Human Rights, was adopted by the General Assembly of the United Nations on 30th November 1989.

The CRC represents a turning point in the international movement on behalf of Child Rights.

A comprehensive document containing a set of universal legal standards for the protection and well-being of children.

The umbrella principle of the CRC is "The Best Interest of the Child" and that the essential needs of children should be given the highest priority at all times in the allocation of resources.

The CRC gives children their basic human rights - civil, economic, social,cultural and political, which enable children to achieve their full potential.

The CRC derives strength from its ratification by governments, implying that governments agree to follow the principles and are committed to certain standards in dealing with children.

India ratified the Convention on 11th December 1992, thereby re-affirming its commitment to the cause of children in India

The Juvenile Justice ACT 1986

The Juvenile Justice system in India is based on the principle of promoting, protecting and safeguarding the rights of children. Recognising the vulnerability of children and the need for special and different treatment, it was in 1986 that for the first time, a uniform Juvenile Justice Act (JJA) was enacted for the whole of India, when Parliament decided to replace the Children's Acts in various states in india. This Act incorporated the UN Standard Minimum Rules for administration of Juvenile Justice ('Beijing Rules') of 1985. It was enacted for the care, protection, treatment, development and rehabilitation of neglected or delinquent children. However, the history of the implementation of the JJA, 1986, is a history of hopes not realised and promises not fulfilled Juvenile Justice ACT 2000.

A review of the JJ Act 1986 was undertaken to look in to the lacunae as well as its non implementation. This process together with India's ratification of the UN Convention on the Rights of the Child (CRe)

in 1992, as well as the changing social attitudes towards offences by children and the need for a more child- friendly juvenile justice system were some of the factors that led to the passing of the Juvenile Justice (Care and Protection of Children) Act 2000 (JJA 2000). This Act replaced the earlier Act of 1986.

The JJA, 2000 was based on the principles of the UN Convention on the Rights of the Child, the 'Beijing Rules', the United Rules for the Protection of Juveniles Deprived of their Liberty and all other relevant national and international instruments clearly defining children as persons upto the age of 18 years. The Act is based on the provisions of the Indian Constitution and the UNCRC.

The Juvenile Justice Act, 2000, which is aimed at rehabilitating juvenile offenders in order to bring them back to main-stream society and to give them an opportunity to rehabilitate themselves as useful citizens of the future. In fact, the definition of "juvenile" in the 1986 Act was altered in the Juvenile Justice, Act, 2000 to include persons who had not completed 18 years of age. In other words, the age until which a male child in conflict with law would be treated as a juvenile was raised from 16 years to 18 years.

The Juvenile Justice Act, 2000, was enacted to deal with offences allegedly committed by juveniles on a different footing from adults, with the object of rehabilitating them. The need to treat children differently from adults in relation to commission of offences had been under the consideration of the Central Government ever since India achieved independence With such object in mind, Parliament enacted the Juvenile Justice. Act, 1986, in order to achieve the constitutional goals contemplated in Articles 15(3), 39(e) and (f), 45 and 47 of the Constitution imposing on the State a responsibility of ensuring that all the needs of children are met and that their basic human rights are fully protected.

Juvenile Justice (Care & Protection of Children) Amendment Act, 2006

A review of the JJ Act, 2000 was undertaken to make ammendments in the existing legislation. In 2006, the act was further revised with 26 ammendments and came into effect from 22nd Aug 2006. It was widely perceived that even the 2000 Act did not achieved what it set out to

do and that the justice-delivery system for juveniles continues to suffer from neglect and apathy. For instance, empirical studies indicated that there were extensive delays in the disposal of cases on the account of the omission to constitute Juvenile Justice Boards in many districts. Furthermore, monitoring by voluntary sector organisations regularly indicated that the infrastructure in many of the government-run homes where the children are kept does not meet the minimum standard required for a humane living. Such reports prompted the Parliament to intervene again and an amendment was made to the Act in 2006, with the primary intent of speeding up the administration of justice for juveniles.

Conclusions and Recommendations

The fundamental premise underlying the Juvenile Justice (Care and Protection of Children) Act, 2000 is that children in conflict with Law and children who need care and protection would fall within the ambit of Juvenile Justice System. While building in certain avenues for release of the child either to parents, guardians, fit persons or adoptive parents and to people who would provide foster care, the systems logic is to provide what the preamble of the Act calls 'proper care, protection and treatment by catering to their development needs' within an institutional setting. These institutions designated as observations homes, childrens homes and special homes share one feature in common they are all closed institution, which completely deprive the child of his or her liberty.

The Juvenile Justice (Care and Protection of Children) Act, 2000 has included many new measures for social reintegration of the Juvenile. The most important among them is adoption. The Act recognizes that the primary responsibility of looking after Juveniles lies with their family. After a proper scrutiny, a child falling within the provisions of the Act may be declared available for adoption and given in adoption.

The Juvenile Justice (Care and Protection of Children) Act, 2000 has incorporated various provisions and principles for ensuring additional care and protection to the children is conflict with law and children in need of care and protection for their rehabilitation and reintegration to society. These special provisions are in conformity with the UN Standard Minimum Rules for the Administration of Juvenile Justice 1985 (the Beejing Rules).

The Juvenile Justice (Care and Protection of Children) Amendment Act 2006

To modify the long title of the Juvenile Justice Act (JJA) so as to broaden the scope of rehabilitation of the child in need of care and protection or a juvenile in conflict with law under the Act through not only the institutional but also the non institutional approach and to clarify that the JJA shall apply to all cases of detention or criminal prosecution of juveniles under any other law. Juvenile Justice Amendment Act 2006 to remove doubts regarding the relevant date in determining the juvenility of a person and the applicability of the JJA and to provide for alternatives to detention in the observation home in order to achieve the intentions of the JJA.

Recommendations

For Implementation of International Instruments these mechanisms may be established:

Under the Convention of the Rights of the Child and other important international instruments, a State may require review and amendment of existing legislation and policies in light of the standards enshrined in these instruments. Realizing effectively the rights of the juvenile/child in the field of juvenile justice which provided in the important international instruments, it is necessary to establish 'the mechanisms for advising, monitoring and reporting the implementation of these instruments. Under these mechanisms, a State may request the assistance of the Secretary-General and non-governmental organizations in adapting legislation and policies and in the development of alternatives to institutionalization.

Introducing Reliable Training System for the Personnel Working for the Juvenile Justice Field:

There are various kinds of practical principles and guidelines based on the international instruments. To implement these practical principles and guidelines aimed at a holistic approach, development of systematic and wide range of training system is a keen issue. When developing these training systems, national and local government budgets and various community resources should be provided to them as a first priority of the government policy.

References

1. (1984) 2SSC 244
2. Their state of the world's children 2002
3. UNICEF policy review
4. Ruth S. Cavan and Theodore N. Ferdinand, Juvenile Delinquency (Horper & Row Publishers, New York, 1981) at 26.
5. Random House Dictionary.
6. The America College Encyclopedia.
7. Chamber's Dictionary
8. The Oxford Dictionary IInd ed.
9. Webster Universal Dictionary.
10. Martirl H. Nevmeyer, Delinquency in Modern Society at 25
11. Monrad G. Paulsen", liThe legal Framework for Child Protection", Columbia Law Review, 1966, Vol. 66 at 694.
12. Ved Kumari, Treatise on the Juvenile Justice Act, 1986, (Indian Law Institute, New Delhi, 1993) at 18.
13. Child protection and juvenile justice system for children in need of care and protection (Dr Nilima Mehta)
14. Juvenile justice system (a project of Legal Assistance Forum in association with Unicef) 2008

Pro-Active Judgment but Retro-Active Implementation Pertaining to Human Rights

Dr. K.R. Shyamsundar*

Kewords

Judgement, The Supreme Court of India, Human Rights, Pro-active, Judgement, Retro-active Judgement, Contempt of Court.

Abstract

The purpose of the Supreme Court's pro-active judgment in DK Basu is to bring in transparency and accountability and on record it appeared to have been complied with to the extent of 100%. However, it is evident from scientific research that the very purpose of SC requirements has been defeated not only by the police but also by the defense lawyers of victims of the entire sample of 411 cases. Unfortunately, not even a single case has been taken for Contempt of Court against any one of the Investigating officers, either by defense counsels or by any human rights activist NGO and consequently no erring police officer faced departmental disciplinary action.

Introduction

POLICE officers at the cutting edge level were found wanting in knowledge on the recent pronouncements of the Apex Court regarding arrest, search, seizure, investigation etc. in 70's. The National Police Commission of India opined that 60% of arrests were unnecessary and that except in heinous offences like murder, rape, dacoity or other professional property offences, arrests of the suspect needed to be made, while in other cases unless the accused would abscond or would threaten witnesses or tamper evidence no arrest was required to be made. The Supreme Court not only agreed with

Author Intro:

* DGP (Retd) and Special Rapporteur, SZ – I, National Human Rights Commission, New Delhi

the recommendations of National Police Commission but also made it a mandatory requirement. In this connection, it is appropriate to present the observations of the Supreme Court in Joginder Singh V. Uttar Pradesh (Joginder Singh V. State of Punjab, 1994 3 SCC 423), in which it held that the existence of power to arrest was one thing and the justification for exercise of it was quite another and remarked that it would be prudent for a police officer in the interest of protection of the constitutional rights of a citizen and perhaps in his own interest that no arrest shall be made without a reasonable satisfaction, reached after some investigation as to the genuineness and bonafieds of a complaint, and a reasonable belief both as to person's complicity and even as to the need to effect arrest.

In order to bring in transparency and accountability in police functioning, the Supreme Court in D.K.Basu V. State of U.P. case issued eleven requirements to be followed scrupulously and added that non-implementation would not only amount to Contempt of Court but also attract department action against the erring police officers. In addition, as per the directions of SC, the eleven commandments were painted in two conspicuous places in every Police Station throughout India.

The author did research for his Ph.D. to find out whether the police have complied with the requirements of Supreme Court concerning the rights of the arrested persons given in D.K.Basu V. State of West Bengal and chose the following requirements of Supreme Court:

- Not preparing the arrest memo immediately after the arrest.
- Denial of right to entitlement of having one of the relatives informed of the arrest.
- Failure to inform telegraphically to the next friend or relative of the arrested person who had committed the crime outside his native district.
- Denial of right to the arrested person to meet his / her lawyer for counseling.
- Denial of right to medical examination at the request of the arrested person by the police.
- Not issuing a copy of the medical memo to the arrested person.
- Not subjecting the arrested person to medical examination every 48 hours during his detention in police custody.

Description of the Tool

Two structured interview schedules, one to interview the arrested persons and the other to interview the relatives of the arrested persons who witnessed the violations of human rights by the police were framed.

Interview Schedule-I

The first interview schedule is the schedule for the arrested person. It has two parts:

- Part-I of the schedule contains 12 questions dealing with the personal data of the arrested person.
- Part-II of the schedule contains 52 questions with regard to treatment of the arrested person by the police from the time of picking up till either releasing the arrested person on bail from police station or till production before a magistrate.

Interview Schedule-II

As far as the interview schedule of the relatives of the arrested person is concerned, it has only one part, which consists of 25 questions. It is mainly to find out the veracity of the statement of the arrested person made during the interview regarding his or her human rights violations so as to ensure that there were no exaggerations by the arrested person. In addition, it is to find out violations of the human rights of the relatives interviewed and also that of other relatives, who were not interviewed.

Universe

The universe of the study are: 1] the arrested persons by the police of the chosen categories of offences against whom a criminal case is registered and 2] the adult relative of the arrested person, who had been an eye witness to the violation of the rights of the arrested person by the police.

Primary data

The primary data were collected from the arrested persons with the help of the interview schedule designed for this purpose. Not only the personal data particulars in the interview schedule I but also the interview schedule II concerning observance of human rights of the arrested persons were in local regional language, Tamil.

Secondary data

The statistics were collected from the respective district Crime Records Bureau. Since the sample size available in the chosen categories of

offences in two selected districts pertaining to one year was sufficient, it was decided to confine to the offences of the chosen categories registered for one year. The offences registered during the year 2000 was chosen for the present study instead of the offences of previous years for the simple reason that memory of common man, by and large is short and that forgetfulness should not come handy either for mitigating the offence or for exaggerating the incidence of violation by the police.

Size of the Sample

After carefully considering the statistics collected from the Crime Records Bureau, due to the availability of a larger sample in simple hurt, grievous hurt and in theft cases, the respondents of those three categories of offences were identified by stratified random sampling technique. As far as other categories of offences, the entire population was selected as the size of the sample was relatively small. In the case of the arrested persons, a sample size of 411was taken for the present study excluding those accused persons who were either undergoing imprisonment in jail or who had shifted their residence and gone away without even informing their present address not only to their neighbours but also to their nearest kith and kin and those who were not available due to other reasons. Among them, 191 were from metropolitan city and 220 from a moffusil district. For the purpose of the present study, the samples of the arrested person selected were categorized as under:

Table - 1: Sample Size In Various Categories of offences

Categories	Metropolitan City	Moffusil District
Property offences	46	24
Murder	15	34
Rape	11	12
Dowry death	15	18
Grievous Hurt	17	25
Simple Hurt	76	77
POA cases	Nil	15
Assault on Public Servants	11	15
TOTAL - 411	**191**	**220**

Statistical Analysis

The data collected were classified and subjected to statistical analysis on the basis of inferential analysis, Bi-variate analysis and Content analysis. These analyses were done in order to accept or reject the chosen hypotheses for the study.

Statistical Tools used for analyzing the results

- As in any social science research, content analysis has been performed using the percentages.
- In order to get more accurate conclusions on the hypotheses of the study, chi-square analysis has been performed as detailed below:

  With respect to the hypotheses to find out whether the police discriminate, it is assumed that human rights violations occur independent of the sub-categories of the particular variable viz. area.

5) The requirements of the Supreme Court as enumerated in D.K. Basu case and human rights violations – Frequencies and percentages

Table - 2

S. No.		No. of samples with violations	No. of samples without violation
1.	Not preparing Arrest Memo immediately	208 (50.60%)	203 (49.40%)
2.	Denial of right to entitlement of informing one of the relatives about the arrest	252 (61.31%)	159 (38.69%)
3.	Denial of right to counsel	157 (38.20%)	254 (61.80%)
4.	Not sending a telegram	39 (66.10%)	20 (33.90%)
5.	Denial of right to Med. Ex.	17 (60.72%)	11 (39.28%)
6.	Not getting signature in the medical memo for the injuries sustained	17 (60.72%)	11 (39.28%)
7.	Not issuing a copy of med. memo	25 (89.28%)	3 (10.72%)
8.	Med. Ex – 48 hrs	4 (40%)	6 (60%)
	Total	719 (51.88%)	667 (48.12%)

It is evident from the above table that violations were found to be the rule rather than an exception notwithstanding the stringent requirements. The high frequency of violations is a very serious matter and it reflects perhaps the lack of awareness of the victims and their relatives regarding the rights of the arrestee, the absence of any scientific study with regard to the extent and magnitude of violations, failure of human rights activists, continued lack of transparency in the police organization and above all the unwillingness of the police to change for the better.

Relationship between gender and human rights violations of the arrested persons due to non-compliance of the requirements of the Supreme Court as enumerated in D.K.Basu case

Table - 3

S. No.	Violations		Gender		x2 value & Significant level
1	Not preparing arrest memo immediately after effecting arrest	Gender	Arrested women Sample	Arrested men Sample	.16989 P>0.05
		With violations	15 (57.7%)	193 (50.12%)	
		Without violations	11 (42.3%)	192 (49.88%)	
2	DOR to entitlement of informing one of the relatives about the arrest	With violations	18 (69.2%)	234 (60.77%)	
		Without violations	8 (30.8%)	151 (39.23%)	
3	DOR to counsel	With violations	11 (42.3%)	146 (37.92%)	.65087 P< 0.01
		Without violations	15 (57.7%)	239 (62.08%)	

It is evident from the above table that there is a relationship between the gender and the denial of right to counsel while there is no relationship between the gender and non-preparation of the arrest memo immediately and the denial of right to entitlement of informing one of

the relatives about the arrest. Perhaps the awareness level of the arrested women regarding their right to counsel would have been lesser when compared to the awareness level of their male counterparts. However, more violations of the arrested women in relation to denial of right to counsel show the absence of sympathetic attitude of women police officers even towards the arrested women or their failure to influence men investigating police officers with whom they were attached for investigation purpose to be sympathetic towards the arrestee.

While there is a relationship between gender and use of force, and denial of right to counsel, there is no relationship between gender and not informing the grounds of arrest, denial of right to bail, not preparing the arrest memo immediately and denial of right to entitlement. Since in the majority of the cases there is no relationship between gender and human rights violations, the hypothesis that there will be no correlation between gender and human rights violations indulged in by the police is accepted.

Relationship between income level and human rights violations of the arrested persons due to non-compliance of the requirements of Supreme Court as enumerated in D.K.Basu Case

From the research, it is evident that there was no association between the income level of the arrested persons and all the human rights violations chosen for the research, except the parading of the arrestee in public as the value of $P > 0.05$. Hence the hypothesis that there will be no human rights violations of the arrested persons indulged in by the police based on the income level of the arrested persons is accepted. In spite of 51 per cent violations in this category, the only satisfying feature is that the police did not discriminate between the various income groups.

Relationship between income level and human rights violations of the arrested persons due to non-compliance of the requirements of Supreme Court as enumerated in D.K.Basu Case

It is evident from the research that human rights violations arising out of non-compliance of the requirements of the Supreme Court as enumerated in D.K. Basu case have no association with the educational level of the arrested as the value of $P > 0.05$.

Relationship between caste factor and human rights violations of the arrested persons due to non-compliance of the requirements of the Supreme Court as enumerated in D.K. Basu Case

Table – 4:

S. No.	Violations		Caste of the arrested person				x2 value & Significant level
1	Not preparing the arrest memo immediately	No. of Cases	SC & ST	MBC	BC	Others	4.69 P> 0.05
		With violations	77 (48.4%)	59 (48.4%)	66 (55%)	6 (60%)	
		Without violations	82 (51.6%)	63 (51.6%)	54 (45%)	4 (40%)	
2	DOR to entitlement of informing one of the relatives about the arrest	With violations	98 (61.63%)	67 (54.9%)	79 (65.8%)	8 (80%)	4.85 P> 0.05
		Without violations	61 (38.37%)	55 (45.1%)	41 (34.2%)	2 (20%)	
3	Denial of right to counsel	With violations	54 (33.5%)	44 (36.1%)	57 (47.5%)	2 (20%)	7.69 P> 0.05
		Without violations	105 (66.5%)	78 (63.9%)	63 (52.5%)	8 (80%)	
4	Not sending a telegram	With violations	17 (62.96%)	5 (55.56%)	14 (70%)	3 (100%)	17.84 P> 0.05
		Without violations	10 (37.04%)	4 (44.44%)	6 (30%)	NIL (0%)	
5	Denial of right to medical examination	With violations	6 (46.2%)	6 (75%)	4 (66.67%)	1 (100%)	2.58 P > 0.05
		Without violations	7 (53.8%)	2 (25%)	2 (33.33%)	NIL (0%)	
6	DOR to medical examina-tion every 48 hours	With violations	7 (53.8%)	1 (12.5%)	1 (16.7%)	1 (100%)	9.86 P> 0.05
		Without violations	6 (46.2%)	7 (87.5%)	5 (83.3%)	NIL (0%)	

It is evidently clear from a perusal of the above table that the caste of the arrested persons has no influence on the violations of their rights arising out of non-compliance of the requirements of the Supreme Court as enumerated in D.K. Basu Case. Nevertheless, the only satisfying outcome of the study is that the police did not discriminate the arrested persons based on their caste.

Relationship between Awareness Level of the Arrested Persons and Human Rights Violations

To find out the awareness level of the arrested persons, some specific questions were put forth while interviewing them and the results were computed and presented below.

Table - 5

Sl. No.	Awareness of the arrested persons relating to	Number of arrested persons who were aware	Number of arrested persons who were not aware (% in bracket)	x2 value & Significant level
1.	Preparation of the arrest memo immediately after the arrest	15	396 (96.35%)	355.04 P<.01
2.	Right to entitlement of informing one of the relatives about the arrest	36	375 (91.24%)	281.26 P<.01
3.	Right to be released in bail in bailable offences	90	321 (78.10%)	130.95 P<.01
4.	Right to counsel a lawyer of his choice by the arrested person	267	144 (35.04%)	36.21 P<.01

It is evident from the above table that lack of awareness of the arrested persons in relation to the rights conferred on them by the Constitution, law or the Supreme Court is highly significant. Unless the arrested persons are aware of their rights, the question of requesting the police to uphold their rights, if not demanding them does not arise. Perhaps the police capitalize on the lack of awareness of the arrested persons and violate their rights with impunity.

Summary

There were violations in all the chosen seven requirements of D.K. Basu case that were taken as dependent variables for the research.

Right to entitlement of informing one of the relatives about the arrest was found violated in 252 cases (61.3%); violation of this requirement was found very high in dowry death cases (84.84%) followed by simple hurt cases (69.04%) and the least violations of 20 per cent in Prevention of Atrocity cases.

Preparing arrest memo immediately was found not implemented in 208 cases (50.6%); it was to the extent of 72.7 per cent of dowry death cases; 57.5 per cent of simple hurt cases; 51.42 per cent of property cases with least violations of 11.5 per cent in assault on public servants.

Right to counsel was found violated in 157 cases (38.2%).

Right to medical examination was found denied in 17 out of 28 cases (60.7%)

Right to medical examination every 48 hours was found violated in 4 out of 10 police custody cases (40%).

The police failed in their duty in not sending a telegram to one of the relatives staying in a different district in 39 out of 59 cases (66%).

The total number of rights of 411 samples pertaining to DK Basu case is 1386 and number of violations was 719 (51.88%), which was higher than number without violations that stood at 667 (48.18%). Since the sample size is 411, for each case there was almost 2 violations (1.75 to be precise).

