

# Academy Journal

VOLUME 55 NO 1

- 3**                    **INTERNATIONAL TERRORISM FINANCING**  
**KK Attri (1971:Pun) &**  
**Dr GD Pandey (1981:Pun)**  
Additional Director General of Police (Crime) Punjab  
Inspector General of Police Commando Punjab
- 18**                    **CRIMINAL ABUSE OF THE INTERNET & SOFTWARE PIRACY**  
**Dr SC Agarwal IPS (1973:WB)**  
Inspector General of Police (Training) West Bengal
- 28**                    **INDIAN POLICE SERVICE: A SERVICE TURNED TOPSY-TURVY**  
**Balwinder Singh IPS (1976:AP)**  
Inspector General of Police Andhra Pradesh
- 31**                    **COMMUNITY POLICING - A COMPARATIVE PERSPECTIVE**  
**Meeran Chadha Borwankar IPS (1981:Mah)**  
Deputy Director General YC Academy of Development Administration Pune
- 38**                    **CYBER CRIME: INVESTIGATION & PREVENTION**  
**Dr AP Maheshwari IPS (1984:UP)**  
Deputy Inspector General of Police OPS CRPF Bongaigon Assam
- 42**                    **STRESS IN INDIAN POLICE**  
**M Madana Mohan IPS (1987:MT)**  
Deputy Inspector General of Police (Training) Tripura Agartala
- 47**                    **QUALITY AND COST OPTIMIZATION IN POLICE WORKFORCE**  
**Nawal Bajaj IPS (1995:Mah)**  
Deputy Commissioner of Police, Zone III Pune City
- 53**                    **HUMAN RIGHTS AND CRIMINAL JUSTICE ADMINISTRATION**  
**AM Bhattacharjee**  
Former Chief Justice of High Court, Kolkata & High Court Mumbai

**SVP National Police Academy**  
**JOURNAL**  
**Vol 55 No 1 Jan - June 2003**

**Editor**  
**Aditya Mishra IPS**  
**Assistant Director**

Copyright by SVP National Police Academy, Hyderabad. All rights reserved. No part of this book may be used or reproduced by any means without written permission from the publisher. Neither the Editor, nor the Publisher assumes responsibility for statements of facts or opinions in the papers printed. Authors are responsible for obtaining copyright permissions.

**About the Academy**

The Sardar Vallabhbhai Patel National Police Academy is the premier police training Institution in the country for the training of senior police officers. It was established at Mount Abu on 15th September, 1948 as Central Police Training College. Subsequently, it was named after the 'Iron Man' of India, Sardar Vallabhbhai Patel, whose vision and determination resulted in the establishment of the institution. The Academy was shifted to Hyderabad in November, 1975.

The Mission of the Academy is primarily to prepare leaders for the Indian Police. The Academy also endeavours to be a focal point of Training of Trainers for police training institutions all over the country as well as a centre for research studies on police subjects.

Apart from conducting the basic course for the IPS Officers, the Academy also conducts three regular in-service courses for serving officers of various seniorities, three Training of Trainers courses and several short duration thematic courses.

The Academy rendered yeoman service to the nation during the last 55 years in imparting basic training to IPS Officers and other officers many of whom occupy leadership positions in the country not only in police organizations but in other fields also. The alumni of the Academy include past as well as present Governors of States and several other distinguished personalities. In recognition of its services to the nation the Academy was awarded the President's Colours in 1988.

The regular publications of the Academy include a half-yearly professional journal and a quarterly newsletter. The Academy also publishes, from time to time, books written by the faculty and research scholars of the Academy, besides reading material on varied subjects relating to policing, for basic as well as in-service courses.