Conclusion

The purpose of the Supreme Court's pro-active judgment in DK Basu is to bring in transparency and accountability and on record it appeared to have been complied with to the extent of 100%. However, it is evident from scientific research that the very purpose of SC requirements has

been defeated not only by the police but also by the defense lawyers of victims of the entire sample of 411 cases. Unfortunately, not even a single case has been taken for contempt of Court against any one of the Investigating officers either by defense counsels or by any human rights activist NGO and consequently no erring police officer faced departmental disciplinary action. Furthermore, as per section 167 of the Code of Criminal Procedure, 1973 it is incumbent upon the magistrate to ask the accused person whether he has been informed of the grounds of his arrest (Vimal Kishore V. State 1956) and also about the treatment meted out to the arrestee. Owing to retro-active implementation by the stakeholders, the much celebrated pro-active judgment remains on paper only.

Indian Police Stations need an Overhaul: Veracity of the Statement

Shashank Pathak* & Dr. S. Karthikeyan**

Keywords

Police Station, Overhaul, Cyber Police Station, SHO.

Abstract

The Indian police are the manifestation of the responsibility of the state for maintaining peace and harmony for its subject in the society and therefore the question important for discussion is the proficiency and efficiency of this social institution. The problems like lack of women officers in the police stations, lack of IT facilities and infrastructure are the main reasons for the required revamp of the Indian police stations. This paper discusses these main issues and therefore reiterates the need of overhaul.

Few police stations are so drastic in condition that even the basic facilities of toilet and changing rooms for lady police officers are missing, even the police stations of the countries are facing the problem of not being considered to be trustworthy due to bad conduct of the police officers with people who visit police stations for filing complaint. They have to win the trust of the society as a institution which will solve their problems instead of treating them with ill behavior.

The police stations of India need overhaul so that they practice their work perfectly for which they are meant.

Introduction

THIS deep, sensational and fruitful thought that Indian Police Stations needs an Overhaul in the recent time, has always been a predicament for many contemplators and thereof it becomes a very interesting conundrum to be solved. This is a matter of a debate to clearly justify why and why not there is a need of Indian police stations to be renovated.

Author Intro:

* National Law University and Judicial Academy, Assam.

** Assistant Director, BPR&D, MHA, New Delhi-03.

Tracing back to the historical theory of social contract, the society is in a contract with the state for security and according to an interpretation state has taken the responsibility of its citizens and the manifestation of this promise is the police force. Police is an instrument of social security. It can be remarked again and again that the human race gradually realized the importance of the police with time.

Change is required when it is vindicated that the work which is assigned or expected from an institution, is not doing it properly or is insipid in its approach. The question of 'need of change' then comes up in the minds of many but mostly and ironically only after witnessing instances by which they are shocked. Reasons can be due to irresponsible actions from the bodies which are expected to work reliably. This makes them accept that overhaul is the only alternative left to resort to perfection. To understand this, there are many occasion where innocuous people have to suffer the evils of the unorganized, unsystematic and rude Indian police stations. The human rights activists are the biggest adherent to recite these instances where Indian police station is proved to be the places of devils rather than rescuer or savior.[1]

This question may be retorted by saying that it is not possible for the police stations in the developing nations like India to work with same gravity like the police stations of developed nations, due to lack of structural development and training facilities. This implies that it requires us to swiftly bring the overhaul in the Indian police stations for extracting the full use of them for which they are instituted. The Indian police stations certainly need overhaul, and this is reiterated whenever improvement in criminal justice system is demanded, demanders came and gone but the idea remained alive.

Here are few points of discussion which provides the edifice of the requirement of revamp in police stations of India.

Need for Women Officers in Police Station: An Inevitable Step required in Indian Police Stations

This is one of the points of consideration which explains that why overhaul is needed in the Indian police stations.

Imagining a situation where a complainant is a women in the police station. For a typical women of Indian society, it seems to be a very

1 India: Overhaul Abusive, Failing Police System, The Human Rights Watch, http://www.hrw.org/news/2009/07/29/india-overhaul-abusive-failing-police-system, Last visited 0n October 30, 2014.

difficult task for her to lodge complaint which is of a nature of sexual harassment or an act of such similar nature, by explaining it properly to the male police officers. Rather a proper number of women police officers should be put in police stations.

Besides cases of rape and molestation, male police officers also find it difficult to handle violent protests and processions in which women are used as shields. Any action against such violence gets branded as atrocities against women.[2]

Police is primarily a responsibility of the state government according to Constitution and so an overall evaluation can be traced based upon different police stations of different states. Every state has different scenario and our endeavor is to bring out instances which are provocative enough to explain overhaul from anywhere in India, whereas in case of national capital, Delhi the scenario is very pathetic. With sudden spurt in the crimes against women the demand for more sensitivity in hearing women's grievances has increased. Despite an urgent need of women-centric policing in the city, the number of women in Delhi Police is woefully low just 7 per cent of the Delhi Police strength. What's worse is that they are usually given routine and inconsequential posts and are rarely seen patrolling the city streets. Each year, the percentage of women officer drops, admit Delhi Police officials. Shockingly, of the 161 district police stations in Delhi, only one (Maurice Nagar in north campus) has a woman station house officer (SHO).[3] These figures are relevant to portray the exact condition of police stations of the national capital which any day are believed and expected to have good proportion and perfect establishment but same is not the case. There are 4,809 women officers of various ranks, ranging from constables to inspectors. Delhi Police statistics reveal that there are 72 women inspectors - the rank at which they are made SHOs - but there are hardly a handful of such cops posted as SHOs, and that too at places like the Crime against Women cell, Rithala metro station and New Delhi railway station.[4]Now when the big question of ability comes into picture and as far as the training of

2 TNN, Kolkata police set to recruit more women personnel, The Times of India, http://articles.timesofindia.indiatimes.com/2012-08-06/kolkata/33064510_1_police-stations-police-officer-women-officers, last visited on February 24, 2013.

3 Indrani Basu, Women officers rare in Delhi Police, The Times of India- Delhi, http://articles.timesofindia.indiatimes.com/2012-12-20/delhi/35932757_1_women-officers-police-stations-women-constables, last visited on February 27, 2013.

4 Ibid.

these women officers is concerned then again it can be seen that it needs a tremendous positive efforts and approach towards achieving it, otherwise the little we have will be of no use and may be equal to nil. A constant effort to increase and uplift the figures of proportion of women officials should be continued in police stations for betterment of women victims of crime.

The degree of need of such change is also noticeable from the statements of a former Union Home Minister of India, who said that he had told the police to post at least one woman officer in each of the capital's 166 stations. Delhi Police would launch a special drive to recruit women personnel in order to make city police stations more women-friendly.[5] When it comes to the collections of evidences, then again it is reiterated that in rape cases the victim should be handled by the women officer and so the department will send 80 to 90 men and women cops for 'advanced training' on investigation of rape cases, handling a woman victim, following guidelines and collecting evidence in such cases.[6]The revamp of police stations has to be done from such measures and such propositions show us the desperate need of overhaul.

Moving away from the case of Delhi, the same endeavour for overhaul can be traced in the Karnataka too. The Karnataka government also looks interested in bringing measures to ensure safety of women by bringing changes in the police stations. This includes deploying at least five women police personnel at every police station and disposing of complaints related to women within a month.[7]

So these are the concrete steps, showing that the required change in the police stations is also felt by the state and it is trying to do every bit of those endeavors to protect the rights of its citizens by changing the unacceptable conditions of police stations.

5 Bharti Jain & Neeraj Chauhan, All Delhi police stations to have women officers: Shinde, The Times of India, http://articles.timesofindia.indiatimes.com/2012-12-29/delhi/36050564_1_women-police-police-stations-women-officers, last visited on February 24, 2013.

6 Ibid.

7 TNN, Police stations to have 5 women staffers each , The Times of India, http://articles.timesofindia.indiatimes.com/2012-12-25/bangalore/35998652_1_police-station-police-officers-police-personnel, last visited on February 24, 2013.

Need of Cyber Crime Police Stations: India Ranks fifth in Cyber Crime Affected Countries[8]

Even we have cyber crime stations but the truth is that it's not adequate. To counter crime at best in the era of information and technology requires the establishment of cyber police stations, and to make India a place of peace and harmony this will play an important role in this regard. The need of overhaul here is a necessary condition and thus requires a great attention from the side of policy makers. The process of cyber station in India is being undertaken but it requires a fast establishment. Consideration in this aspect needs a real attention of the state government.

This can turn out to be boon for country like India, as India is a country which ranks fifth in the cyber crime affected countries, claims a report by the Security and Defence Agenda (SDA) and McAfee.[9] India is much vulnerable because of the widespread computer illiteracy and easily pirated machines and same becomes the reason of a necessary change in the police stations; installation of information and technology and training of police officers is hence a requirement for the revolution of overhaul and therefore Indian police stations need this refurbish.

The need of Specialization in Information and Technology (IT) to Prepare Police Stations to Counter Crime in the Changing World of Technology

An institute which does not change with changing patterns of society has to face problems of capable and proper working. The analogy that IT development in the world is increasing at a high speed and therefore to counter the prevailing cyber crimes installation of high level technology is suggested, because in case of India technology is used but it has to cover a lot to bring cent percent success rate in their accomplishments.

In the era of globalization, the problems of crime in India has gone in more wider dimensions and so it is important to make efforts which make Indian police stations ready for any sort of problem, and more accurate and efficient in their working.

8 SheetalSukhija, India 5th among cyber crime affected countries, ibnlive.in.com, http://ibnlive.in.com/news/india-5th-among-cyber-crime-affected-countries/255393-60-115.html, last visited on March 3, 2013.

9 Ibid.

Either there is no computer in a police station or there is no expert who can properly make use of it in the clerical work. The information and technology which is used in the police stations is for the fact of proper and proficient working but providing with the tools and not providing proper training may be a waste of resources.

The documents of the police stations should also be properly made so that the authentic information can be derived from the documents.

The process of technical establishment of the neo-ICT i.e. information, communication and technology has started in India and this gives the evidence that overhaul was required to be brought in. Since there is a need of overhaul of police stations and so we see that the state governments in India have come up with the implementations of Crime and Criminal Information System (CCIS) and CIPA. As there was need of change felt by the government of different state, we witnessed these recommendations and so is the result there have been many attempts which CCIS or the crime and criminal information system, which is established in the departments. This project is aimed at building in a planned manner infrastructure and mechanism to provide the basis for evolution for CCIS which is uniform across the country from police station level onwards. CIPA was developed for planned induction of Information Technology towards better management of public order and criminal activities.[10]This is just the initial step towards the positive changes and more is required and continuous policies are demanded.

Urgent need for Infrastructure of Sufficient Level

The criticism that police stations of India are having bad infrastructure is not a hidden phenomenon and this has sort of created unavoidable ineffectiveness and inefficient working of police. Police stations are the social infrastructures of the society and hence the way for smooth running of the society can be quenched from perfect infrastructure of police stations.

The official files in the police station are also not kept in systematic manner in few examples and this should be taken care of in a more systematic manner, because this will add to the proficiency of working.

10 Manish Gupta, B. Chandra and M. P. Gupta, Crime Data Mining for Indian Police Information System, computer society of India, http://www.csi-sigegov.org/1/40_410.pdf, last visited on March 26, 2013.

This is a serious issue and in the illustration, where the Commissioner of Police, Mumbai, when visited to police stations across the city has himself revealed that apart from five police stations slated for relocation, there are several other facing similar problems of poor infrastructure. He saw for himself the poor condition of more than 10 police stations. Apart from dilapidated buildings, there were many other problems that the officers faced. He prepared a list of these police stations that he would follow up on after the five police stations.[11] According to him, when he visited the V.B. Nagar police station once, he saw that it was located in two rooms with no place for women officers to change clothes. He said it was not just the state of the buildings and hygiene that raised concern, but space in the existing police stations was also inadequate for police officers to function.[12]

"For example, according to the law when a woman arrives at a police station with a problem, a lady police officer should take her to a private room. But there are many police stations that do not have space for women counselling," the Commissioner said.[13]

Anyone who has an experience of visiting police stations in India can concur with the fact that even the basic infrastructure in the Indian police stations is hopeless, except for leaving one or two examples of police stations which have good infrastructure, but most of them do not comply with this fact. To prove these facts a real illustration can be given where a women officer confesses that traditionally, some necessary infrastructure is missing. Women personnel find it difficult to get separate toilet or changing rooms in police stations. These problems need to be addressed immediately, said a lady officer.[14]

If infrastructure can be improved it, can add on to the glory of Indian police stations.

Conclusion: How and What to Revamp

For getting positive results, one should always be systematic and so should be the police stations in such a vast country, India. The control

11 Meghasood, Police stations need revamp: Dayal after night patrol, The Indian express, http://www.indianexpress.com/news/police-stations-need-revamp-dayal-after-night-patrol/755084, last visited on February 27, 2013.

12 Ibid.

13 Ibid.

14 TNN, Kolkata police set to recruit more women personnel, The times of India, http://articles.timesofindia.indiatimes.com/2012-08-06/kolkata/33064510_1_police-stations-police-officer-women-officers, last visited March 2, 2013.

of crime, delinquency and attainment of harmonious society can be achieved through the positive renovation of the police stations. The behavior of the police officers and the condition of the police station, when improves, it will surely improve the society with it.

The steps like having women police officers in the police station for comfort of women victims who come to complain, improving the infrastructure, training the police officers to converse properly with victims and improving the clerical work can help a lot in establishing police stations as a temple of social control. Steps like e-governance will provide a more strengthened edifice to the police stations. According to a report by The Pioneer, the integrated system will help with the efficiency and effectiveness of policing at the police station level through adoption of e-governance and creation of a nationwide networked infrastructure for evolution of IT-enabled tracking system around "investigation of crime and detection of criminals."[15]

Doing a work of merit will always gather appreciation and laurels; overhaul will make police stations more trustworthy and eventually make this world a safer place to live.

15 News desk, New crime tracking system to connect 14,000 police stations in India, cxotoday.com, http://www.cxotoday.com/story/new-crime-tracking-system-to-connect-14000-police-stations-in-india/, published on Jan 04, 2013, last visited on March 3, 2013

Digital Forensic and Cloud Computing

Sandeep Kumar Pathak* , Sarvesh Kumar Pathak and A.K. Gupta***

Keywords

Cloud Computing, Digital Forensic Investigation for Cloud Computing, LEAs.

Abstract

In computer networking, cloud computing is the computer network that have a large number of computers connected to communicable media/ communication network such as Internet, having the ability to run a program/application on many connected computers at the same time; therefore, cloud computing also known as distributed computing over a network. Increasing interest as well as use of cloud computing increases the opportunities for criminal exploitation and challenges for LEAs (Law Enforcement Agencies), especially with respect to data protection policies. Therefore, present work demonstrates to identify the required challenge to current forensic investigation needed to successfully conduct cloud computing investigation, and propose an integrated concept, which emphasizes the preservation of forensic data collection of cloud computing data for forensic purpose.

Introduction

CLOUD computing is the computer network that have a large number of computers connected to communicable media/ communication network such as Internet, having the ability to run a program/application on many connected computers at the same time. Therefore, cloud computing is also known as distributed computing over a network. Cloud computing generally refers to

Author Intro:

* Department of Forensic Science, SHIATS Allahabad, UP, India.
E-mail: sandeeppathak003@gmail.com

** Department of CBBI, JSBB, SHIATS Allahabad, UP, India.

incorporative software as services (that provides useful applications online and accessed from a web browser; where the software and data are stored on the servers), platform as a services and infrastructure as services. For instance, Webmail such as Microsoft's Windows Live Hotmail, Gmail. Rediffmail, Yahoo mail, Facebook, Twitter, Apple's MobileMe calendar, and Amazon's S3 storage service (which numerous other Web applications rely on to hold their data) are examples of cloud computing.

Cloud computing is having the both applications to be delivered as services over the Internet as well as hardware and systems software in the data centers that provide those services. The datacenter hardware and software is known as "Cloud"[1]. Cloud computer is non-commercial as well as commercial[2] also because:

Large amount of data: In 21th century advancement in the analytical method lead to huge amount of data generated every day from field of education and researches. With the aid of cloud computing these large amounts of data are collected and maintained in usable form by help of various software[3]. Collection and storage of these data further help in research e.g. NCBI for retrieval of biological database.

Advance technology support and cost: Development of online security with simple and secure mode of transition of money/payment mode, increase the interest in Internet. Simple payment mode with time saving, protection against robbery of money and reducing the problem during payment, these are the features of cloud computing. Advance technology increases the interest in Internet with speed accompanying in introduction of 2G and 3G services, these are also the features of cloud computing[3].

Miniaturization technologies continuously help in reduction of overall cost of cloud computing as compared to earlier technologies such as grid computing, distributed system, and utility computing[3].

Model of cloud computing/service model of cloud computing

The service provided under the cloud computing can be categorised in the following three major groups-

1. Software as a Service (SaaS)[3,4],
2. Platform as a Service (PaaS)[3,4] and
3. Infrastructure as a Service (Iaas)[3,4].

In SaaS software having the complete application is served on demand to the clients. In this model software providers provide a software application to be used and purchased on demand, and applications can be accessed through network from various clients such as web browser and mobile phone etc, by application user. The application requires no client installation; only use the browser or other client device with network connectivity[4]. The service model for SaaS is tabulated in figure1 and examples are tabulated in table1.

Figure 1. Service model for SaaS

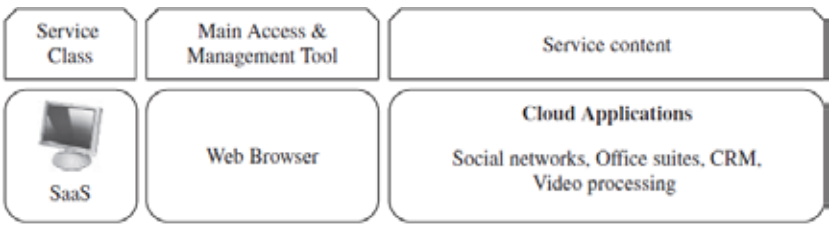


Table 1. Example of SaaS

Service class	Management tool	Uses	Pricing model
Google Gmail	Web Browser	E. mail	Free
Facebook	Web Browser	Social network	Free
Twitter	Web Browser	Social network	Free
Salesforce.com	Web Browser	CRM*	Pay per use
Process Maker Live	Web Browser	BPM**	Pay per use
Appian Anywhere	Web Browser	BPM**	Pay per use
Box.net	Web Browser	Storage	Pay per use
XDrive	Web Browser	Storage	Subscription
SmugMug	Web Browser	Data sharing	Subscription
OpSource	Web Browser	Billing	Subscription

*CRM- Customer relationship management

**BPM- Business process management

In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications[5]. PaaS provide the environment where user can create and deploy application. In PaaS user do not necessarily need to know about how

much memory and how many processor and their applications are evolved in processing[6]. PaaS provide the platform to user foe used to a complete software development, life cycle management, database management, and design to building applications to development to testing to maintenance[7].

PaaS provide the working platform which acts as a service by encapsulating the required software and working environment to the provider, then this platform is used by client[3]. PaaS can be classified by the availability of features such as programming models, programming languages, frameworks and persistence options, that influence the application development[4]. The service model for PaaS is tabulated in figure 2 and examples are tabulated in table 2.

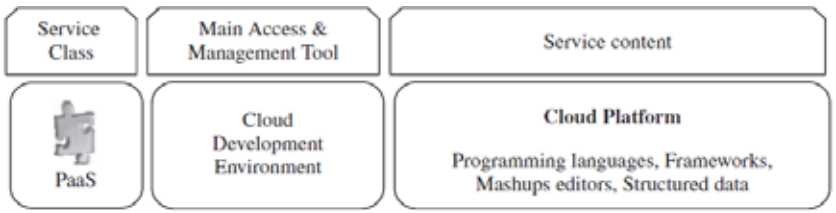


Figure 2. Service model for PaaS

The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications[3]. There are following characteristics and component included in IaaS:

- Utility computing service and billing model[8].
- Automation of administrative tasks[8].
- Dynamic scaling[8].
- Desktop virtualization[8].
- Policy-based services[8] and
- Internet connective[8].

In IaaS, the user directly uses infrastructure component such as storage, firewalls, networks, and other computing resources, provided by the cloud provider. Virtualization is widely used in IaaS[6]. Virtualization is resource of one physical computer which can be portioned in to logical resources and rearrangement in to multiple virtual machines[9].

The service model for IaaS is tabulated in figure 3 and example of a hardware virtualized server hosting three virtual machines, each one running different operating system and user level software are tabulated in figure 4. The example of service provider for IaaS is tabulated in table 3.

Table 2: Examples of PaaS providers (Reference 4)

Provider	Management tool	Uses	Programming language	Persistence option
Aneka	NET enterprise applications, Web applications	Flat files, RDBMS	.NET	Flat files, RDBMS
AppEngine	Web applications	BigTable	Python, Java	BigTable
Force.com	Enterprise applications	Own object database	Apex	Own object database
Azure	Enterprise applications, Web applications	Table/BLOB/ queue storage, SQL Services	.NET	Table/BLOB/ queue storage, SQL Services
Heroku	Web applications	PostgreSQL, Amazon RDS	Ruby on Rails	PostgreSQL, Amazon RDS
Amazon Elastic MapReduce	Data processing	Amazon S3	Hive and Pirg, Cascading, Java, Ruby, Perl, Python, PHP, C++	Amazon S3

Figure 3: Service model for IaaS

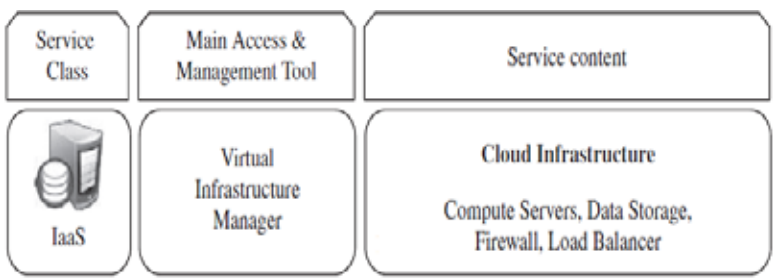


Figure 4. Virtualization (Reference 4)

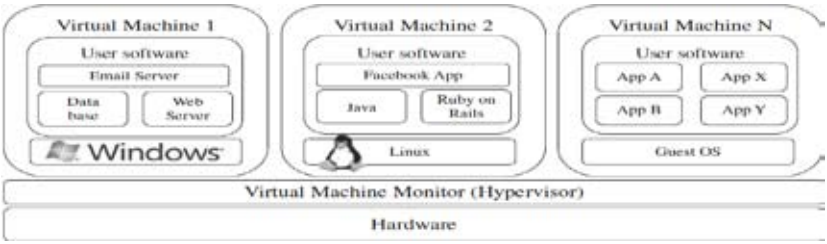


Table 3: Example of service provider for IaaS (Reference 4).

Provider	User interfaces and APIs	Hardware capacity	Guest operating systems
Amazon E2C	CLI, WS, Portal	CPU: 1_20 EC2 compute units Memory: 1.7-15 GB Storage: 160-1690 GB, 1GB-1TB (per ESB units)	Linux Windows
Flexiscale	Web console	CPU: 1-4, Memory: 0.5-16 GB Storage: 20-270 GB	Linux, Windows
GoGrid	REST, Java, PHP, Python, Ruby	CPU: 1-4, Memory: 0.5-16 GB Storage: 20-270 GB	Linux, Windows
Joyent	---	CPU: 1-6, Memory: 0.5-8 GB Storage: 30-480 GB	OpenSolaris
RackSpace	Portal, REST, Python, PHP, Java, .NET	CPU: 1-6, Memory: 0.5-8 GB Storage: 10-620 GB	Linux

Types of cloud computing

Based on the availability of the cloud and its components to the clients using this service, these are of following three types[10,11].

- Public clouds
- Private clouds and
- Hybrid clouds

Public clouds are owned and operated by third parties and available publicly with some constraint of security and data variance[11]. While

private clouds are clouds that are owned and operated by an enterprise solely for its own use[3]. Hybrid clouds are mixture of public and private cloud, and the some parts of services are publicly available whereas some are private and can be accessed only by organization and its permission[11].

Digital Forensic

Digital forensics or computer forensics is the path of the overall forensic science consisting of preparation, acquisition, preservation, examination, analysis and reporting of digital data, and main purpose is to recover and obtain legal evidence found in digital media and/or computers[12]. According to the National Institute of Standards and Technology (NIST), digital forensics is the scientific procedures used to recognize and classify, collect, evaluate, and analyze the data while maintaining the level of integrity of the information throughout the forensics process[13].

Digital forensic provides digital evidence of specific or general activities[14] such as:

- Child pornography
- Industrial espionage
- Criminal fraud and deception cases
- Unauthorized access to and/or
- Cyber warfare attacks

Computers can be used for virtually any type of pornography, identity theft and espionage. It is the job of computer forensics professionals to use technology to catch and stop these criminals. To do so effectively, however, requires periodic updates to stay current with the latest technology and trends in computer investigation[14]. Digital Forensic involves:

Computer Forensic: The fundamental factor of computer forensic is to retrieve data along with guideline and procedure to create legal audit. This audit needs to be presentable in court and to be effectively acceptable[15].

Intrusion Forensic: The functionality intrusion forensic refers to the detection of the intrusion attack or any suspicious attack of any sort of malicious user. It even involves any suspected attack against the system[15].

Network Forensic: The fundamental work of intrusion forensic is to refer any natural source evidence towards crime & criminals through which the crime can be investigated further. It involves keeping track of network accessing factor. In this context; network along with intrusion forensic will tackle the issue of network forensic[15].

Mobile Forensic: It refers to the crime that is being conducted through mobile phones as their medium. As the users of mobile phones are maximum in today's era therefore, maximum crime are being conducted through it only[15].

Cloud Forensic

Cloud forensic is the sub part of Network Forensic within Digital Forensic. It means cloud forensic is a part of both Network Forensic as well as Digital Forensic, that means the investigation about the attacks taking place through digital medium in the cloud world[15]. It is the sub part of Network Forensic helping in all crime investigation carried over Network Layer.

Crime and Security Risks involving in Cloud Service Providers

Authentication Issues

Authentication issues in cloud computing is access, the unauthorized access to cloud computing systems may occur when a username and password has been unauthorized/obtained without authorization. This can occur using the various technical and non technical methods, for example in social engineering the password may also be guessed or obtained using keylogging malware or cracked using brute force or weak password recovery mechanisms or by provider when claiming that urgent access is required but the password is not working and needs to be reset[16].

DoS Attacks

Cloud services are becoming increasingly popular these days, both among the public and business enterprises. While convenient, Cloud services can be extremely vulnerable to Denial of Service attacks (DoS). Denial of service (DoS) attacks against cloud service providers may leave tenants without access to their accounts[16]. This can occur by sending a flood of traffic to overwhelm websites to make them inaccessible to

legitimate users. The eighth annual Worldwide Infrastructure Security Report indicated that 94% of data center operators reported security attacks, 76% had suffered distributed denial of service (DDoS) attacks towards their customers; while just under half (43%) had partial or total infrastructure outages due to DDoS and yet only 14% of respondents had seen attacks targeting any form of cloud service. In the past, many websites like eBay, CNN, and Yahoo have become victims of DoS attack[17].

Use of Cloud Computing for Criminal Activities

Cloud computing accounts can be created or existing accounts compromised for criminal purposes. New cloud computing accounts may be created with stolen credentials and credit card details, thereby reducing the cost to the offender(s), as well as anonymising the offender and creating further difficulties in tracking down the source of the attack, particularly when jurisdictions are crossed[16].

Attacks on Physical Security

Cloud service providers' data centre may also be physically attacked, resulting in hardware theft, unauthorised access to servers or loss of access to data.

Malware

Malware also known as malicious software refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information and Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers[18].

SQL Injection

SQL (Structured Query Language) is a computer language aimed to store, manipulate, and query data stored in relational databases. SQL injection attacks can result in data being accessed and modified without authorisation[19]. Another injection attack is OS injection or command injection, whereby the input contains commands that are erroneously executed by the operating system.

DNS Attacks

A Domain Name Server (DNS) amplification attack is a popular form of distributed denial of service (DDoS) that relies on the use of publically accessible open DNS servers to overwhelm a victim system with DNS response traffic[20]. DNS attacks are aimed at obtaining authentication credentials from Internet users, including cloud service tenants.

Network / Packet Sniffing

Network or packet sniffing involves the interception and monitoring of network traffic. Data that are being transmitted across a network, such as passwords, can therefore be captured and read if not adequately encrypted. In the cloud environment, this is particularly important as passwords play a critical role in establishing access to the provider's services

Detection of Crime in Cloud Environment

There are following tools and technique which are used in detection of crime in cloud environment.

FRED (Forensic Recovery of Evidence Device) System

FRED systems are optimized for stationary laboratory acquisition and analysis. Simply remove the hard drive(s) from the suspect system and plug them into FRED and acquire the digital evidence. FRED will acquire data directly from IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/USB hard drives and storage devices and save forensic images to Blu-Ray, DVD, CD or hard drives. FRED systems also acquire data from Blu-Ray, CD-ROM, DVD-ROM, Compact Flash, Micro Drives, Smart Media, Memory Stick, Memory Stick Pro, xD Cards, Secure Digital Media and Multimedia Cards. Furthermore, with the optional tape drive FRED is capable of archiving to or acquiring evidence from DLT-V4 tapes. All FRED systems include the UltraBay, front panel connections, and removable drive trays so there is no need to open up the processing system to install drives or crawl around the back of the unit to attach devices[21].

Forensic Network

Forensic Network is a series of processing and imaging computers connected and integrated directly with a high speed, high-capacity server to share resources. The file server operates as the core of the

Forensic Network and can be used as a central storage facility for Forensic Images as well as applications software for use by the client processing and imaging stations. Workstation clients on the network perform the actual imaging and processing tasks, while the central file server stores the images and case work[15].

Forensic Write Blockers

Digital Intelligence designs offer parallel IDE, serial ATA and SCSI hardware write blockers, as well as other custom solutions, to effectively address specific write blocking requirements[15].

Forensic Devices

FANNIE (Forensic Area Network Numerous Imaging Enclosure)

Each FANNIE contains eight imaging bays which are directly accessible via the Ethernet network. Each imaging bay is capable of supporting both SATA and IDE hard drives. Each imaging bay has its own dedicated Gigabit Ethernet port for communication directly with a Gigabit switch. These bays are shareable between all workstations on the Forensic Area Network

The FANNIE imaging enclosure operates over pure AOE (ATAPI over Ethernet) Ethernet Protocols. As such, no high level protocols (TCP/IP, IPX/SPX, NETBEUI, etc) need to be associated with the NIC attached to the acquisition network. The workstations selectively attach and acquire from the imaging bays using only extremely efficient Ethernet protocols. Workstations with high quality NIC's can expect to achieve image acquisition speeds of 2 GB/Min and higher[22].

Rack-A-TACC 2U Module

The Rack-A-TACC is a modular building block for decryption. Running the Access Data Password Recovery Toolkit (PRTK) or Distributed Network Attack (DNA) a single Rack-A-TACC can provide 24x to 180x performance gain over a standalone quad core computer system[23].

ElcomSoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery employs a revolutionary, patent pending technology to accelerate password recovery when a compatible NVidia graphics card is present in addition to the CPU-only mode. The acceleration technology offloads parts of computational-heavy processing onto the fast and highly scalable processors featured

in the NVidia's latest graphic accelerators. Additionally, EDPR also operates in a distributed environment where multiple workstations can work together to distribute the workload of a single task[24].

It breaks complex passwords, recovering strong encryption keys and unlocking the documents in a production environment. Elcomsoft distributed password recovery is a high-end solution for forensic and government agencies, data recovery and password recovery services and corporate users with multiple networked workstations connected over a LAN or the Internet. Featuring unique acceleration technologies and providing linear scalability with no overhead, Elcomsoft distributed password recovery offers the fastest password recovery by a huge margin, and is the most technologically advanced password recovery product currently available[24].

Forensic Duplicators

Tableau forensic duplicators offer hard drive imaging with no compromises. In addition to being fast and reliable, duplicators are easy to use, yet still come packed with useful features for the advanced user[25].

HardCopy 3P - 1:2 Forensic Hard Drive Duplicator

It is potable forensic hard drive duplicator and disk imaging for user needs[26]

Shadow 2

The Shadow 2 is a patented computer hardware device that is designed to aid the investigation of a computer's hard drive. It provides investigators with read write access from the host computer's perspective, while maintaining the original hard drive unchanged[27].

Softwares and Tools

Digital Intelligence Software

Digital Intelligence has created several forensic software tools in-house specifically for forensic use[28]. These tools include-

PDWipe CE: PDWIPE (Physical Drive WIPE) is a standalone utility to wipe entire physical hard drives. PDWipe is based on the wiping technology found in DRIVESPY. PDWIPE is capable of wiping large hard drives at amazing speeds.

PDWipe LE: PDWIPE (Physical Drive WIPE) is a standalone utility to wipe entire physical hard drives. PDWipe is based on the wiping technology found in DRIVESPY. PDWIPE is capable of wiping large hard drives (in excess of 8.4Gb) at amazing speeds.

PDBlock LE: PDBlock is a write blocker which not only provides customary write protection from older Interrupt 13 disk access methods, but also provides protection from the newer Interrupt 13 Extensions associated with Large Hard Drives.

PDBlock CE: PDBlock is a write blocker which not only provides customary write protection from older Interrupt 13 disk access methods, but also provides protection from the newer Interrupt 13 Extensions associated with Large Hard Drives.

Image LE: Image Law Enforcement Edition. IMAGE is a standalone DOS utility to generate physical images of floppy disks. The program is capable of generating highly compressed or "flat" images for forensic analysis.

Image CE: Image Commercial Edition. IMAGE is a standalone DOS utility to generate physical images of floppy disks. The program is capable of generating highly compressed or "flat" images for forensic analysis

DriveSpy LE: DRIVESPY is a DOS application designed to emulate and extend the capabilities of DOS to meet forensic needs

DriveSpy CE: DRIVESPY is DOS application designed to emulate and extend the capabilities of DOS to meet forensic needs.

Access Data

AccessData has been a leader in password recovery and applied cryptography. The forensic tools available are Ultimate Toolkit, Forensic Toolkit, Password Recovery Toolkit and Registry Viewer[15].

Guidance Software

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. EnCase® Enterprise platform is used by numerous government agencies, more than 65 percent of the Fortune 100, and more than 40 percent of the Fortune 500, to conduct digital investigations of servers, laptops, desktops and mobile devices[29].

Paraben Forensic Tools

Paraben has forensic software for PDAs, password recovery, text searching, data acquisition, e-mail examination and more[15].

Hot Pepper Technology

Hot Pepper Technology, Inc. provides custom applications for clients throughout the world. HPT is a software development and consulting firm targeting the Microsoft Windows Platform and products cover Telephony, Communications, Pagers, Software Simulations, and Computer Forensics[29].

StepanetDataLifter

Stepanet'sDataLifter is a suite of products built on years of investigative experience. These tools have been specifically designed to assist with Computer Forensics, Information Auditing, Information Security and Data Recovery[15].

Security and Privacy Issues in Cloud Computing

There are following security issues and privacy are required for cloud computing.

- Infrastructure Security
- Network Level
- Host Level
- Application Level
- Data Security and Storage
- Identity and Access Management (IAM)
- Privacy

Network level security

Network security measures control access to operating system and other network systems. When the network is connected to the Internet, there is a need to ensure that adequate network level security measures is in place to protect the internal network resources from unauthorized access and intrusion. A firewall is the most common means for providing network security. Internet service provider (ISP) can provide an important element in network security plan. Network security scheme needs to outline what security measures ISP provides, such as filtering rules for the ISP router connection and public Domain Name System (DNS) precautions[30].

Host Level Security

Host level security measures protect data communications within and across networks. When one communicates across an untrusted network like the Internet, user cannot control the traffic flows from source to destination. The user traffic and the data it carries flows through a number of different systems that user cannot control. Unless you set up security measures, such as configuring your applications to use the Secure Sockets Layer (SSL), your routed data is available for anyone to view and use. Transmission level security measures protect your data as it flows between the other security level boundaries[30].

Application Level Security

Application level security measures control how users can interact with specific applications such as DoS, EDoS etc. These applications and services are vulnerable to the misuse by unauthorized users looking for a way to gain access to your network systems. The security measures that you decide to use need to include both server-side and client-side security exposures[30].

Conclusion

Forensic research is a tough task in cloud computing environments. It is always possible to acquire data from unconventionally installed operating systems after their use, but the amount of data which can be recovered varies. Examining operating systems on external drives can yield the same data as a normal operating system, but it is essential to find the device on which the operating system is stored. Recovering data from operating systems on removable media is very problematic because it is time sensitive. The best methodology to handle such scenarios with the rare unconventional installed operating systems is not to be dependent solely on the information retrieved through the host machine.

Acknowledgements

Authors express to acknowledgements to Department of Forensic Science and Department of Computational Biology & Bioinformatics, SHIATS, Allahabad, Uttar Pradesh, India.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H. et al. Above the clouds: A berkeley view of cloud computing. Electrical Engineering and Computer Sciences University of California at Berkeley. 1-25 (2009).

2. Qiu, J., Ekanayake, J., Gunarathne, T., Choi, J.Y., Bae S.H. & Li, H. et al. Hybrid cloud and cluster computing paradigms for life science applications. BMC Bioinformatics 11(S-3):1-6 (2010).

3. Thakur, R.S., Bandopadhyay, R., Chaudhary, B. & Chatterjee, S. Now and next-generation sequencing techniques: future of sequence analysis using cloud computing. Frontiers in genetics- Genomic assay technology. 3(280):1-8 (2012).

4. Buyya, R., Broberg, J. & Goscinski, A. Cloud computing principles and paradigms. John Wiley & Sons, Inc., Publication USA. 10-36 (2011).

5. Introduction to cloud computing. http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf. 18/03/2014.

6. Mell. P. & Grance. T. The NIST definition of cloud computing. NIST special publication 800-145. 1-5 (2011).

7. Subashini, S. & Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 34(1):1-11(2011).

8. Arora, P., Wadhawan, R.C. & Ahuja, S. P. Cloud Computing Security Issues in Infrastructure as a Service. International journal of advanced research in computer science and software engineering. 2(1):1-7 (2012).

9. Hugos, M. & Hulitzky, D. Business in the Cloud: What Every Business Needs to Know About Cloud Computing. John Wiley & Sons, Inc. Publication USA. 9-22 (2010).

10. Rao, S., & Rao, V.N. Cloud computing: an overview. J TheorAppl Info Technol. 9:71-76 (2009).

11. Thakur, R.S. & Bandopadhyay, R. Role of cloud computing in bioinformatics research for handling the huge biological data. Biology of useful plants and microbes. Narosa publishing house, New Delhi, India. 321-329 (2014).

12. Sharma, H., Sabharwal, N. Investigating the Implications of Virtual Forensics. International conference on advance in engineering, science and management (ICAESM-2012). 617-620 (2012).

13. Daryabar, F., Dehghantanha, A., Udzir, N. I., Sani,N. F. B. M., Shamsuddin, S. B. &Norouzizadeh, F. A survey about impacts of cloud computing on digital forensics. IJCSDF 2(2): 77-94 (2013).

14. Slusky, L., Partow-Navid, P. &Doshi, M. Cloud computing and computer forensics for business applications. Journal of Technology Research. 3:1-10 (2012).

15. Saxena, A., Shrivastava, G., Sharma, K. Forensic investigation in cloud computing environment. The International Journal of forensic computer science. 2:64-74 (2012).

16. Hutchings, A., Smith, R. G. & James, L. Cloud computing for small business: Criminal and security threats and prevention measures. Trends & issues in crime and criminal justice. 456: 1-8 (2013).
17. Kalyani, M. Cloud Computing and Denial of Service Attacks: Examining the Vulnerability of NTP Servers. https://spideroak.com/privacypost/cloud-security/cloud-computing-and-denial-of-service-attacks-examining-vulnerability-of-ntp-servers/. 10/03/2014.
18. Malware. http://www.techterms.com/definition/malware. 01/03/2014.
19. SQL Query Reference. http://www.1keydata.com/sql/sql.html. 16/03/2014.
20. DNS Amplification Attacks. https://www.us-cert.gov/ncas/alerts/TA13-088A. 26/03/2014.
21. TheCompleteForensicHardwareSolution.http://www.digitalintelligence.com/products/fred/. 01/03/2014.
22. About FANNIE. https://www.digitalintelligence.com/products/fannie/. 01/03/2014
23. Rack-A-TACC 2U Module. http://oic.com.vn/english/Rack-A-TACC-2U-Module_product_841_9179.html. 26/03/2014.
24. ElcomsoftDistributedPasswordRecovery.http://www.digitalintelligence.com/products/gpupowerstation/. 16/03/2014.
25. Forensic Duplicators. http://www.guidancesoftware.com/products/Pages/tableau/products/duplicators.aspx. 25/03/2014.
26. HardCopy 3P - 1:2 Forensic Hard Drive Duplicator.http://www.voomtech.com/content/hardcopy-3p. 11/03/2014.
27. What is the SHADOW 2? http://www.digitalintelligence.com/products/shadow2/. 16/03/2014.
28. Digital Intelligence Software. http://www.digitalintelligence.com/cart/ComputerForensicsProducts/Digital-Intelligence-Software-p1.html. 15/03/2014.
29. World leader in digital investigations™. http://www.guidancesoftware.com/. 14/03/2014.
30. The layered defense approach to security. http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzaj4%2Frzaj40a0internetsecurity.htm. 13/03/2014.
31. The Basics of Cloud Forensics. http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/. 30/03/2014.

Gait Pattern: A Walking Image to Determine Sex of An Individual

Swapnil Gupta* & Kopal Gupta**

Keywords

FL, RSA, LSA, RSL, LSL.

Abstract

A single step is a complex series of actions and its combination develops a pattern known to as Gait Pattern. Gait refers to the style of walking of an individual. Gait Pattern depends upon sex, height, weight and age of an individual. Every species either belonging to human or animal is having different way of walking pattern. Identification of a human by analysis of Gait Pattern has recently become a popular biometric problem. Human Gait is a spatio-temporal phenomenon that characterizes the motion of an individual. In the present study 100 subjects (50 males & 50 females) of Baniya Community of India and between 17 to 47 year age group were evaluated for determining the sex of a human. This paper explains the study of Gait Pattern on walking surface where walking image is clearly visible.

Introduction

THE culprit approaches, stays and then leaves the scene of occurrence. What clue is there only the track mark as footprints or footwear marks either in visible or invisible form. This evidence often connects the criminal with the crime conclusively. The series of either footprints or footwear marks are referred to as Gait. The art of tracking through gait pattern is an ancient art. It is practised in various parts of India by certain families. The trackers are known as Khojis or Paggies. They follow the track mark of individual at the scene of crime

Author Intro:

* Laboratory Assistant, CFSL (CBI), New Delhi. E-mail: [swapnil4inspire@gmail.com]

** Scientific Assistant, FSL, Delhi. E-mail: [kopal4bud@gmail.com]

for identification. The trackers don't take any extensive measurements nor do they take down any notes. They create the impression of uncanny powder to identify the culprits.

Human walking system involves two essential abilities. The first in equilibrium, which is the ability to assume an upright posture and maintain balance while another is locomotion, which is the ability to initiate and maintain rhythmic stepping.

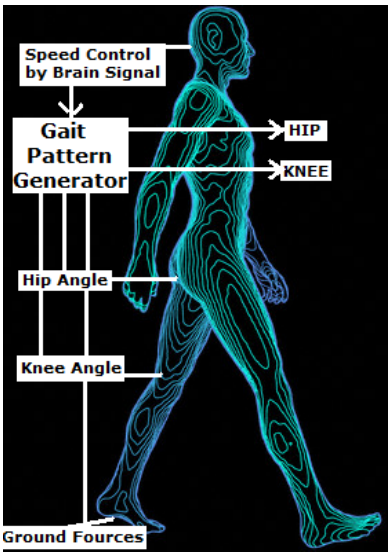


Fig 1: Human Walking System

A human Gait cycle can be broadly classified into two phases: wiz: Swing Phase and Stance Phase. The walking can be subdivided into following phases:

- **Initial Contact:** It is the moment when the swing leg foot just touches the floor. The heel strikes at first place. The hip is flexed, the knee is extended and the ankle is dorsiflexed to neutral. The other leg is the end of terminal stance. This phase can be skipped in the fast walking. At heel strikes, the foot can have acceleration of several hundred m/s over periods of some 25 ms. In fact, it is a deceleration, the foot moves down and backward at 2-3 m/s and is stopped by the floor very abruptly, in 10-15 ms.

- **Loading Response:** It is the double stance period beginning when the foot contacts the floor and continues untill the other foot

is lifted for swing. This is a period of extensive muscle activity. The ankle dorsiflexors act electronically to prevent slapping of the foot on the ground. The knee flexes up to 20 degrees in this phase. The acceleration and energy transfer changes the speed.

- **Mid Stance:** In this phase the leg advances over the foot by ankle dorsiflexion while the hip and knee extend. The other leg is advancing in its mid-swing phase.

- **Terminal Stance:** It begins with the heel rise of the stance foot and continues until the swing leg strikes the ground.

- **Pre-Swing:** It's the second double stance interval in the Gait cycle. It begins with the initial contact of the opposite leg's foot and ends with toe-off. Along with loading response, this is the period of widespread muscle activity. The foot is in its most supinated and rigid position, which produces a propulsive push off. The change in speed can take place in this phase.

- **Initial Swing:** It begins when the foot is lifted from the floor and ends when the swinging foot is opposite the stance foot.

- **Mid Swing:** It continues from the end point of the initial swing and continues until the swinging limb is in front of the body and the tibia is vertical. The other leg is in late mid stance.

- **Terminal Swing:** It begins when the tibia is vertical and ends when the foot touches the floor. The hip maintains its flexion and ankle remain dorsiflexed to neutral.

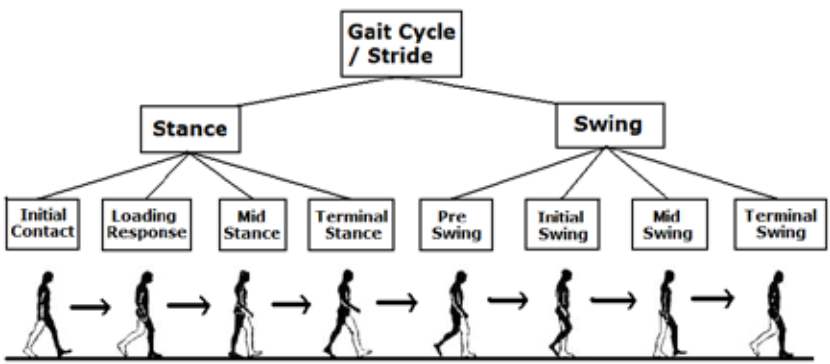


Fig. 2: Phases of Human Walking System

When a person, while walking or running, makes a series of impression, it is called a Gait Pattern or Walking Picture or Walking Ensemble. It is possible to deduce some of the characteristics of the owner's manner of walking. Walking Pattern is found to be highly individualistic. The Gait Pattern is analysed by Gait Pattern Parameters which are as follows:

- **Direction Line (DL):** It is an imaginary line, which indicates the direction in which person is walking. It is a straight line.

- **Walk Line (WL)/ Gait Line:** It is formed when person's walk coincides with direction line and along the inner sides of both heel prints. It is a zigzag line due to maintaining of the equilibrium.

- **Foot Line (FL)** - It is a straight line running through the longitudinal axis of footprint. This line passes through 2nd toe to the centre of the heel.

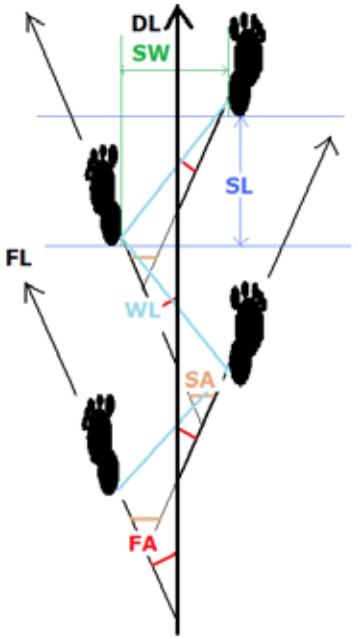


Fig. 3: Elements of a Gait Pattern

- **Foot Angle (FA):** It is an angle between the direction line and foot line. It may vary for the right & left foot of same person.

- **Step Angle (SA)/Principle angle:** It is the angle between the foot lines of two feet. So it is the sum of the two foot angles.

- **Step Length (SL):** It is the distance between the centres of two successive heel prints. It depends upon the height and speed of walker.

- **Step Width (SW):** It is distance between the parallel drawn in the direction of direction line touching the inner sides of the right and the left foot.

It is customary at present to study it as evaluation of Gait Pattern requires at least four consecutive feet or footwear marks. They are available only on the scene of occurrence only. As the clarity of the individual marks is not so important in Gait Pattern studies, it is expected that Gait Pattern evidence will be found useful in more cases than the individual foot or footwear marks. Gait Pattern can be studied scientifically. Although its study involves Gait Parameters i.e. Direction Line (DL), Walk Line (WL), Foot Line (FL), Foot Angle (FA), Step Angle (SA), Step Length (SL) and Step Width (SW) but also dimensions, peculiarities, pressure points, and defects of marks are also important.

Gait Pattern can be present on two form on to any surface i.e. footprints & footwear marks:

1. **Footprints:** When footprints are present in series, it form Gait Pattern. It is commonly present on the crime scene. It is mainly found in the rural areas. Footprints are more valuable marks because in case of footwear mark, it has to be proved that particular footwear belongs to the same person.

Fig. 4: A Series of Footprints

2. **Footwear Marks:** When footwear marks are present in series, it form Gait Pattern. It is found on both rural and urban areas. Footwear marks are less valuable than footprint because after some time footwear looses their characteristics.

Fig. 5: A Series of Footwear Marks

Gait Pattern can be formed into two types according to the surface i.e. surface & sunken pattern.

i. Surface Gait Pattern: When the footprint or footwear marks are formed in dirt, dust, oil, blood and by its deposition on to other surface, it is called Surface Gait Pattern. They are mainly formed in Indoor Crime Scene. It is of 2D type.

Fig. 6: Surface Pattern

ii. Sunken Gait Pattern: When the footprint or footwear marks are formed in mud, sand, soil, snow and their related parts, it is called Sunken Gait Pattern. It is of 3D type.

Fig. 7: Sunken Pattern

Material & Methodology

In the present work, an attempt has been made to analyze the Gait Pattern for Sex determination. For this, a total of 100 subjects (50 males & 50 females) of Baniya Community of India ranging between 17 to 47 year age group were evaluated. The present study has been made from the volunteer (both male and female) Gait Pattern on the dirty soil surface. Volunteer were asked to give their Gait Pattern on this surface. This Gait Pattern was then collected by method of Tracing.

Although there are different method of collecting Gait Pattern i.e. Photography, Tracing, Lifting and Casting. But the present study involves method of Tracing because it collects Xerox of Gait Pattern. So by this all Gait Parameters can be analyzed very easily.

Tracing is the best method to record the Gait Pattern of an individual. Firstly, a surface was created on the soil surface. For that fine dust was scattered on the solid soil surface with 1 inch thickness. Then each volunteer was asked to give his footwear marks in form of Gait Pattern. They were asked to walk along 16 feet in order to reduce the error and normal Gait Pattern. After formation of Gait Pattern, a glass plate approx. 8 feet in length and 3 feet in width is taken, which is supported at its all four corners by wood blocks. Then this glass plate is placed over the Gait Pattern. Now with the help of Black Marker outline is drawn to obtain minimum four successive marks. Afterwards a plastic sheet of same dimension as glass sheet is placed over the same glass sheet. Again tracing of marks is done now with Permanent Black Marker from glass sheet. In this way, a Gait Pattern of individual was collected on the Plastic sheet. The same whole procedure was continued to collect Gait Pattern of 100 subjects and each plastic sheets were collected for the examination purpose.

Fig. 8: Step 1 [Creation of Gait Pattern on Soil Surface]

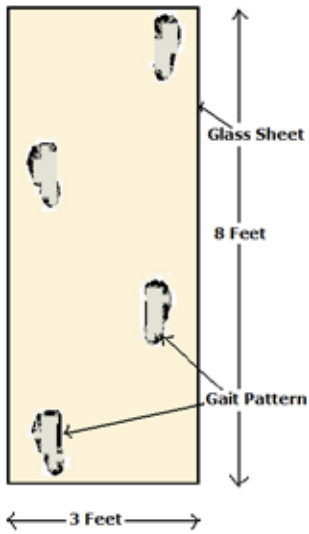


Fig. 9: Step 2 [Placing of glass plate over the gait pattern]

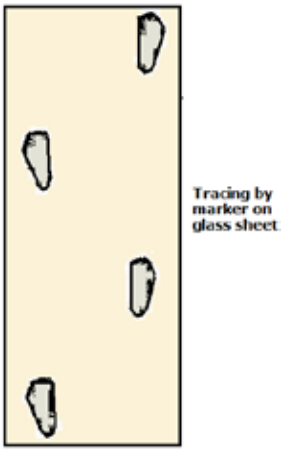


Fig. 10: Step 3 [Tracing of gait pattern by marker on glass sheet]

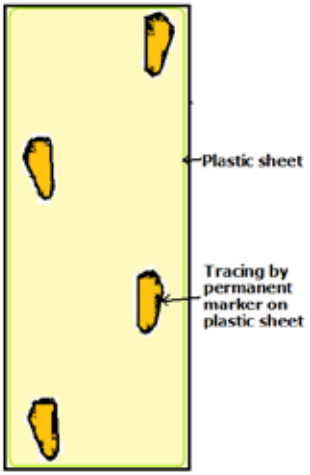


Fig. 11: Step 4 [Tracing of gait pattern by permanent marker on plastic sheet]

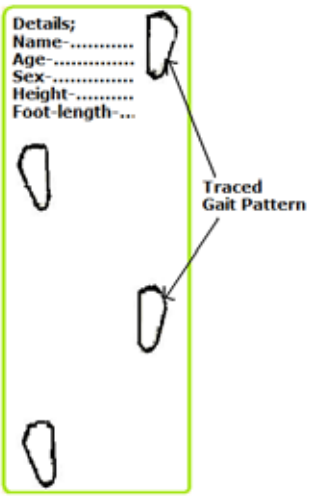


Fig. 12: Step 5 [Traced gait pattern]

Examination of Gait Pattern is performed by analysis of recorded pattern in the plastic sheet. Each plastic sheet should contain the details of the Volunteer including their Name, Age, Sex, Height, Foot-length. Afterwards all the lengths & angles i.e. Foot Length [FL], Right Step Angle [RSA], Left Step Angle [LSA], Right Step Length [RSL] and Left Step Length [LSL] are noted on the one side of the plastic sheet.

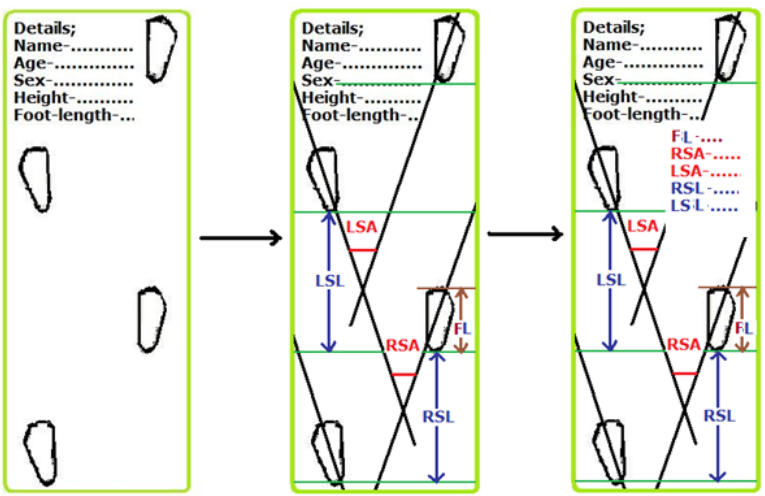


Fig. 13: Step 6 [Examination of gait pattern]

Result

The current studies focus on the importance of Gait Pattern for the discrimination of the Sexes. Men and women walk differently, hence their walking pattern also showing the differentiation. By the statical calculation of all the Gait Parameters of the Gait Pattern i.e. Foot Length [FL], Right Step Angle [RSA], Left Step Angle [LSA], Right Step Length [RSL] and Left Step Length [LSL] a definite observation about the sex difference can be made. Foot Length [**FL**] of Male and Female shows difference of approx 2.6 cm in the length, Right Step Angle [**RSA**] shows difference of approx 6.5 degree in the angle, Left Step Angle [**LSA**] shows difference of approx 6.1 degree in the angle, Right Step Length [**RSL**] shows difference of approx 4.1 cm in the length and Left Step Length [**LSL**] shows difference of approx 4.7 cm in the length.

Table 1: Readings of Gait Pattern for Male

Subject	Age	Sex	Foot-length	Right Step Angle	Left Step Angle	Right Step Length	Left Step Length
			(FL)	(RSA)	(LSA)	(RSL)	(LSL)
SUB 1	21	M	25.3	44	46	26	27
SUB 2	23	M	25	30	35	29	30
SUB 3	17	M	22.4	37	30	30	32.5
SUB 4	17	M	26	20	18	30	29.5
SUB 5	17	M	26.6	14	10	31.5	30.5
SUB 6	22	M	24.2	18	20	24.5	26.5
SUB 7	45	M	23.5	30	28	21.5	24.5
SUB 8	31	M	25	18	15	22	23.5
SUB 9	40	M	26	30	26	23	23.5
SUB 10	23	M	24.2	41	47	28.5	28
SUB 11	23	M	24.8	35	40	22.5	23.5
SUB 12	18	M	24	22	23	30	31
SUB 13	21	M	26	8	8	29	29.5
SUB 14	17	M	23.7	20	18	25.5	26.5
SUB 15	18	M	24.7	20	20	29.5	29
SUB 16	24	M	24	30	20	27.5	30
SUB 17	50	M	25.3	36	38	18	20
SUB 18	18	M	25.4	15	13	24.5	25.5

Subject	Age	Sex	Foot-length	Right Step Angle	Left Step Angle	Right Step Length	Left Step Length
			(FL)	(RSA)	(LSA)	(RSL)	(LSL)
SUB 19	17	M	25	43	43	25	26.5
SUB 20	37	M	25	33	32	23.5	25
SUB 21	20	M	25	8	10	29	30
SUB 22	50	M	24.7	20	21	25.5	27.5
SUB 23	22	M	26.5	16	15	24	25
SUB 24	18	M	26	40	42	27	28
SUB 25	20	M	23.6	24	25	24	25
SUB 26	18	M	23.8	36	37	22.5	24.5
SUB 27	40	M	26.5	25	31	24	25.5
SUB 28	18	M	25.1	25	29	22	22.5
SUB 29	17	M	23.2	31	37	24	23.5
SUB 30	23	M	23.4	20	25	20	20.5
SUB 31	27	M	24	22	23	26.5	27.5
SUB 32	35	M	24.8	35	41	28.5	29.5
SUB 33	32	M	23.6	26	28	30.5	33
SUB 34	33	M	23.6	25	29	29.5	29
SUB 35	33	M	22.7	15	12	32	31
SUB 36	31	M	24.4	22	24	24	26
SUB 37	21	M	26.5	15	12	22	25
SUB 38	19	M	27	30	32	21.5	23
SUB 39	45	M	25.3	32	35	22	23.5
SUB 40	29	M	24.2	30	23	23	23.5
SUB 41	22	M	24.5	20	18	29	29.5
SUB 42	37	M	23.7	20	22	28	28.5
SUB 43	18	M	26.3	15	16	25	27
SUB 44	20	M	22.9	19	25	27.5	30
SUB 45	22	M	24.1	27	19	22	22
SUB 46	25	M	22.3	32	32	24.5	25.5
SUB 47	26	M	26.5	21	23	25	26.5
SUB 48	32	M	26	34	34	24	25
SUB 49	19	M	26.1	21	23	23.5	23
SUB 50	40	M	25	15	16	29	30
	Total	**Mean**	**24.748**	**25.3**	**25.78**	**25.6**	**26.64**

Table 2: Readings of Gait Pattern for Female

Subject	Age	Sex	Foot-length	Right Step Angle	Left Step Angle	Right Step Length	Left Step Length
			(FL)	(RSA)	(LSA)	(RSL)	(LSL)
SUB1	19	F	22	18	22	20.5	21.5
SUB2	20	F	22.2	17	17	19	19
SUB3	18	F	21.4	17	10	23.5	24
SUB4	17	F	22.5	30	30	19	20.5
SUB5	17	F	22	20	15	23.5	25.5
SUB6	17	F	22.3	29	30	24.5	26.5
SUB7	19	F	24.1	17	25	22	23
SUB8	40	F	20.6	20	20	21	23
SUB9	48	F	23.9	25	25	18	20.5
SUB10	47	F	22.5	20	20	21.5	23
SUB11	17	F	20.8	20	23	20.5	22.5
SUB12	20	F	21.6	20	20	22	22
SUB13	18	F	23	15	15	22.5	21.5
SUB14	19	F	20.5	8	8	22.5	21.5
SUB15	35	F	24.2	30	30	23	24
SUB16	19	F	21.3	18	15	23.5	24.5
SUB17	18	F	24.5	20	22	21	21.5
SUB18	22	F	23.9	10	12	22.5	22
SUB19	42	F	23	15	16	20	20.5
SUB20	27	F	23.7	25	25	23	24
SUB21	18	F	22.2	16	17	19	20.5
SUB22	45	F	25	15	17	24	25
SUB23	35	F	21.5	17	20	23.5	25
SUB24	42	F	24	15	18	20	20.5
SUB25	20	F	22.9	17	19	23	23.5
SUB26	29	F	21.9	15	16	20.5	21.5
SUB27	22	F	22.1	12	15	22	20
SUB28	18	F	22.2	25	25	22.5	22.5
SUB29	24	F	23.7	15	20	22	21.5
SUB30	18	F	22.7	17	21	21.5	22
SUB31	42	F	23.4	20	25	23	22.5

Subject	Age	Sex	Foot-length	Right Step Angle	Left Step Angle	Right Step Length	Left Step Length
			(FL)	(RSA)	(LSA)	(RSL)	(LSL)
SUB32	20	F	22	15	15	20	20.5
SUB33	21	F	21.3	25	25	20	20
SUB34	24	F	23.6	21	20	19.5	19
SUB35	29	F	20.5	12	15	21.5	20.5
SUB36	25	F	19.8	15	18	21	23
SUB37	19	F	21.2	19	15	23	22
SUB38	39	F	22	30	25	20	19.5
SUB39	26	F	21.7	20	21	23	22.5
SUB40	26	F	20.2	14	14	19	20
SUB41	21	F	20.5	10	12	21	20
SUB42	23	F	23.1	19	20	22	21
SUB43	18	F	20.7	16	19	23	24
SUB44	19	F	19.7	20	18	18	19
SUB45	20	F	21.5	17	20	23.5	24
SUB46	27	F	20.8	25	25	22	21
SUB47	29	F	21.3	30	31	20.5	20.5
SUB48	31	F	21.4	15	16	21	21
SUB49	33	F	23	18	20	22.5	22
SUB50	32	F	21	21	20	20	20
	Total	**Mean**	**22.138**	**18.8**	**19.64**	**21.49**	**21.89**

Table 3: Mean of Gait Parameters for Male & Female

Gait Parameters	Male (Mean) = X	Female (Mean) = Y	Mean Difference = Z
Foot Length (FL) (cm)	24.748	22.138	2.610 cm
Right Step Angle (RSA) (degree)	25.30	18.80	6.50 degree
Left Step Angle (LSA) (degree)	25.78	19.64	6.14 degree
Right Step Length (RSL) (cm)	25.60	21.49	4.11 cm
Left Step Length (LSL) (cm)	26.64	21.89	4.75 cm

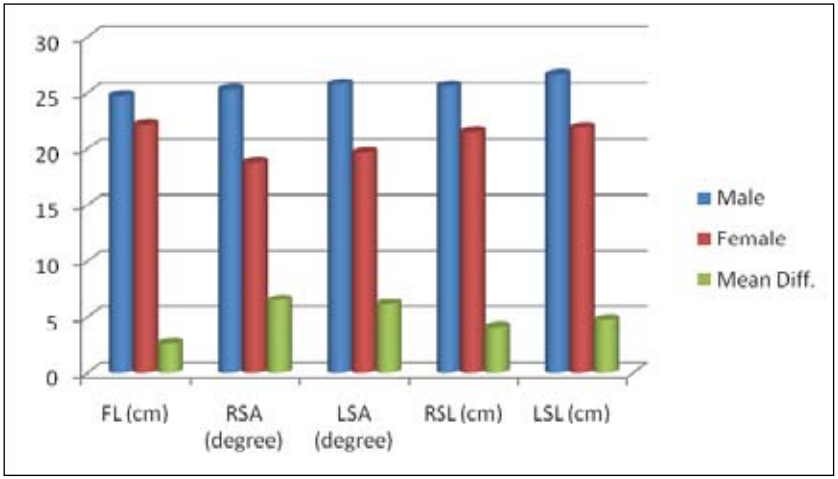


Fig. 14: Mean of Gait Parameters for Male & Female

Conclusion

Gait as a biometric has many advantages over other forms of human identification. However, for security applications, it would be useful to determine physical attributes of a subject, such as gender, height, weight, etc to decrease the number of suspects.

The present work can be useful to judge the sex of an individual by the forensic analysis of Gait Pattern. Hence Image of a sex of a person on the mind can be differentiated after the examination and calculation of Walking Pattern. Just five parameters can distinguish the sex by Gait Pattern i.e. Foot Length [FL], Right Step Angle [RSA], Left Step Angle [LSA], Right Step Length [RSL] and Left Step Length [LSL]. This paper certainly is useful to Forensic Scientist.

References

1. Cordero, A.F. (2003), "Human gait, stumble and... fall?", University of Twente, *Enschede, Netherlands*.
2. Eek, M.N. (2009), "Muscle Strength, Gross Motor Function and Gait Pattern in Children with Cerebral Palsy", *Institute of Clinical Sciences/ department of Pediatrics at Sahlgrenska Academy, University of Gothenburg*.
3. Fessler, D.M.T. et al. (2005), "Sexual dimorphism in foot length proportionate to stature", *Annals of Human Biology, January-February 2005; 32(1): 44–59*.

4. Johnsoni, K.L. & Tassinary L.G. (2005), "Perceiving Sex Directly and Indirectly Meaning in Motion and Morphology", *American Psychological Society Volume 16-Number 11*.

5. Kuhlman, M. (2007), "Determining Height and Gender of a Subject Using Gait", *Clarkson University*.

6. Lee, L. (2003), "Gait Analysis for Classification", *Massachusetts institute of technology -artificial intelligence laboratory*.

7. Ozden, H. et al. (2005), "Stature and sex estimate using foot and shoe dimensions", *Forensic Science International 147 (2005) 181–184*.

8. Riemann, B.L. (2001), "The Effects of Sex, Joint Angle, and the Gastrocnemius Muscle on Passive Ankle Joint Complex Stiffness", *Journal of Athletic Training 2001; 36 (4):369–377*.

9. Ronkkonen, J. (2004), "Video Based Gait Analysis in Biometric Person Authentication : An Brief Overview", *Lappeenranta University of Technology, Finland*.

Management of a Welfare Programme: "Bhadratha Scheme" in Andhra Pradesh – A Study

Dr. G. Siva Rama Sarma*

Keywords

Bhadratha Scheme, Hazardous, Managing Committee, Subscription, Ex-gratia, House Building Advance, Loans, Perception, Social Security, Financial Relief, Red Tapism.

Abstract

Police job has become increasingly hazardous during the last few decades. A comprehensive social security scheme called "Bhadratha" aims to provide financial relief to the police personnel who die in harness and provides financial relief to the employees who are permanently disabled due to accident or disease. The scheme is managed by Managing board consisting of Police Officers headed by Director General of Police.

The opinion of the police personnel have been taken by administering a semi-structured questionnaire on the working of the scheme. The data furnished by the Department and sample responders reveal that the scheme, though it is being implemented smoothly, it needs every care so as to avoid delay in sanctioning the loan amount to the employees.

Introduction

POLICE job is not only arduous and stressful, but has become increasingly hazardous during the last few decades. A large number of police personnel are losing their lives in the line of duty. Keeping in view of problem a comprehensive social security scheme called "BHADRATHA" was introduced with effect from 01/03/1997 in Andhra Pradesh with an aim to provide substantial financial relief to the families of employees who die in harness[1].

Author Intro:

* Professor (Retd.), Osmania University, A.P.

The scheme also provides financial relief to the employees who are permanently disabled or partially disabled due to accident or disease. All these benefits are available out of corpus made up by a uniform monthly subscriptions, fixed by the Board irrespective of the age of the employees.

Managing Committee

The bye-laws of the association are registered under the AP (Telangana) Public Societies Registration Act and the scheme is managed by a Managing Committee whose members are nominated by Director General of Police and Inspector General of Police, who functions as its ex-officio Chairman. A General Body consisting of representatives from all the units is nominated by the Chairman. The term of both the Managing Committee and General Body is for a period of three years. The Managing Committee consists of not more than 10 members and not less than 7 members, including Chairman. The managing committee consists Chairman, Vice-Chairman and Executive Members.

The Managing Committee normally meets once in a month, but not later than once in three months for the transaction of business. Three members or 1/3rd of the members, whichever is more, shall constitute quorum. The Managing Committee authorizes the Secretary/Executive Officer to open Bank account and draw the amount of the Association by a resolution. One of the managing committee members as nominated by the Chairman will be the Joint Secretary.

Enrolment Fee and Subscription

Each member should pay the enrolment fee of Rs. 10 at the time of his joining as a member in the association. The enrolment fee shall be recovered through his salary. Each member should pay the monthly subscription which would be recovered during the period of service from his salary every month at the rates mentioned hereunder or as may be decided by the Managing Committee from time to time[2].

a) Rs. 100-00: in respect of employees in the Police Department in the categories of Constables to Assistant Sub Inspectors/Equivalent cadres.

b) Rs. 200-00: in respect of employees in the categories of Sub Inspector to Director General of Police/Equivalent cadres.

The benefits accrued to employees from the scheme may be discussed under four headings.

- **While in service:** The member will be eligible for grant of House Building Advances (HRA) loan for purchase of plot, for construction of house, for purchase of ready built flat, for construction of additional accommodation to the already existing house or completion of house already started with loan from Government.

- **On retirement, resignation, removal, dismissal:** The subscription outstanding to the credit of the member will be refunded to the member with interest which will not be not less than saving bank interest as decided by the Managing Committee from time to time.

- **On Death of a Member:** The subscription deducted from the members pay is repaid to the nominee, nominated by the member from among his family members. Rs. 1,00,000/- is paid as an ex-gratia to the member in the category of Constable to Assistant Sub Inspector and equivalent categories in other department, and Rs. 2,00,000 is paid as an ex-gratia to the members in the category from Sub Inspector to Director General of Police and equivalent categories. An additional ex-gratia of Rs. 15,000/- is also payable besides the ex-gratia in case of the death has arose out of eventualities such as accident, burning, drowning, firing, murder, etc.

- **On disablement of member:** A ex-gratia of Rs. 15,000/- is paid to a member who sustains total / permanent disability i.e. two limbs and both eyes or total eye vision and an ex-gratia of Rs. 7,500/- is paid to a member who sustains partial or permanent disablement i.e. loss of one limb, one eye as result of accident or disease.

The scheme covers all the employees of police department including ministerial and last grade employees. The nominee of the employees who dies while in service is paid Rs. 1,00,000/- in case of subscription of Rs. 100/- and Rs. 2,00,000/- in case of subscription of Rs. 200/-.

As discussed earlier, the Bhadrata scheme is being managed by a Managing Committee nominated by the Chairman, and the Committee will conduct the business and affairs of the fund through the secretary. In addition to the Managing Committee, a General Body is also constituted by the Chairman drafting different category of employees from different units. The general body will meet once in a year to approve the statement of accounts of the previous year and ratify actions of managing committee, which are not covered by the Bye-laws. The Managing Committee publishes the Annual Administration Report under the caption 'Bhadrata'. The annual general body meeting generally be held at Hyderabad, a number of delegates from Units will participate in the annual meeting.

All employees of the Police Department appointed on regular basis including those away on deputation are eligible to become members of Bhadrata Scheme. The scheme is not applicable to those who are employed on casual and contract basis and also to the employees who are working in Police Department on deputation from other departments.[3]

The amount of subscription shall be remitted through the demand draft in case of units in muffisil areas and cash remittance at Indian Overseas Bank extension counter at DG and IGP Office in case of units situated in twin cities of Hyderabad and Secunderabad. The remittances of the subscription must reach the secretary, Bhadrata Scheme on or before 5th of the following month in order to avoid loss of interest, which is the source of income for payment of ex-gratia, etc to the members or families of the deceased members.

House Building Advance Loan from Bhadrata Scheme

Every employee of the Police Department should have a shelter by owning a house with in the affordable cost is reflected in this house building concept under the Bhadratha Scheme. Keeping this in view the Managing Committee of Bhadratha has formulated a scheme for extending house, building advance loans to the members duly utilizing the Bhadrata funds.

The member should have put up at least 5 years of service in the department and 12 months membership in Bhadrata scheme and should

have 5 years of left over service and must submit Bhadrata nomination forms along with Bhadrata account number for the sanction of loan. The maximum loan recoverable period is 180 months.

Table – 1
Statement showing quantum of loan and interest rates under BHADRATHA SCHEME

S.No.	Category	Loan eligibility	Rate of Interest
1	Police Constable to Assistant Sub Inspector & Equivalent	Rs. 2,50,000	9.5
2	Sub Inspector & Circle Inspector & Equivalent	Rs. 5,00,000	9.5
3	Dy. Superintendent of Police and above	Rs. 7,50,000	9.5

Source : DGP Office, Welfare Division, Hyderabad.

All sanctions under the Bhadratha Scheme were charged with 1 per cent processing charges as one time payment, which will be recovered up while releasing the loan amount.

Activities of Bhadratha Scheme

House Building Advances

- o House Loans were introduced in 1998.
- o From 1998 to Dec' 2006 an amount of Rs. 3,428.47 lakhs was sanctioned to 1541 members.
- o During current year 2007, an amount of Rs. 878.75 lakhs was sanctioned to 223 members.
- o During the current year 2007, an amount of Rs. 5.03 lakhs were written-off in respect of 3 death cases reported.
- o An amount of Rs. 211.00 lakhs is utilized from investment Maturities to release the more number of HBA loans in addition to regular budget.

Personal Loan

- o Personal loans were introduced in 2003.
- o During the period from 2003 to 2006, an amount of Rs. 4,150.34 lakhs was sanctioned to 8136 members.

- During the year 2007, an amount of Rs. 759.85 lakhs were released to 1782 members.
- During the year 2007 an amount of Rs. 7.84 lakhs were written-off in respect of 18 deaths reported.

Personal Loan for Daughter's marriage :

- Personal loans to the members for Daughter's marriage were sanctioned for meeting the expenditure. A maximum amount of Rs. 1 lakh is being sanctioned to all cadres.
- The rate of Interest on Personal Loans for Daughter's marriage is 11%.
- During the year 2006 an amount of Rs. 618.15 lakhs was sanctioned to 697 members.
- During the year 2007 an amount of Rs. 341.70 lakhs was sanctioned to 411 members for their daughter's marriage.

Educational Loans

- Educational Loans were introduced in June, 2006.
- These loans are provided @ 9.5% p.a. to the members.
- The maximum limit of Educational loan is Rs. 1 lakh.
- During the financial year 2006, an amount of Rs. 1.5 lakhs was sanctioned as Educational loan to 2 members.
- During the year 2007, an amount of Rs. 28.34 lakhs was sanctioned as educational loans to 36 members.

Computer Loans

- Computer loans were introduced in 2001.
- The rate of interest on computer loans is 9%.
- During the period from 2001 to 2006, an amount of Rs. 20.04 lakhs was sanctioned as computer loans to 103 members.
- During the year 2007, an amount of Rs. 32.27 lakhs were released as Computer loans to 83 members.
- Due to the relaxation of the procedure for purchase of computers – the cheques are given to the applicant in favour of the dealer, so that the applicant can approach the dealer and collect the computer by handing over the cheque to the dealer.

Settlements – Ex-gratia :

- During the year 2006, an amount of Rs. 636.00 lakhs was paid in respect of 581 death cases.
- During the year 2007, an amount of Rs. 508.00 lakhs was paid as retirement benefits to 1521 retired officers.
- In retirement cases rate is increased from 3% to 5%.

The major inflow of funds of the association and its utilization for the year 2005-06 are as under.

Table - 2

Inflow of Funds			Utilization of Funds		
Particulars	**2004-05**	**2005-06**	**Particulars**	**2004-05**	**2005-06**
Subscription	1118.60	1126.37	Investments (net)	782.00	-75.00
Interest on Investments	345.12	363.06	Subscriptions repaid	114.80	145.07
Insurance claims received	446.00	828.50	Interest on subscriptions repaid	12.33	18.33
HBA Principal Recovery/ Repayment	191.32	136.34	Insurance premium paid	429.22	457.31
Interest on HBA Loans	156.50	181.07	HBA Loans	186.72	268.48
PL Principal amount Recovery/ Repayment	103.64	256.46	Personal loans	492.35	1785.16
Interest on P Loans	74.04	182.78	Computer loans		1.60
PL Caution deposit	12.40	32.52	Ex-gratia paid	428.00	858.75
CL Principal recovery	3.10	3.47	Salaries & Wages	17.50	17.09
Int on Computer loan	1.27	0.79	Interest on AB deposits		20.41
Loan from AB		350.00	Office equipment/ Furniture	4.04	7.63
Other recipients (net)	14.97	43.47			
Total Amount	**2466.96**	**3504.83**		**2466.96**	**3504.83**
PL Personal Loans - CL Computer Loans - HBA House Building Advances					

Source : Welfare Division, DGP Office, Hyderabad.

It may be noted that data provided in Table - 2 shows that the scheme is being maintained systematically for serving police personnel. All these prove that "Bhadratha" is comprehensive social security scheme

which is providing substantial financial relief to the members and also to the families of the employees who die in harness.

Perception of Police Personnel on the Scheme

A semi-structured questionnaire is used in order to know how the scheme is being utilized in Andhra Pradesh, covering 100 sample police personnel which include 80 Constables, 13 ASIs/Head Constables and 7 Sub Inspectors in Ranga Reddy District. As discussed earlier, ex-gratia amount is paid from Bhadratha scheme. In order to know the opinion of Police Personnel, a question is administered on the sample Police personnel in regard to adequacy of the ex-gratia amount paid to the members of the scheme. Opinion of the sample respondents is presented in the Table – 3.

Table - 3
Statement showing the distribution of the sample Police Personnel in regard to adequacy of ex-gratia received from BHADRATHA SCHEME Inflow of Funds

S. No.	Opinion of the sample Police Personnel	No of sample Police Personnel
1	Adequate	61
2	Not Adequate	39
	Total	**100**

The analysis of the opinion of sample police personnel on adequacy of ex-gratia presented in the Table – 3 reveals that 61% of the police personnel have expressed their feelings that ex-gratia received from Bhadratha scheme is sufficient or adequate in case of death of a member or on disablement of a member. 39% of the sample respondents have noted that ex-gratia amount is not adequate and the amount should be doubled in case of death or permanent disablement.

As Bhadratha scheme functions on the monthly subscription of police personnel , a question is administered on the sample police personnel to collect their opinion on the rate of subscription to the scheme. The date is presented in Table - 4.

Table - 4
Statement showing the distribution of the sample Police Personnel in regard to Subscription towards BHADRATHA SCHEME

S. No.	Opinion of the sample Police Personnel	No of sample Police Personnel
1	Normal	28%
2	Adequate	56%
3	Low	13%
4	Don't know	3%
	Total	**100%**

The analysis of data presented in Table – 4 reveals that 28% feel that the rate of contribution to the Bhadratha Scheme is normal and they neither supported for upward revision nor reduction of subscription amount paid by the police personnel. 56% of the respondents have reported the existing monthly subscription is substantially adequate for strengthening the schemes. 13% of these are of the viewed that the subscription rate may be doubled so that the benefits accrued from the scheme would also be doubled to the beneficiaries. 3% sample respondents have kept silent.

A question is also administered on the sample respondents regarding the process of sanction and releasing of loan and adequacy of loan. The opinions are presented in the following Tables;

Table - 5
Statement showing the opinion of the sample respondents on the process of Loan sanction

S. No.	Opinion of the sample Police Personnel	No of sample Police Personnel
1	Quick	12%
2	Delay	86%
3	Abnormal delay	2%
	Total	**100%**

Table - 6
Statement showing the distribution of sample Police Personnel on the opinion of Loans release

S. No.	Opinion of the sample Police Personnel	No of sample Police Personnel
1	Quick	28%
2	Delay	72%
3	Abnormal delay	0%
	Total	**100%**

Table - 7
Statement showing the opinions of the sample Police Personnel on the adequacy of Loan amount

S. No.	Opinion of the sample Police Personnel	Nof of sample Police Personnel
1	Adequate	9%
2	Inadequate	91%
	Total	**100%**

An analysis of data on the opinion of sample police personnel regarding the process of loan sanction, shown in the Table - 5 reveals that surprisingly many of the sample respondents are of the opinion that the time taken for the process of loan sanction is delay due to the rules and regulations prescribed for sanctioning the loan to the police personnel and it is a hurdle for the police personnel that delay causes thus much anxiety in knowing the sanction of the loan along with their arduous and tension oriented duties. They are of the opinion that the loan is not sanctioned on time, they have to face financial stringencies in meeting their emergent needs. Only two respondents have noted there is abnormal delay in getting sanction the loan. 12% of the sample respondents are of the opinion that the loans are sanctioned quickly.

An analysis of opinion of the sample respondents regarding the loan release provided in the Table 3.7 shows that 72 sample respondents are of the opinion that when once the loan is sanctioned by the committee of Bhadrathathe incumbent has to get long period to get the release of loan amount. 28 respondent expressed that loan is sanctioned quickly.

No respondent has noted about the abnormal delay in getting the loan. The sample police personnel, who have supported their argument of delay both in the sanctioning and releasing loan amount are the two important hurdles coming in a way of successful functioning of the scheme. They are of the view that delay caused in these process should be enrouted for the benefit of the police personnel who require financial assistance on time.

In order to know the opinion of the sample respondents on the adequacy of the loan amount, a question is administered and their opinions are analyzed in the Table - 7. It is very important to note that 91 sample respondents reported that sanctioned loan amount is not adequate to meet the expenditure because of unpredictable changes in the market system. Hence, they strongly supported the upward revision of eligibility of the loan to the entire police officers from lower cadre to upper cadre. Only 9 respondents mentioned that the loan amount sanctioned and released to the police personnel is adequate for meeting their needs. So 9 respondents did not support the idea of increasing the loan amount and in addition to this they have suggested that the committee members should also take into account the repaying capacity of the police personnel and this would reduce the mis-utilization of the loan.

Conclusion

A comprehensive social security scheme called "Bhadratha" aims to provide financial relief to the families of the employees who die in harness. The scheme also provides financial relief to the employees who are permanently disable or partially disabled due to accident or disease. All these benefits are available out of corpus made up by the uniform monthly subscription fixed by the Managing Board. Though the novel scheme has been designed by the police department, many respondents are of the opinion that it has to be implemented more effectively as the police department is the biggest department in the state and every care has to be taken for proper implementation without any red-tapism.

References

1. Memo No. 1S-850/Pol.A1/97-1, dated 28/02/1997 of Home Department.
2. Bhadratha – AP Police Department Employee Benevolent and Thrift Mutual Association (Reg.No.1574 of 1997) – Bye-Laws.
3. Ibid, p.16

ERCHL Method for DNA Isolation from Hair Shafts: A Wildlife Forensic Approach

S.K. Yadav* & M.S. Dahiya**

Keywords

Forensic Hair, Mitochondrial DNA, DNA Extraction, Hair Lyses, Hair Shaft, DTT, SDS.

Abstract

An efficient, rapid and convenient hair lysis method (ERCHLM) for DNA extraction has been developed for forensic investigation which lyses hairs within 1h. To optimize this method, a mix concentration of DTT, SDS and Proteinase K was used in lysis buffer. Further DNA isolation process was carried out using an Automate-Express TM. This method was applied on hair shafts of Felidae animals to check its validity that provided fast hair lysis with minimal experimental sophistication as well as contamination.

Introduction

HAIR is most common evidence in wildlife crime as biological material associated with animals. Microscopic examination of hair remained a method of choice in earlier times, while later on protein and Genomic DNA from hair root cells have gained the interest of wildlife investigators due to its non-invasive nature in 21st century [1]. Ability of DNA in inhabitant's statistics to allocate influence to associations of questioned hairs and references made DNA-based investigation the favorite technique for source recognition of forensic hair samples. But, Genomic DNA examination is feasible only when the root segment of hair and/or tissue is present, it was a limitation

Author Intro:

* Wildlife Forensic Biotechnology Research Laboratory, IFS, GFSU, Gandhinagar, India.

** Department of Forensic Science, Jain University, JC Road Campus, Bangalore, India. Email: Sameerforensics@gmail.com; msdahiya49@rediffmail.com

[2]. In case of shaded hairs, they do not adhere nuclear DNA due to hardening or keratinization process, whereas, mitochondrial DNA (mt-DNA) stay behind moderately undamaged in hair shafts [3] which makes mt-DNA achievable for further investigation [4]. Unfortunately, the keratinous nature of hair makes DNA extraction difficult which requires a series of treatments and lastly organic extraction using SDS and alkaline treatment for hours that increases the jeopardy of contaminations [5]. These treatments/ methods are time consuming and also decrease the DNA yields that make inconsistency in analysis [6]. Therefore, to overcome these problems, an easy, precise and rapid method (ERCHLM) has been developed to isolate DNA from hair shafts. This method lyses hair in single step using DTT, sodium dodsylsulphate (SDS) and Proteinase-K together in lysis buffer. For further DNA extraction, a magnetic bead and cartridge based Automate-express™ DNA extraction system was used. To establish this method, DNA isolation was carried out from hair shafts of 60 animals belonging to three different species viz. Panthera leo persica, Panthera pradus fusca and Panthera tigris tigris. The extracted DNA was quantified using Flurometer evaluations as well as Nanodrop [7] and samples were amplified with 12srRNA, 16srRNa and cytochrome b primers using gradient and verity thermal cycler. Amplicon was further sequenced using capillary sequencing which were identified by BLAST search. Nucleotide sequences were found to be identical in nucleotide database.

Thus, this newly developed method (ERCHLM) would be useful in wildlife crime investigation where hair shaft would be used as strong evidence.

Materials and Methods

Sample Collection: Shaded hair samples were taken from the reference repository of FWBRL, Institute of Forensic Science, Gandhinagar where these were collected previously vide letter no. WLP/28/ B/4651-54/2012-13, from Principle Chief Conservator of Forests, Government of Gujarat State [8]. Hair samples were treated with SDS followed by washing in absolute ethanol and millipore water to remove the impurities from the surface of the hair. Hair shafts were obtained by cutting 5 mm portion from the root side of the hairs. [9] Two hair shafts of lion and three of leopard and tiger were used for DNA extraction.

DNA Isolation: Hair shafts of the animals were dissected in 1-2 mm pieces and placed in 0.5 ml micro centrifuge tubes. A mix buffer solution (MBS) of 300 μL lysis buffer 1X TNE (50 mM Tris-HCl, 100 mM NaCl, 6.3 mM EDTA, pH 7.5) + 30 μL 1 mM Tris-HCl, pH 7.5 + 10 μL 20 mg/mL proteinase K solution (Invitrogen) + 10 μL 25% aq. SDS + 10 μL 1M DTT (in milli-Q) was used for the lysis of hairs. Centrifuge tubes were vortexed for15 sec. then transferred to shaking water bath at 560C till hairs dissolved to obtain lysed hair solution. Then this solution was transferred to lysep columns (Life Technologies) and kept inside sample tube which was centrifuged at 10000 rpm for 10 minutes at 40C. The sample tubes containing lysed hair solution were then placed in Automate-express to extract DNA using BTA-Forensic DNA extraction kit (Life Technologies). A 28 minute run for DNA extraction was followed and final elution volume was kept 25 μL. The qualitative and quantitative analysis of the isolated DNA was done using Nanodrop [7] and Flurometer where 1.5% and 2.0% agarose gel electrophoresis along with DNA ladders was used to ensure the quality of DNA.

DNA Amplification: The polymerase chain reaction (PCR) amplification of cytochrome b, 12srRNA and 16srRNA genes was carried out for 60 Felidae animals using reaction mixture (10X PCR buffer-1.2μl, MgCl2 (25mM)-1.1μl, dNTPs (2.5 mM)-1.1μl, 10X BSA-1.0μl, forward and reverse primers (5 pmoles/μl)-2 μl of each, taq polymerase (5 units/μl)-0.5μl, milli Q-6.1μl and DNA - 5μl) with standardized PCR conditions (initial denaturation at 940C for 10 min, denaturation at 940C, annealing at 55 0C for 1 min, extension at 72 0C for 1 min, final extension at 72 0C for 12 min and hold at 4 0C for infinity) for 42 cycles. PCR products were electrophoresed in 2.5% agarose gel and then visualized under UV in gel documentation system. DNA amplification for cytochrome b was done using primers L14724 and H15915 [10]. Sequences of 16 srRNA primers were CGC CTG TTT ATC AAA AAC AT and CTC CGG TTT CTC AGA TC. Primers for 12 srRNA were TAT GAG ACA GCT GAA CAA GGG and CTG CAC CTC TTT GGT ATC TGA.

Sequencing: The amplified products were purified using gel elution protocol with purification kit (Bioserve, India) for removing non-specific amplification and primmer dimmers. The amplicons were processed for PCR using a fluorescence based cycle technique with PCR mix [Big dyeTM -1.8 μl, Primer (1pMoles/μl)- 2μl and DNA (Purified PCR Product)-3μl]. The sequencing was done using a capillary electrophoresis method based DNA sequencer.

Results and discussion

After primary cleaning and sterilization with 10% SDS and ethanol, the dissected hair samples were treated with newly prepared buffer MBS in shaking water bath at 560C. DTT reduced the disulfide bonds of proteins and prevented intra and intermolecular disulfide bonds which are formed between cysteine residues of proteins [11]. While SDS disrupted non-covalent bonds of the proteins which denatured them and made proteins free from their native shape (conformation) [12]. Therefore, the negative charge on the protein will become significantly greater than the original charge of that protein [13]. Due to interaction with SDS, the electrostatic repulsion formed that caused unfolding of proteins. Thus, these elimination differences in shape worked as a factor for DNA isolation from hair shafts. The third component of MBS, Proteinase-K, digested and removed proteins from preparations of nucleic acid; it also inactivates the nucleases that might degrade the DNA [14]. Use of MBS resulted a faster and convenient hair lysis by forming a translucent light brown solution. The solution was centrifuged at 10000rpm for 10 minutes through lysep column in a centrifuge tube and then added 100 μl of BTA lysis Buffer into it and incubated for 20 minutes at 760C on heat block. The solution was transferred to sample tube and preceded within the Automate-express cartridge based DNA extraction system using BTA Protocol for DNA binding and elution. DNA extraction from shaded hair shafts using current method have shown significant results in less time as well as better DNA recovery from traces of hairs. Thus, this study imparts a suitable method for DNA extraction from hair shaft with accuracy and higher yield of DNA for forensic examination. In this study, the DNA isolated from two hair shafts of 10mm length of all 60 hair samples where it was obtained a maximum of 32 pg/μL in case of leopard and minimum 6 pg/μL in lion (Table 1).

The DNA yield was measured using by Nanodrop and Flurometer orbit 3.0TM spectrophotometers. The results were found in concordance with both the instruments having slight variations of + 0.1pg/μL. The extracted DNA samples were amplified with standard primers using PCR in standardized conditions. The PCR products were amplified with three different reverse and forward primers of Cytochrome b, 12srRNA and 16srRNA. The Amplicon were visualized by gel electrophoresis in agarose where significant DNA bands were observed Figure 1. The amplicons were further fluorescently labeled and sequenced

in capillary sequencer where the results of the forward and reverse primers obtained individually which edited in SEQUENCE ANALYSIS software (ABI, USA) in FASTA files (Figure 2). These were assembled using codon code and AUTO ASSEMBLER software (ABI, USA) to generate consensus sequence (CS). The consensus sequences were subjected to the Basic Local Alignment Search Tool (BLAST) search in NCBI data base for nucleotides search. These CSs were found to be identical with previously submitted NCBI data which proved validity of our newly developed ERCHL method. The BLAST results for fast minimum evolution, maximum sequence difference tree, lineage report, organism report, taxonomy report are shown in Table 2, which justified purity, integrity and quality of DNA of the specified organism.

Thus, this study provide a ERCHLM for DNA extraction from hair shaft which would be applicable for forensic examination including STR, RFLP, SNP, VNTR and genome sequencing. This method provides DNA from hair shafts which is a strain less and non-invasive method that could be employed in wildlife population genetics and other genetic studies without handling the animal.

Conclusion

ERCHLM provides a new hair lysis and DNA isolation protocol which is more effective than previously reported protocols those are time consuming and have low DNA yield. The method described here constitutes a promising way for non-invasive investigations in DNA analysis for precious, trace samples as well as forensic casework analysis.

References

1. R.E. Bisbing, The forensic identification and association of human hair. In: Saferstein R, editor. Forensic science handbook, Vol. I. Englewood Cliffs, New Jersey: Prentice Hall Regents 1 (1982) 184–221.

2. C.C. Alberts, J.T. Ribeiro-Paes, G. Aranda-Selverio, J.R. Cursino-Santos, V.R. Moreno-Cotulio, A.L.D. Oliveira, B.F.M.M. Porchia, W.F.Santos and E.B.Souza, DNA extraction from hair shafts of wild Brazilian felids and canids. Genetics and Molecular Research. 9 (2010) 4: 2429-2435.

3. E. Jehaes, A. Gilissen, J.J. Cassiman and R. Decorte, Evaluation of a decontamination protocol for hair shafts before mtDNA sequencing. Forensic Sci. Int. 94 (1998) 65-71.

4. A.G. Elizabeth and R.F. David, A simplified method for mitochondrial DNA extraction from head hair shafts. J Forensic Sci, (2005) 50:5.

5. M. Thomas, P.G. Andrew, S. Wilson, B. Michael, A.J. Hansen, E. Willerslev, B. Shapiro, F.G.H. Thomas, M.P. Richards, T.C.O. Connell, J.T. Desmond, C.J. Robert and A. Cooper. Ancient mitochondrial DNA from hair. Current Biology 14 (2004)12:464.

6. B. Forslind and G. Swanbeck, Keratin formation in the hair follicle. Exp. Cell Res. 43 (1966) 191–209.

7. L.A. David and F.P. Andrew, Microvolume quantification of nucleic acids in molecular diagnostics. Thermo scientific nanodrop products. Wilmington, (2004) DE 19810.

8. M.S. Dahiya and S.K. Yadav, Scanning electron microscopic characterization and elemental analysis of hair: A tool in identification of felidae animals. J Forensic Res 4 (2013) 178.

9. M.M. Houck and B. Budowle, Correlation of microscopic and mitochondrial DNA hair comparisons. J Forensic Sci 47 (2002) 5:964–7.

10. T.D. Kocher, W.K. Thomas, A. Meyer, S.V. Edwards, S. Paabo, F.X. Villablanca and A.C. Wilson, Dynamics of mitochondrial DNA evolution in animals: amplification and sequencing with conserved primers. proceedings of national academics of science. USA, 86 (1989) 6196-6200.

11. J.C. Lukesh, M.J. Palte, and R.T. Raines, A Potent, Versatile Disulfide-Reducing Agent from Aspartic Acid. J Am Chem Soc. (2012) 134(9): 4057–4059.

12. H. Helmuth, W. Ulrich and A. Peter, Stimulation of proteinase K action by denaturing agents: application to the isolation of nucleic acids and the degradation of 'masked' proteins. Eur. J. Biochem. 56 (1975) 103-108.

13. D. Goldenberger, I. Perschil, A. Martin and M. Ritzler, A simple "universal" DNA extraction procedure using SDS and proteinase K is compatible with direct PCR amplification. Genome Res. 4 (1995) 368-370.

14. E.A. Graffy, Development and validation of an alkaline extraction method for isolating mitochondrial DNA from human hair shafts (thesis). East Lansing (MI): michigan state univ., (2004).

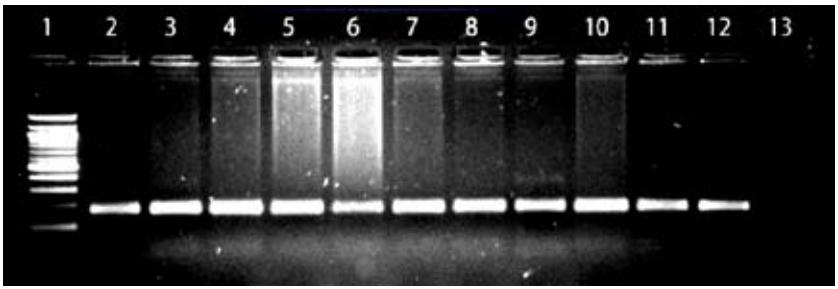


Figure 1. Showing amplified DNA bands in Agarose gel with DNA ladder in well 1, Positive control in well 2 and negative control on well no. 13

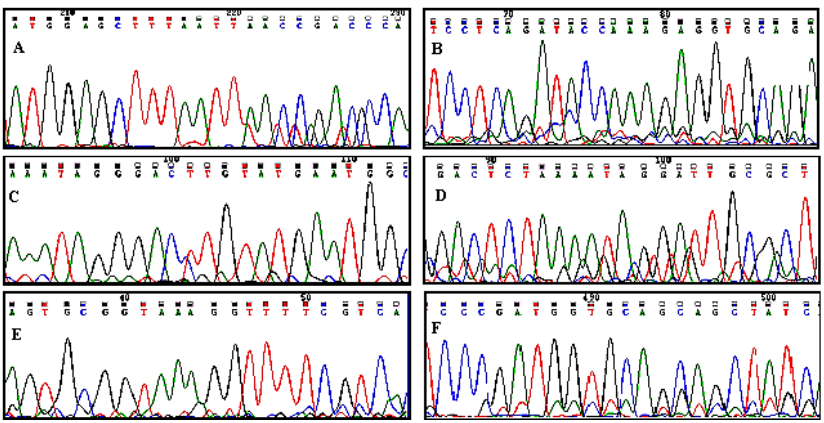


Figure 2 showing DNA sequencing peaks, where A, B, C,D,E and F represents sequencing for leopard 12 srRNA forward primer, leopard 12 srRNA reverse primer, lion 16 srRNA forward primer, lion 16 srRNA reverse primer, tiger 12 srRNA forward primer and tiger12 srRNA reverse primer respectively.

Table No. 1

S. No.	ID No.	DNA (pg/μl)	S. No.	ID No.	DNA (pg/μl)	S. No.	ID No.	DNA (pg/μl)
1	L 1	**10**	21	LE 1	**10**	41	T 1	**11**
2	L 2	**10**	22	LE 2	**11**	42	T 2	**13**
3	L 3	**10**	23	LE 3	**10**	43	T 3	**14**
4	L 4	**10**	24	LE 4	**10**	44	T 4	**12**
5	L 5	**10**	25	LE 5	**11**	45	T 5	**15**
6	L 6	**10**	26	LE 6	**9**	46	T 6	**15**
7	L 7	**20**	27	LE 7	**10**	47	T 7	**10**
8	L 8	**10**	28	LE 8	**14**	48	T 8	**10**
9	L 9	**10**	29	LE 9	**12**	49	T 9	**10**
10	L 10	**9**	30	LE 10	**16**	50	T 10	**10**
11	L 11	**12**	31	LE 11	**15**	51	T 11	**11**
12	L 12	**07**	32	LE 12	**15**	52	T 12	**9**
13	L 13	**10**	33	LE 13	**19**	53	T 13	**7**
14	L 14	**10**	34	LE 14	**15**	54	T 14	**4**
15	L 15	**11**	35	LE 15	**14**	55	T 15	**8**
16	L 15	**10**	36	LE 16	**10**	56	T 16	**19**
17	L 17	**6**	37	LE 17	**7**	57	T 17	**15**
18	L 18	**10**	38	LE 18	**12**	58	T 18	**12**
19	L 19	**11**	39	LE 19	**9**	59	T 19	**10**
20	L 20	**14**	40	LE 20	**11**	60	T 20	**17**

L-Lion, LE- Leopard, T-Tiger

Incorporation of Various Security Features for Protection of Important Valuable Documents

Mohinder Singh*

Keywords

Security Features, Protection, Valuable Documents, Civil Documents, Routine Documents, Security Documents.

Abstract

This paper discusses various aspects relating to preparation and protection of documents like the classification of documents; classification of various types of overt and covert security features available for protection; important features available in valuable documents like Passports, ID Cards etc., besides discussing several security features of 'Indian PAN Cards' analyzed forensically with modern scientific equipments.

Introduction

WE are living in an age of 'Documents', which affect our lives from birth till death. The transition from physical documents to virtual documents has made the situation even more complex. Wherever there are documents, there will be an intention to defraud as even affluent sections of the society take the recourse to short cuts and bye pass the cumbersome procedures with an intention to get rich overnight. No civilized person or the Government can afford to tolerate such corrupt practices and, hence, there is always a need to protect the security and integrity of important and valuable documents so as to thwart any move to defraud.

True value of a document is a relative term and is directly proportional to its utility to any individual, institution, or the Government and

Author Intro:

* Retired GEQD, Central Forensic Science Laboratory, Hyderabad;
E-mail: vermamdr52@rediffmail.com, vermamdr@hotmail.com

resultant gain by their fraudulent misuse to some and loss to others. Therefore, the necessary level of protection also varies accordingly. Obviously, we cannot afford to spend twenty rupees to protect a ten rupee note and cannot ignore to spend a reasonable amount to safeguard a thousand rupee note, because their planned counterfeiting attempts may ultimately lead to cripple the economy of a country.

Classification of Documents

For the purpose of discussion, the important documents which affect our day to day lives may be classified into following categories:

Civil Documents: Birth Registration Certificate, Death Certificate, Marriage Registration/Divorce Certificate etc.

Routine Documents: ID card, Voter ID Card, PAN Card, AADHAR Card, Domicile Certificate, OBC/Caste Certificate, BPL Certificate, Ration Card, Examination Mark Sheets/Degrees/Certificates/Testimonials. Motor Vehicle Registration Certificate, Driving License.

Travel Documents: Passport, Visa, Nationality Certificate, Resident Alien Card, Permanent Resident Card, Naturalization and Citizenship Certificates.

Bank Documents: Cheques, Drafts, Traveler Cheques, DW, Currency Notes, Credit Card, Debit Card, Smart Card.

Security Documents Executed on Stamp Papers: DP Note, Hypothecation/Bank Guarantee etc., Agreement, Property Transfer/ Registration etc.

Judicial Documents: Important Court Orders/Judgments, Laboratory Reports

Commerce Related Documents: Patents & Copy Rights Certification, Logo etc.

Paper-Less or Digital Documents: Electronic Money Transfers Through Websites, Online Transactions, E-Banking Solutions etc.

Classification of Security Features

The security features available for protection broadly fall into following categories:

- **Paper Security Features**
- **Photo Security Features**

– **Printing Security Features**

– **Optical Security Features, like Hologram, Kinegram, etc.**

– **Other Security Features, like Lamination, Binding**

Digital Security Features

Some of the documents like bank cheques and drafts contain simple security features like background security printing and watermarks, whereas other documents like passport contain combination of security features including the optical security features and intaglio printing.

Indian Pan Cards

Security Features incorporated in PAN Cards include print versions that are difficult to photocopy and features like 'Hologram' have been introduced to ensure that the original cannot be duplicated.

The new PAN Card is a superior card and in case of individual applicants it will carry a colored photo image. It is said to be tamper proof and has built-in security features like 'Hologram' and 'U.V. Line'. These security features will thwart forgery of PAN Cards._

Security Features in Current Pan Card

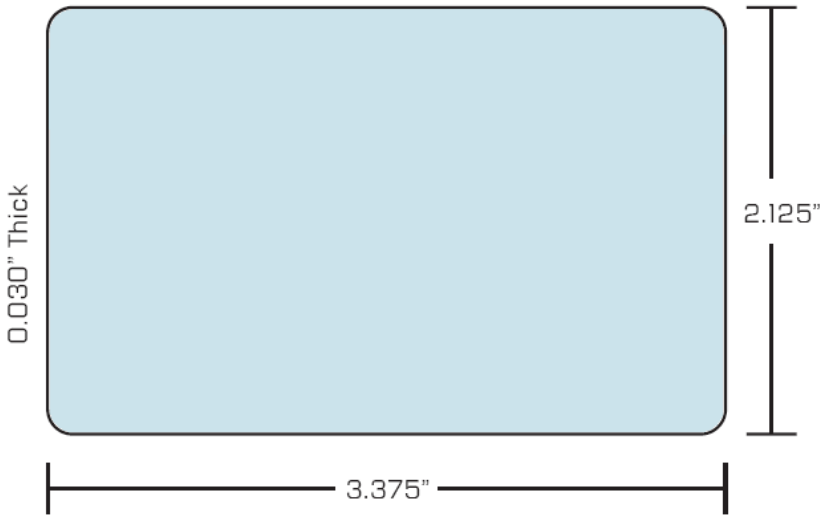
The current PAN card has several security features, which are not easily visible to the naked eye. To study these security features, various scientific instruments have been used, such as hand lenses of various magnification, Stereo Microscope & VSC 2000/5000 (Video Spectral Comparator). On the basis of this study, security features of current PAN Card can be grouped into three categories:

A. Specification of Current PAN Card

It includes a standard format, which was found to have the following general features:

- **Card Material:** It is made up of PVC (Poly Vinyl Chloride), a thermoplastic material, which is cheap, durable & easy to assemble.
- **Card Size:** It has a standard size of CR80/Credit Card based on the specification of ISO 7810.
- **Card Dimension:** It has standard dimensions of 3.375″ x 2.215″ or 85.6mm x 54mm.

- **Card Thickness:** It has thickness of min. 0.030" or 30mil.
- **Printed Matter:** PAN Card is printed with color printing including water mark and overlay lamination. Different types of printing methods including Dye-Sublimation/Resin Thermal Transfer/ Color Inkjet or Comparable Technology appear to have been used for their production.
- **Life Cycle:** It has a life time of 10 years, which is for the card as well as for printing on the card.

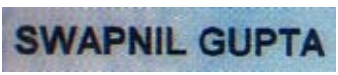


Dimension & Thickness of Indian PAN Card

B. Basic Features of Current PAN Card

It includes some basic features which are related to the particular individual, such as:

- **Name of the Person/Company/Firm:** Name is present on the PAN Card in capital letters on the front left side.

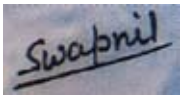


- **Father's Name:** Father's name is present in case of only Individuals in capital letters on the front left side.

- **Date of Birth:** Date of Birth present as DD/MM/YYYY format on the front left side.

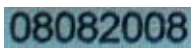
- **Permanent Account Number:** PAN is present as 10 digits alphanumeric format on the front left side.

- **Signature of the Person:** Signature is present as scanned format on the front left side.



- **Photo of the Person:** Photo is present as scanned format on the front right side, which includes facial portion.

- **Issue date of PAN Card:** Issue date of PAN Card is written as DDMMYYYY format on right side of image of the person.



C. Security Features of Current PAN Card

Indian PAN Card also contains some embedded Security Features, which are as follows:

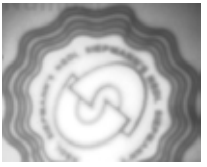
- **Image of Mahatma Gandhi:** A partial image of Mahatma Gandhi can be viewed in the center part of both sides of PAN Card in normal (flood) lighting conditions.

- **Image of 5 Rupee Coin:** A partial image of half part of Indian 5 rupee coin can be viewed on both side of PAN Card in normal (flood) lighting conditions.

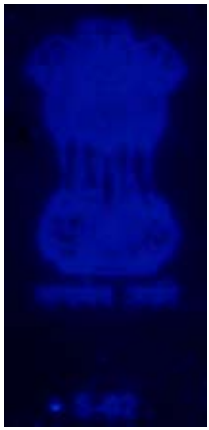
- **Image of Ashoka Pillar Emblem:** A blue colored image of Ashoka Pillar can be viewed on the upper front center part of the PAN Card. "Satyameva Jayate" in Hindi is also written below it. It can be seen under normal (flood) lighting conditions.

- **Hologram:** A Hologram is a 3D image of varying shapes and color depending on the angle at which it is viewed. It is a type of optically variable device (OVD) created by photographic process. A squared hologram can be viewed in the front right corner of the PAN Card. "Bharat Sarkar" or "Bharat Sarkar + Image of Ashoka Pillar + Aaykar Vibhag" can be viewed from different angles of light source. These features can be best seen by Stereo Microscope and VSC 5000.

- **Logo Stamp of NSDL:** A logo stamp of NSDL can be seen the right side where PAN Number is written. It can only be seen under transmitted light of IR region under VSC2000/ 5000.



- **Water Mark of Ashoka Pillar:** Watermark is produced during the paper manufacturing process and is an integral part of the card. The card fibers are made less dense in certain area than others, which allow more light to pass through at that point thereby forming an image. In the PAN Card water mark of Ashoka Pillar can be viewed in UV light under VSC 5000. A special code is also present below the Ashoka Pillar. It is a 3 digit alphanumeric character (i.e. S-02).



Some important features of Indian PAN Card which are resolved under VSC 5000 in different light arrangements like normal light, oblique light, transmitted light, UV and IR etc., are shown below:

Indian Pan Card as seen in Visible Light Under VSC 5000

Indian Pan Card as seen in Infrared Light Under VSC 5000

Indian Pan Card as seen in Ultraviolet Light Under VSC 5000

The Future of Overt Security Features for ID Card Protection

Increasing number of security cards is an ongoing concern for consumers and Governments everywhere. Although a single **'multifunction card'** is more practical than several single—function cards, putting so much information on one card creates an even greater need for security.

Multi-technology cards that offer **'machine readable element's**—with **'contact'** and **'contactless chips'** and **'overt security features'—**are the trend. Because consumers will want direct visual interaction with their cards, **'optical security features'** will remain the standard.

Innovation will involve new ways to combine unique **'color and holographic effects'** to create more highly integrated, harder-to-reproduce images and surfaces.

An Overview of Electronic Passport Security Features

An e-passport supports a combination of electronic and optical security features including watermark, OVD and Hologram. If an e-passport is misused, the immigration check point will be able to detect a mismatch between the printed and the digital information, and authorities can take action against the offender. The International Civil Aviation Organization (ICAO) sets the standards for the e-passports that have been implemented in over 70 countries. Data in the Indian e-passports can be read in other countries as it adheres to the ICAO global standards for biometrics and secure storage of personal data in travel documents.

Electronic Passports include contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution. In its simplest form, an Electronic Passport contains just a collection of 'Read Only' files; more advanced variants can include sophisticated cryptographic mechanisms protecting security of the document and/or privacy of the passport holder.

Optical Security Features

They protect the desired image and offer an effective defense against counterfeiting. These economical and widely used features make attempt that genuine products stay genuine

System for Verifying Security Features of Valuable Documents (Big Patents India)

The invention relates to a system for verifying security features of valuable documents comprising at least one sensor in areas of different security categories. The fabrication/forgery is prevented with particular reliability by virtue of the fact that, according to the security category different sensor parameters are provided for the respective verification of security features in order to verify the same security feature in a different manner.

Machine Readable Passports

- Standardized presentation in which some information appear as strings of alphanumeric characters (rather than full text)

- These characters are printed in a manner that is suitable for 'Optical Character Recognition (OCR)
- OCR is a format that is able to be read by a machine like the characters printed at the bottom of a Bank cheque

RFID Chip

- Contains a duplicate of the information printed on a passport's physical pages.
- RFID Passport is activated when an electronic reader sends it a signal on a designated frequency.
- The chip channels that radio energy and responds back by sending back the passport holder name, address, date and place of birth, and digital photograph.
- A computer chip that uses communication via a radio frequency to uniquely identify an object, such as a 'VISA'

Paper Security Features

Security Fibers

- Cloth or plastic fibers incorporated randomly within the paper of a document. These fibers may appear under normal light as being a different color(s) than the rest of the paper, or under ultraviolet light in various colors.
- A characteristic of security fibers is that they may be detached from the paper with tweezers and are randomly located.
- Forgers often resort to "painting" the fibers onto a document to mimic security fibers, which is normally detected by the 'repeating pattern' of the 'simulated security fibers'.

Planchettes

Small discs placed within the fibers or on the surface of security paper, often in a random manner, during the paper manufacturing process.

They are of various colors and can have a variety of features, such as fluorescence.

They can generally be lifted away from the paper surface by mechanical means, such as 'scrapping' or 'erasure'.

Security Thread

- A plastic or metallic foil strip incorporated within the paper of a document. The thread becomes visible when the page is viewed in 'transmitted light'.
- Because the thread is an integral part of the paper structure, it is very difficult to simulate.
- There are a variety of security threads found in travel documents, such as
  - Multi-colored
  - Fluorescent
  - Micro printed
  - Chemically sensitive
  - Machine readable
  - Windowed
  - Thermo text

Watermark

- A design into paper during the paper manufacturing process by varying the density of paper fibers.
- Watermark designs are an integral part of the paper and become visible when viewed with 'Transmitted light'
- A line watermark consists of text or simple line designs which can be read with 'Transmitted light'
- Watermarks are visible in 'Transmitted light' and not in 'Ultraviolet light' in genuine passports
- A shadow watermark creates an image with light and dark areas of shadowing and is more detailed than a line watermark
- A genuine watermark does not fluoresce when exposed to UV light.

Photo Security Features

Grommet, Rivets, or Eyelets

- Small, circular metal rivets (often made of brass, aluminum or steel), which are
- Used to secure photograph to a passport page or to an ID Card

Ink Seal

- An inked impression which is produced when an inked 'relief surface' is pressed against the substrate.
- Ink seals are sometimes used to secure passports in photographs and frequently used to endorse civil documents.
- The text found on ink seals in passports frequently pertains to the issuing authority.
- The clarity of ink seals are dependent on several factors, including the amount of ink used, the condition of the stamp, the pressure applied when impressed onto the page, etc.

Dry Seal or Embossing Seal

- A dry seal is a seal embossed without ink and may be referred to as an "Embossed Seal".
- The seal's pattern is impressed into the paper (or plastic material, such as lamina) with a mechanical die.
- Stamping an image by hand, without ink, onto the paper or the photograph
- The 'relief' can be felt as well as seen
- The image is produced with pressure rather than ink.
- The text found on dry seals used in passports frequently pertains to the issuing authority.
- Details of the dry seal design and text are generally easier to see when illuminated from the side by a strong light.

Die-Cut Photo

- Photos that are machine cut with uniform, round edges.

Lamina

- A layer of plastic intended to cover and secure a photo and/or data upon a passport page.
- Most contemporary passports incorporate a design within the security film or lamina.

Retro-Reflective Lamina, or the "3m" Confirm Lamina

- A laminate containing patterns made up of tiny glass beads that become visible through the use of a retro reflective viewer, or a flashlight at a 'specific angle.'
- Alterations to the document should result in damage to the retro-reflective designs.
- If a retro-reflective viewer is not available, the examiner can use a flashlight to view the safeguard design.
- In some cases, the forgers have skillfully altered the document with minimal damage to the 3M lamina.
- One disadvantage of the 3M lamina is that due to its opacity, it obscures examination of the background printing.

Integrated Photo

- Process by which the bearer's image and/or personal information details are entered directly onto the substrate.
- The holder's image is not a separate photograph affixed to the page.
- Many contemporary passports, ID Cards, and driver's licenses contain photo images of the bearer which are integrated into the biographical data page or the document itself.
- Digital photographs are designed to be more resistant to alteration than a traditional photograph.

Printing Security Features

Offset Printing

- The biographical page and interior pages of most genuine passports contain intricate line designs in the background printing produced by 'offset lithography'
- In offset printing or offset lithography, ink is transferred from the image plate to the paper by means of an intermediate drum.
- The process uses printing surfaces which are ink receptive and non printing surfaces which are ink repellent.
- As a result, the print appears uniform and consistent.

- Offset printing is frequently used in the **'background printing'** and **'pre-printed data descriptors'** of passports and national ID Cards.

Rainbow Printing, or Split Fountain Technique

- Interior pages of most contemporary passports contain fine line detailing
- The fine line detail of the background printing may comprise of geometric or floral designs, as well as texts.
- High level of print quality can be seen on close examination.

Microline Printing

- Micro line printing is 'very small printed text' which normally requires magnification to be read.
- Micro line printing is normally printed by either 'offset lithography' or 'intaglio'.
- Micro line printing due to its 'size' is often difficult to reproduce with the clarity and detail of the genuine.
- In security documents, micro printing often pertains to the issuing authority or the document itself.

Letterpress Printing

- A printing technique that uses a printing form with a raised edge which is inked and pressed directly onto the paper.
- This results in an 'irregular beaded edge' or characteristic 'ring of ink' around the outside of the printed design.
- In general, the passport numbers on any given biographical data page or on its reverse side, and in the number panel of the currency notes are printed in letterpress.

Intaglio Printing

- The most formidable threat to security documents is from computer technology through scanners and printers.
- An important countermeasure to this threat is 'INTAGLIO PRINTING'. It is a printing process in which the image is etched or engraved below the surface of the printing plate. Ink is placed

in the etched area, the surface (non-image area) is the wiped clean, and with the use of heavy pressure the ink is transferred to the paper.

- Even the most sophisticated scanners are unable to duplicate the **'3 dimensional feel'**
- The thickness of the ink on the paper creates the raised images which can be felt.
- The surface of the note feels slightly raised, while the reverse side feels slightly indented.
- Intaglio allows for very fine details of printed pages and is a **'very expensive process'.**

Latent Image

- A latent image is a **'hidden image'** that lies within another printed feature and is produced using the intaglio process.
- The image becomes visible by holding it obliquely to a strong light source.
- Latent images are most often formed in decorative borders, such as the front and back end-sheets of passports.

Ink Jet Printing

- Ink jet printing is a method of printing created by spraying droplets of inks through computer controlled nozzles.
- It is mostly used for personalization, as it is quicker and cheaper than other printing techniques, e.g., laser printing, although there is great variance in the printing quality.
- Ink jet printing penetrates the paper (substrates) of the document thereby hindering data alteration.
- Counterfeit biographical data pages and poor reproductions of completely counterfeit passports are often imprinted with ink jet printing rather than offset lithography, as it is most cost effective to the forger.

Laser Etching, or Laser Engraving

- The practice of using lasers to engrave to mark an object.

- The technique does not involve the use of inks, nor does it involve 'tool bits' which contact the engraving surface and wear out.
- The term 'laser marking' is also used as a generic term covering a broad spectrum of 'surfacing techniques' including printing, hot branding and laser bonding.
- The impact of laser engraving has been more pronounced for specially designed 'laser able materials', which include laser sensitive polymers and novel metal alloys.
- In 'Slovenian Passport, all of the bearer's information, including photograph and machine readable zone data, are laser etched into the surface of the bio page.
- Additionally, the bio page contains a 'tactile element' (meaning that they can be felt in the card surface). Having both convex (outward curving) and concave (inward curving) printing helps to deter alteration.
- Due to complexity of 'laser engraving technology' and its high cost, most forgers will not replicate these features.
- Examination of the biographical page by **'touch'** and with side light is recommended to determine the presence of laser engraving.

Ultraviolet Security Features

- Most travel documents contain some form of UV-reactive safeguards to hinder tampering of data and photo substitution.
- UV light is a useful tool in revealing the presence of UV-reactive inks in security documents.
- UV light can also be used to reveal un-authorized changes or variation in the base fluorescence of paper which can be caused by bleach or solvents commonly used in un-authorized alterations.

Optically Variable Ink (OVI)

- OVI changes colors when tilted in varying directions depending on the light source.
- Because this process is more expensive than many of the other security features often employed, most often there will be a sole use of this feature in any given document.

Photochromic Ink

- Photochromism is the change in color that certain substances undergo when exposed to irradiation or UV light.
- Photo chromic ink darkens after exposure to UV light.
- After removal from the UV light source, the viewed feature will gradually fade back, reverting to what you would see with normal light.

Other Security Features

Binding

- Passports are often assembled in a manner in which the sheets are divided in half by the binding, which is generally stitched.
- The stitching can consist of one or multiple threads, and can be stitched in several different ways.
- **'The reverse chain stitch'** is the method of binding in the 1998 version of the U.S.Passport.

Uv-Reactive Safeguards in Security Film (Lamina)

- Many passports incorporate security features that become visible under UV light as an additional safeguard.
- As these designs are not visible in normal light, they could be easily overlooked by the forger.

Optical Security Features

Hologram

- A hologram is a three-dimensional image of varying shapes and colors depending on the angle at which it is viewed.
- It is also a type of an optically variable device (OVD).
- Holograms are created by a photographic process and, hence, are iridescent under only a limited number of angles.
- Holographic layer can be applied over printed data to hinder data alterations.

Kinegram or Optically Variable Device (OVD)

- A kinegram is a computer generated image with the distinctive characteristic of not only changing colors and shapes, but appearing to move when held at different viewing angles.
- Kinegrams are also iridescent at almost every angle.
- A kinegram is an optically variable device (OVD).
- An OVD is a design, pattern, or image that changes color or appearance depending upon the angle at which it is held to a light source.

Changeable Laser Image (CLI)

- A multiple laser image (also called a changeable or tilted laser image) is a laser engraved image or text that changes depending upon the angle at which it is viewed.
- Some of the passports incorporate this phenomenon to protect the bearer's photo and/or date of birth, etc.

Image Perf, or Laser Micro Perforation

- It is an additional image which is perforated into some passport biographical data pages and national ID Cards.
- The 'Image Perf' becomes visible when it is held up to a light source or with transmitted light.
- This enhanced security feature has curtailed passport photo substitutions.

Digital Security Features

Digital Watermarking

- A measure of Copy rights protection
- Introduction of visible, partially visible or invisible watermarks, embedded in the document to prevent its fraudulent reproduction

A pattern of bits embedded into a file that is used to identify the source of illegal copies. For example, if a digital watermark is placed into a master copy of an audio CD or DVD movie, then all copies of that disc are uniquely identified. If a license were to manufacture and distribute

them in areas outside of their authorized territories, the watermark provides a trace.

The watermark developer has to find creative ways of altering the file without disturbing it for the user. It is extremely difficult to embed a watermark within an ASCII file, which is just raw text. But it is relatively easy to alter a few bits within audio, video and graphics formats without making a noticeable difference on playback or display.

Hashing

- A method for converting representations of values within fields, usually keys, to a more compact form. An addressing technique that uses keys to store and retrieve data in a file.
- To protect integrity of a document
- Comparison of 'hash value' of source document and target documents to detect any alteration in its contents
- MD5, SHA 256 software are available for hashing

Encryption

- Encryption is a process of translating a message, called the plain text into an encoded message called the cipher text. This is usually accomplished using a secret encryption key and a cryptographic cipher.
- To protect confidentiality of data
- Application software which makes the contents of a document, illegible, invisible or inaccessible to the forger
- Can be decrypted with the 'key / password' which is known to the real owner

Digital Signature

- The digital signature is simply a small block of data that is attached to documents you sign. It is generated from your digital id, which includes both a private and public key. The private key is used to apply the signature to the document, while the public key is sent with the file. The public key contains encrypted code, also called a "hash" that verifies your identity.
- Combination of all the above stated '3' elements

- Software application which protects the 'authenticity, integrity', confidentiality and non-repudiability' of a document

Security Requirements

Criminal acts related to documents which require protection, take many forms, such as-

– Leaking confidential document s
– Tampering with printed documents
– Counterfeiting printed documents

How can printed documents be adequately protected in Offices?

The following aspects needs to be addressed:

– Visibility or non-visibility of security features
– Resistance to photocopying or fax transmission
– Resistance to eradication or alteration of security features
– Distinguishing a true original from a copied version
– Detecting the security element on a fragment of the document
– Duration of the security element for archived printed documents
– Easy integration into the existing document-processing stream
– Machine-readable verification processes for industrial document processing.

Overt and Covert Anti-Counterfeiting Processes

Among specialists, it is commonly agreed that anti-counterfeiting processes can be sorted into two main categories:

- The visible or overt processes.
- The invisible to the naked eye or covert processes

Various companies have added visible security features, such as holograms, embossing, special ink and two dimensional bar codes, onto their packaging. **However, these visible elements offer not only very low security but also require training for effective authentication.** It is interesting to note that various Asian companies offer hologram duplication services at very low prices.

More sophisticated techniques can be found in the field of covert security elements, that is, features not visible to the naked eye and requiring dedicated detection means. The most popular solution is invisible ink, such as ultraviolet ink or infrared ink. To authenticate these inks, a lamp emitting light in the required wavelength range is sufficient. The drawback of these inks is that they can be bought very easily on the market by any one. There are other chemical tracers or ink additives providing counterfeiting security, such as DNA or magnetic tracers.

The problem with such special inks or ink additives is the related logistics and manufacturing procedures, such as press cleaning, temperature and pressure sensitivity, as well as interaction with other chemicals. Although very efficient and effective, their implementation and deployment are quite costly. Authentication on the fly, in the retail space for example, is also difficult. These techniques can be qualified as "analogue or hardware based" because they require additional elements or special substances, and they subsequently have to be managed by the manufacturer in a secured environment.

The Digital Breakthrough

As in other industries, the digital revolution opens exciting new possibilities. Digital technologies can now be used to fight counterfeiting and to track and trace products. These digital technologies are breakthroughs compared to former "analogues or hardware" ones. Instead of being issued by optical, chemical, or biology experts, they are developed by computer software and digital imaging scientists.

Cost Effectiveness of Various Security Features

- There has to be a balance between the degree of utility of a document vis-à-vis the cost of various security features to be introduced
- Some of the security features are more costly than others.
- Irrespective of their cost, introduction of security features is linked again with the relative utility /value of a document.
- Routine documents need routine protection
- Security documents needs higher level of protection

- Balance has to be struck between utility and futility of a document.

Conclusion

There is no single, universal solution to secure a printed document. A combination of overt and covert techniques is required. Any solution will have to be adapted to specifications and various needs, and take into consideration the needed level of protection measured against the cost.

Cost must take into account the generation of the secured printed document in addition to the cost of detection and authentication. This includes in particular the cost of integrating the solution into existing IT processes, as well as specific hardware/software detection systems and their deployment. Further a machine-readable feature is required when large batches of documents have to be processed.

Acknowledgements

The author gratefully acknowledges the assistance rendered by Mr. Swapnil Gupta of CFSL (CBI), New Delhi by way of permission to use some of the processed images of 'Indian PAN Cards' prepared by him for presentation in XXI All India Forensic Science Conference 2010.

References

1. New Security Features in PAN Cards (www.business-standard.com, 7.10.2002)
2. New Biometric PAN Card (www.investmentsandmoney.com, 13.4.2011)
3. Indian PAN Card: What it Contains & What it requires?—S. Gupta, et.al (XXI All India Forensic Science Conference, Dec. 2010, Aurangabad))
4. The future of overt security features for ID Card protection (www.icma.com, Dec 2011/ICMA Card Manufacturing)
5. Indian Passports (www.wikipedia.org)
6. Biometric Passports (www.wikipedia.org)
7. An overview of Electronic Passport Security Features-Z. Riha (www.springlink.com, 2009)
8. Your Biometric Passports can be hacked (Connect-Jaiman Joseph, 6.7.2010)
9. A pain called Indian Passport Office (www.praveens.in)

10. Genuine but Fraudulent-Problems with Indian Passports (www.thehindu.com, 21.4.2011)

11. Wikileaks Cables expose India Visa Fraud Tactics (www.travel-impact-newswire.com, 27.4.2011)

12. Fraudulent Travel Documents, Developed by Forensic Document Laboratory, Immigration and Customs Enforcement, US Dept. of Homeland Security & Antiterrorism assistance, Bureau of Diplomatic Security, US Dept. of State.

13. Aadhar Technology [UIADI] (http://en.wikipedia.org)

14. Critical Threats to UID Security (www.searchsecurity.techtarget.in/news).

15. Security and Privacy Challenges in the UIDAI (http://www.dsci.in/taxonomy/term/308)

16. Counterfeiting Of Rupees 1000 Denomination Indian Banknotes of Mahatama Gandhi Series and their Forensic Examination and Detection—M.C. Joshi (CBI Bulletin, June 2005)

17. Fraudulent Alteration in One Million Euro (Annual Report 2008, Tripura State Forensic Science Laboratory, Tripura)

18. Security Features of Indian Bank Notes (www.rbi.org.in)

19. A New Print Based Security Strategy for the protection of valuable documents and products using Moire' intensity profiles—Isaac Amidror (Proc. SPIE Vol. 4677, p-89-100)

20. Introduction of Security Features in routine Bank Instruments to prevent Frauds— B.A. Vaid et.al (Submitted for publication in CBI Bulletin)

21. Forensic Awareness for detection of counterfeit/genuine Indian Bank Notes of Rs. 1000 denomination— S. Gupta et.al (unpublished article)

22. Accused a master forger, knew all security features (www.expressindia.com, 23.7.2008)

23. Covert and overt protection for valuable documents (ISSA Journal/ Nov 2006,p-32-34)

24. Forensic Watermarking: A Tool for Securing Forensic Case Documents—Nivedita Yadav et. al (XXI All India Forensic Science Conference, Dec. 2010, Aurangabad)

25. The Council of the EU Glossary of Security documents, security features and other related technical terms.(http://prado.consilium.europa.eu/en/glossarypopup.html)

26. Intrinsic Characteristics for Authentication (Authentication News, Sept. 2006, Vol. 12, No.9, P- 2)

27. Towards a paperless society, Dr. Fred Jordan (Keesing Journal of Documents and Identity, Issue 22, 2007, P-8 to 10)

28. Brand Protection with Micro-Dots, Dr. Martin Kutter (http://www.alpvision.com)

29. ePassport: Securing International Contacts with Contactless Chips, G Avoine et. Al [g.Tsudik (Ed.): FC 2008, LNCS 5143, PP. 141-155, 2008].

Death Is Due To Poisning: Negative Viscera Report- Intricacies Thereof

Dr. Abhishek Yadav*, Dr. S.K. Gupta, Dr. Kulbhushan***
Dr. Adarsh Kumar@, Dr. Shashank Punia# and Dr. A.K. Jaiswal$

Keywords

Toxicology, Poisoning, Viscera, Autopsy, Collection, Preservation, Analysis, False Negative Report.

Abstract

The conclusion of cause of death in a case where the death is due to poisoning but viscera report gives negative result, poses a confusion to the autopsy doctor, law and public. The intricacy of failure to find poison in viscera of the individual whose death is due to poisoning is a routine problem in India and the reasons of it are many like delay in examination of the viscera, improper preservation of the viscera, use of wrong analytical techniques, early disintegration of poisons, complete metabolism of poisons in the body, the amount of poison in the viscera being negligible, lack of suitable chemical test for certain poisons, tampering of viscera, and the biggest issue is that only common poisons are tested. The residual analysis of poisons is limited to 10-15 poisons commonly available in the area. The other major killer poisons/chemicals like insulin, KCl, Adrenaline can't be detected in viscera. The salient points covering various aspects of viscera analysis in various Forensic Science Laboratories have been discussed with special reference to the false positive or false negative results and interpretation of viscera report when it is negative in truly positive cases and vice-versa.

Author Intro:

* Assistant Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Ansari Nagar, New Delhi-110029. E-Mail: drayad_in@yahoo.com

** Prof. and Head of Department, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Ansari Nagar, New Delhi-110029.

@ Additional Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Ansari Nagar, New Delhi-110029.

\# Senior Resident, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Ansari Nagar, New Delhi-110029.

$ Chemist, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Ansari Nagar, New Delhi-110029.

Introduction

THE diagnosis of poisoning in the dead is done by [1-4]

- History and Circumstantial evidences
- Clinical records
- Postmortem examination
- Chemical analysis

When a poisoning death case is presented to an autopsy surgeon, the doctor is required to preserve the viscera for chemical analysis to know the nature of poisoning. The facility for the same is being provided by the authorities in the State or Central Forensic Science laboratories (FSL). The viscera boxes are submitted in FSL's on a priority basis depending upon the gravity of the case. The report comes from FSL and the same is being read as such by Section 293 CrPC[5].

The role of the autopsy surgeon is generally limited to preservation of viscera and the cause of death is commented upon only after the receipt of chemical analysis report. When the report clearly detects a poison, the cause of death may be easily opined by the autopsy surgeon. In many cases the viscera report comes negative, or detects the poison in the quantity not sufficient to cause death. This puts the autopsy surgeon in a fix as the police expect him to give cause of death so as to reach a logical ending to the investigation.

When there is no allegation in the case, the poisoning being either accidental or suicidal, and no charges under Indian Penal Code (IPC) are being made out after the investigation, the case is closed by the investigating agency/police even in the presence of negative viscera. The problem starts when there is suspicion of foul play in the case. This generally comes in the cases of murder (Sec 302 IPC), dowry deaths (Sec 304B IPC), rash and negligent act while handling the poison (Sec 304A IPC) and abetment of suicide (Sec 306 IPC). In these types of cases after the negative viscera report, when the autopsy surgeon terms the death as unnatural and due to poisoning, his opinion is frequently challenged by the aggrieved/accused party.

We will have a detailed discussion regarding this problem of False Negative cases emphasizing on the methods used by FSLs, problem in detecting specific poisons, past studies and Court Judgments.

Methods used and Poisons Detected by FSLs in India

Around 50 reports submitted in the Department of Forensic Medicine, AIIMS, New Delhi for subsequent opinion by the police were analyzed regarding the methods and the Poisons tested. The following content is derived from the language of the actual reports:

Methods mentioned were:

CFSL (Kolkotta): Physio-chemical method and chromatographic technique.

FSL (Delhi): Chemical, microscopic & TLC examination, GC-HS (for alcohol), GC-MS.

FSL (Ahemdabad): Standard chemical procedures.

FSL (Chandigarh): Color tests, Chromatograhic analysis, Kozelka& Hine method

CFSL (Hyderbad): Physico-chemical method and chromatographic technique.

Poison's tested: (as mentioned in the FSL's report)

CFSL (Kolkotta): Metallic poisons, ethyl alcohol, methyl alcohol, cyanide, phosphides, alkaloids, barbiturates, tranquilizers and pesticides.

FSL (Delhi): Metallic poisons, ethyl alcohol, methyl alcohol, cyanide, phosphides, alkaloids, barbiturates, tranquilizers and pesticides.

FSL (Ahemdabad): no poisons could be detected.

CFSL (Chandigarh): Common insecticides, volatile, metallic/inorganic, sedatives. Ethyl alcohol, phosphides.

CFSL (Hyderabad): Commonvolatile, pesticides, drugs, alkaloids & metallic.

Generally the viscera reports were found to be positive only for ethyl alcohol, methyl alcohol, phosphides, zinc Phosphide, and aluminium phosphide.

Related Observations and Comments in Hon'ble Supreme Court Judgments

- ***Anant ChintamanLagu vs The State of Bombay* [A.I.R. 1960 S.C. 500][6]**

The accused was convicted under Sec 302 IPC. The autopsy surgeon had found no pathological lesion in the pancreas, the kidney, the liver

and any other internal organ. He gave the opinion after the receipt of the negative Chemical Analyser's report and hospital records that death could have occurred due to diabetic coma. He later admitted in the court that he may have expressed incorrect opinion.

The Hon'ble court observed "if circumstantial evidence is so decisive that the Court can unhesitatingly hold that death was a result of administration of poison (though not detected) and that the poison must have been administered by the accused person, then the conviction can be rested on it".

"What assistance a man of science can give he gives, but it is too much to say that the guilt of the accused must, in all cases, should be demonstrated by the isolation of the poison".

- ***Palinoswamy vs State AIR(1968)*** **[Bom 127, 1968 Cr Lj 453][7]**

If the medical evidence is unable to detect/determine the poison even then the conviction can be recorded if the oral and circumstantial evidence establishes the guilt**.**

- ***Mahabir vs State of Bihar*** **[1972 AIR 1331, 1972 SCR (3) 639][7]**

The accused were convicted under Sec302IPC. The doctor who performed the post mortem examination on the dead body gave evidence that the death of the deceased might have been a natural death. He was declared hostile by prosecution in a case of alleged murder by poisoning. The viscera report was negative.

But still the court observed that "the pathologist's role is secondary and several poisons particularly synthetic hypnotics and vegetable alkaloid groups do not leave any characteristic signs which can be noted on PM." The court decided that mere non detection of the poison does not mean that the death was natural.

- ***Bhupender Singh Versus State of Punjab*** **[1988 AIR 1011, 1988 SCR (3) 409][8]**

The court observed that "The chemical examiner does not, as a rule, give an opinion as to the cause of death but merely gives report of the chemical examination. The report itself is not crucial. The report should normally be forwarded to the doctor who conducted the autopsy.

In poison murder cases (302 IPC), the accused are not acquitted solely on the ground that the prosecution has failed to prove that the accused

had the poison in his possession, and are to be acquitted by the Court taking into account the totality of the circumstances".

- ***Taiyab Khan and Others v. State of Bihar (Now Jharkhand)* [2005 13 SCC 455][9]**

In a case of 304B IPC, it was contended by the accused that the viscera report would have shown whether the dowry death of the appellant's wife occurred on account of consumption of poison. Since the chemical examination report of the viscera was not received, it could not be said to be a case of death by poisoning. The Supreme Court rejected the contention and decided that "Since Section 304-B of the IPC refers to death which occurs otherwise than under normal circumstances, the absence of a viscera report would not make any difference to the fate of the case".

- ***Ananda Mohan Sen and Another v. State of West Bengal* [2007 10 SCC 774][10]**

The autopsy surgeon stated that the unnatural death was due to the effect of poisoning but he would be able to conclusively state the cause of death by poisoning only, if he could detect poison in the viscera report. This Court noted that it was not in dispute that the death was an unnatural death and held that the deposition of the witness indicated that the death was due to poisoning. It is only the nature of the poison that could not be identified. In view of this, the conviction of the appellant under Section 498A, 306 of the IPC was upheld.

- ***Bhupendra Versus State of Madhya Pradesh* [CRIMINAL APPEAL NO. 1774 of 2008][9]**

The autopsy surgeon had given the cause of death as suspected poisoning. The accused contended that in absence of viscera report the death could not be attributed to poisoning. The supreme court observed that "In a case of an unnatural death inviting Section 304-B of the IPC or Section 306 of the IPC as long as there is evidence of poisoning, identification of the poison may not be absolutely necessary. Even when a viscera report is sought for, its absence is not necessarily fatal to the case" and rejected the contention of the accused.

Recent Happening[11]

The Calcutta High Court appointed an amicus curiae or 'friend of the court' to assist it in getting answers related to Viscera preservation and

examination. "What comprises viscera, how long can it be preserved and what is the law governing its examination at forensic science laboratories?". The amicus curiae was told by Experts that a viscera can be preserved only if properly refrigerated. If preserved in common salt water, as it is normally done, the sample will decompose in six months.

The amicus curiae has also cited a Supreme Court order which directs that a viscera should be sent to a forensic science laboratory immediately if poisoning is suspected.

Past Studies

Mohanty et al[12]: The poison was not detected by FSL in 17.8% of poisoning cases. Chemical analysis report showed positive in 94% of cases in first three days of admission. There after chance of detection of poison in routine viscera decreases upto 50%.

Malik et al[13]: No poison could be ascertained in 43% of the cases in final report. It was stressed in the study to attach a toxicological unit with the Forensic Medicine Department so as to expedite the justice.

Pathak et al[14]: The study was done to analyze the role of ante-mortem investigations in diagnosis of death due to poisoning and to find the possibilities by which the results of chemical analysis of viscera can be improved. It was observed that when additional sample of gastric lavage was also sent other than routine viscera of autopsy the poison was detected by FSL report in 83.33% cases. When additional sample of gastric lavage was not sent with routine viscera, poisoning was confirmed only in 53.36% cases.

Reasons for non Detection of Poison in the Viscera[1-4,4,15-17]

- ***Residual analysis only***

The procedure followed in our laboratories is of residual analysis of the poisons meaning the actual poisons in their original chemical form are detected and not the metabolites.

- ***Substances not detected in routine examination***

It is well known that usual routine toxicological screening procedures may not detect hemoglobin like carboxyhaemoglobin, sulphamethemoglobin and methemoglobin, diuretics, solvents, radioactive compounds, antibiotics, non-steroid anti-inflammatory

substances except aspirin and paracetamol, calcium channel blockers and beta blockers.

- ***Lack of Suitable Chemical Tests***

If the specific tests are not performed, some poison may be missed in conventional screening procedures by FSL experts, like Insulin, vegetable poisons, organic poison especially alkaloid and glucosides, bacterial toxins & venoms, potassium Chloride, new substances like busiprone, volatile Compounds like aromatic or halogenated hydrocarbons gases toxic anions like thiocyanate, fluoride and nitrites. Fentanyl may have structural dissimilarity from their drug class prototype and give negative results for that particular group.

- ***Removal of poisons from the body***

The poison has been eliminated from the body due to vomiting, purging. Gaseous or volatile poisoning may be excreted thorough lungs by evaporation. Organic solvent poison gets evaporated during extraction and concentration.

- ***Disintegration of the poison***

The poison is metabolized, detoxified, altered in the body and converts to non-toxic form giving the negative analysis for example detection of phenobarbitone in primidone poisoning, morphine in heroin poisoning, oxazepam in diazepam poisoning, succinylcholine metabolizing to succinic acid and choline. Haloperidol and oxycolone are also rapidly metabolized.

There are many drugs, particularly anesthetic agents containing an ester bond, which are unstable in biological tissues and susceptible to chemical or enzymatic hydrolysis.

The treatment given to patient may also alter the nature of poisonous substance.

- ***Decomposition of the tissues***

It leads to chemical changes in certain poisons. Those poisons are then rendered identifiable by chemical tests e.g. chloral hydrate, sodium nitrite, cocaine, aconite, atropine etc.

Some substances are formed in the tissues by decomposition which gives similar chemical reaction to those obtained from drugs or chemicals such as neurin, muscarin and mydalein. These reactions may misguide the analyst.

Volatile substances may be lost as a result of decomposition. There are some drugs which decompose during storage at 40^0 C like clonazepam, cocaine, isoniazid, methadone, morphine and nitrazepam.

- ***Negligible amount of poison in viscera***

The detection of a highly potent poison with a low lethal dose is difficult.

- ***Difficult Extraction***

The proteinous poisons are rather impossible to extract after absorption in tissues. Similarly, the extraction of water soluble compounds is very difficult. So, they are not detected from tissues by chemical methods of analysis.

Catecholamines like adrenaline gets oxidized when are subjected to atmospheric oxygen. Ascorbic acid and sodium metabisulfite may be used to avoid this by removing oxygen from the preservative solution.

- ***Improper preservation***

Leaking Jars, wrong preservative, insufficient quantity of samples, and wrong material of jars are few factors which interferes with the detection of poison.

- ***Tampering of the viscera***

It may be d`one during preservation and in preserved bottles with vested interests or wrong motive. Addition of strong chemicals like soap, bleach powder or glutaraldehyde alters the results in immunoassay.

- ***False Positives***

Cyanide, ethyl alcohol, ketones and sulphides may be formed from normal tissue components. Although the cyanide so formed is always in trace amounts, but the alcohol produced by advanced decomposition may be upto 30 mg per cent.

Some substances other than the poison may come positive which was taken in the hospital for therapeutic reason like promethazine etc.

Specific Poisons Generally Difficult to be detected by FSL

Thallium[18]

It is difficult to isolate thallium in bodily fluids. The monovalent thallium ion, Tl^{+1}, has properties similar to that of the commonly present sodium

and potassium ions, Na^{+1} and K^{+1} respectively, making identification without a sophisticated instrumental chemical laboratory very difficult. net

Polonium-210[19]

It is a rare and highly radioactive isotope. It is hard to detect because all the radiation remains in the body. A lethal dose could be as little as a few milligrams, which could be administered as a powder or dissolved in liquid.net

Nerium oleander [20,21]

It contains oleandrine glycosides which cross-reacts during the positive results of digoxin immunoassay.net

Snake bites[17]

It is not possible to detect the venom by chemical analysis as the venom is destroyed very fast. The 'no poison' given by the toxicologist rules out the presence of other poisons in the tissues than snake venom. Snake venom is a Protein and cannot be separated from body tissues. Immunoassay method may detect these poisons but this facility is not easily available in all FSL's.

Photolabile poisons[16,17]

Ergot alkaloids, phenothiazines and lysergide are sensitive and get decomposed in the light and are not easily identified.

Heroin[17]

The heroin (Diacetyl Morphine) is very difficult to detect as it is rapidly hydrolyzed to monoacetyl morphine and morphine. Therefore, the samples should be tested for morphine.

Recommendations

- It is practically not possible to undertake test for each and every poison, so the police investigators should be meticulous in their approach. They should also give a brief description of the case highlighting the aspects which may point to the nature of poison consumed. It may include crime scene report, statement of the relatives/friends, recent purchases of medicine/drugs by the deceased etc.
- There should be a designated time frame for the police to deposit the viscera in FSL after Postmortem.

- There should be a separate storage facility for the preservation of toxicological specimens at a desired temperature range in the mortuaries, police station and FSL's.
- Strict operating guidelines should be enforced to preserve vomitus and gastric lavage samples, in the casualty of the hospital/ any medical center where the patient first presents.
- In an admitted case, the blood and urine samples should be collected during the first hours of hospital stay.
- A detailed history, including treatment summary should be provided to the FSL's so as to guide them to run tests for those poisons which are not detected in routine examination.

Conclusion

- The investigating police officers and the supervising senior police officers must have a very clear concept that mere a negative viscera report does not rule out death due to poisoning, as the viscera tests has a lot of limitations and restricted to very few common poisons. It should not lead to the end of the investigation into a death due to poisoning.
- FSL's should clearly specify in their reports the exact name of poisons for which the tests have been conducted.
- The laboratory should mention the fallacies and limitations of the tests in their reports. This will prevent the misinformation to the investigators/ relatives who are generally in the impression that a negative viscera report rules out death by poisoning.
- The FSL must have accreditation, its equipments and methods of analysis should be incorporated in report with the credential of scientist.
- As per judgments of the apex court and the facts described above, the autopsy surgeon should not be deterred by mere non-detection of poison in the chemical analysis of viscera.
- The doctor who has conducted the postmortem examination depending upon PM findings, the medical records, circumstantial evidences and after ruling out any other cause of death can very well give the manner of death as unnatural due to a poisonous substance.

References

1. Matiharan K, Patnaik AK, Editors. Modi's Medical jurisprudence and Toxicology, Section-II. 23rded, 5th Reprint. Nagpur: *LexisNexis*; 2010: p 22-43.
2. Parikh CK. Parikh's Textbook of Medical Forensic Medicine and Toxicology. 6thed. New Delhi: *CBS Publisher's and Distributors*; 1999: p 8.09-8.27.
3. Reddy KSN. The essentials of Forensic Medicine and Toxicology. 29th Ed. Hyderabad: *K Suguna Devi*; 2010: p 454-460.
4. Vij K. Textbook of Forensic Medicine and Toxicology: Principles and Practice. 5th Ed. New Delhi: *Elsevier*; 2011: p 446-447.
5. Criminal Procedure code, 1973. [Internet]. [Cited 2014 Aug 07]. Available From: http://www.vakilno1.com/bareacts/crpc/criminal-procedure-code-1973.html#293_Reports_of_certain_Government_scientific_experts.
6. AnantChintamanLagu vs The State of Bombay on 14 December, 1959. [Internet]. [Cited 2014 Jul 30]. Available From: *http://indiankanoon.org/doc/1813863/* .
7. Mahabir Mandal and others vs State of Bihar on 7 March, 1972. [Internet]. [Cited 2014 Jul 26]. Available From: *http://indiankanoon.org/doc/837400/.*
8. Bhupinder Singh vs State Of Punjab on 6 April, 1988. [Internet]. [Cited 2014 Jul 26]. Available From: *http://indiankanoon.org/doc/51736/*.
9. Bhupendra vs State of Madhya Pradesh on 11 November, 2013. [Internet]. [Cited 2014 Jul 26]. Available From: *http://indiankanoon.org/doc/21549647/.*
10. Ananda Mohan Sen and another vs State Of west Bengal on 16/05/2007. [Internet]. [Cited 2014 Jul 26]. Available From: *http://www.legalservicesindia.com/judgments/may/case_16a_5_07.htm*.
11. Gupta J. HC appoints 'amicus curiae' to help it determine what 'viscera' is and how long it can be preserved. The Times of India. [Internet]. [Cited 2014 Aug 08]. Available From: *http://timesofindia.indiatimes.com/topic/Hc-Appoints-'Amicus-Curiae'-To-Help-It-Determine-What-'Viscera'.*
12. Malik Y, Chaliha RR, Malik P, Jaswal M. Toxicology Unit in Department of Forensic Medicine Emphasis from a Study from North East India. *JIAFM*. 2012; 34(4): 23-27.
13. Mohanty MK, Siddhartha P, Arun M, Menezes RG, Palimar V. Correlation between Postmortem diagnosis and survival time in poisoning deaths. *JIAFM*. 2005; 27(1): 23-27.

14. Pathak AK, Rathod B, Mahajan A. Significance of Gastric Lavage in Viscera of Death Due to Poisoning. *JIAFM*. 2013; 35 (1): 7-9.

15. Giroud C. Mangin P. Drug Assay and interpretation of results. In: Payne- ames J, Busuttil A, Smock W. Forensic Medicine: Clinical and Pathological Aspects. London: *Greenwich Medical Media ltd*; 2003: p 609-622.

16. Sharma V.K. Poisons, viscera analysis, report and its interrelation. *IJMTLM*. 2004; 6(2):49-54.

17. Jaiswal AK, MilloT. Handbook of Forensic Analytical Toxicology. New Delhi: *Jaypee Brother's*; 2014: p450-462.

18. Thallium Poisoning. [Internet]. [Cited 2014 Jul 26]. Available From: *http://chemsee.com/index.php?page=44/* .

19. Harding L, Sample I. Polonium-210: the hard-to-detect poison that killed Alexander Litvinenko. The Guardian [Internet]. [Cited 2014 Aug 08]. Available From: *http://www.theguardian.com/world/2013/nov/06/polonium-210-poison-alexander-litvinenko*.

20. Cheung K, Hinds JA, Duffy P. Detection of poisoning by plant-origin cardiac glycoside with the Abbott TDx analyzer. *Clin Chem.*1989 ; 35(2):295-7.

21. Jortani SA, Helm RA, Valdes R Jr. Inhibition of Na,K-ATPase by oleandrin and oleandrigenin, and their detection by digoxin immunoassays. *Clin Chem*. 1996; 42 (10) 1654-1658.

Notes for Contributors

Editorial Objectives

The journal covers articles of general police interest as well as research papers based on empirical data pertaining to police work. Authentic stories of criminal case successfully worked out with the help of scientific aids and techniques are also published. Only original manuscripts are accepted for publication. Articles submitted to the journal should be original contributions and should not be under consideration for any other publication at the same time. A certificate to this effect should invariably accompany the article.

Areas covered include

Crime, criminology, forensic science, forensic medicine, police organization, law & order, cyber-crime, computer crime, organized crime, white collar crime, crime against women, juvenile delinquency, human resource development, police reforms, organizational restructuring, performance appraisal, social defence, police housing, police training, human rights. Insurgency, intelligence, corruption, terrorism etc.

The Review Process

Every article received for publication is subject to the following review procedures:

1. It is reviewed by the editor for general suitability for publication.
2. If it is found suitable, it undergoes a review process by a member of our Board of Referees.
3. Based on the recommendations of the reviewers, the Editorial Board decides whether to accept the particular article as it is, or seek revision, or reject.

Manuscripts Requirements

The manuscripts should be submitted in duplicate in double line spacing with wide margins. Articles should ordinarily be between 2000 and 4000 words in length. Title of the article should be precise. **Authors should also supply an Abstract of 100-150** words with keywords. A copy of the article saved in floppy/CD in MS- Word may be send in addition. Contributors are advised to be very brief in introducing the subject and devote most of the paper to the main theme. Authors should take care to ensure accuracy of the data and references. Quotes should be cited accurately from the original source, should not be edited and should refer to the page numbers of the original publication. Capitalization should be kept to the minimum and should be consistent. British spellings should be used rather than American. The typed script may please be carefully scrutinized for typing errors before dispatch. A brief autobiographical note should also be supplied including full name, designation, postal address and e-mail address, if any. Figures, charts and diagrams, should be kept to a minimum and good quality originals must be provided. ***At the end of the article a reference list and a short bibliography would enhance acceptability of the contribution***. The contributions can also be e-mailed, in addition to being sent by post.

Copyright

Authors submitting articles for publication must warrant that the work is not an infringement of any existing copyright and will indemnify the publisher against any breach of such warranty. Papers and contributions published in the journal become the legal copyright of the publisher unless otherwise agreed.

Submissions should be sent to:

The Editor, The Indian Police Journal, BPR&D, MHA
Block No. 11, 3/4th Floor, CGO Complex, Lodhi Road, New Delhi-110003. INDIA
E-mail: editoripj@bprd.nic.in,Tel:091-11-24362402, Fax:091-11-24362425,24369825

The Indian Police Journal

Vol. LXII ● No. 1 ● January-March, 2015

BOARD OF REFEREES

Website: www.bprd.gov.in

RNI No. 4607/57

Published By: **The Bureau of Police Research & Development,** Ministry of Home Affairs, Govt. of India,
Block No. 11, 3rd 4th Floor, CGO Complex, Lodhi Road, New Delhi-110003. India and
Printed at : **Chandu Press,** D-97, Shakarpur, Delhi-92 Ph.: 22526936