**For more details visit NPA web-site <http://www.svpnpa.gov.in>**

To order or subscribe, contact: The Editor, SVP NPA Journal, SVP National Police Academy, Shivrampally, Hyderabad - 500 052. Fax No. 4015179, Tel 4015151-58

**e-mail** : [administrator@svpnpa.gov.in](mailto:administrator@svpnpa.gov.in)  
Published by SVP National Police Academy & Printed at NPA Printing Press, Hyderabad

## **Instructions for Authors**

1. 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.
2. The length of the article should not generally exceed 5000 words.
3. Two copies of the article typed or printed on any type of computer printer in double space with wide margins on good quality paper should be sent. If the articles are typed on computer, a floppy containing the article may also be sent.
4. An abstract of the article in 100-200 words and a brief autobiographical note about the author including full name, designation, postal address/e-mail address should also accompany the article.
5. One copy of the article may be retained by the author as the original article sent for publication cannot be returned.
6. The article should be proof-read and free of corrections.
7. Foot-notes and bibliographical references wherever required should be provided along with the article with proper numbering.
8. References should be cited in the text by using the last name(s) of author(s) and year of publication, using page numbers only in the case of a quote. Multiple citations should be alphabetized. For references with more than two authors, only the first author should be listed, followed by et al. If more than one work published in the same year by the same author(s) is cited, they should be designated following the footnotes, if any. Example of a bibliographical reference: Raj.S (1989) "The Effects of Crime Rates". The SVP NPA Journal, Volume XV No.2 Jan-June,89.
9. A submission to SVP National Police Academy Journal is regarded as a commitment to publish. Submission to other journals under review is not acceptable.
10. The copyright for articles published is transferred to SVP National Police Academy.

### **Editorial Board**

**Ganeshwar Jha**

Director

**Aditya Mishra**

Editor

**Ashish Gupta**

**Renuka Mishra**

**Pullela Murali Mohan**

Chandrasekhar Savitri Sailaja Murali

## ACADEMY PUBLICATIONS

- |     |                                                                                                                                        |               |
|-----|----------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 01. | Management Concepts for Effective Police Admn.                                                                                         | - Rs. 60/-*   |
| 02. | Law of Evidence - by Shri Ahmed Hussain                                                                                                | - Rs. 55/-*   |
| 03. | Custodial Deaths in India ( A Research Study ) -<br>by Shri Sankar Sen, Shri P.S.V. Prasad,<br>Dr. A.K. Saxena                         | - Rs. 75/-*   |
| 04. | The Handbook for Trainers (Practices & Innovations) -<br>by Shri Sankar Sen and Dr. A.K. Saxena                                        | - Rs. 75/-*   |
| 05. | Gallantry Awards - Academy Alumni                                                                                                      | - Rs. 25/-    |
| 06. | Compendium of Supreme Court Rulings on<br>Criminal Law and Police Work - by Shri R.K. Bag                                              | - Rs. 70/-    |
| 07. | Prime Minister's Silver Cup Essay Competition :<br>Prize Winning Essays                                                                | - Rs. 60/-    |
| 08. | Sardar Vallabhbhai Patel Memorial Lectures                                                                                             | - Rs. 80/-    |
| 09. | Professionalism at the Cutting Edge Level -<br>by Shri Subhash Joshi, IPS and Dr. A.K. Saxena                                          | - Rs. 50/-    |
| 10. | First Charge - A handbook for newly promoted<br>and junior Superintendents of Police -<br>by Dr. Trinath Mishra, IPS (Hard bound book) | - Rs. 150/-   |
| 11. | Stress Management In Police<br>by Dr. Anil K. Saxena                                                                                   | - Rs. 125/-** |
| 12. | Gender Issues in Police -<br>by Shri Subhash Joshi, IPS & Dr. Rekha Pandey<br>(Hard bound book)                                        | - Rs. 195/-** |
| 13. | Organised Crime<br>by Shri V.K. Deuskar, IPS                                                                                           | - Rs. 200/-   |
| 14. | Professionalism in the Constabulary<br>by Shri Giridhari Nayak, IPS                                                                    | - Rs. 200/-   |

---

\* 25% discount is offered on the rate

\*\* These books will be sold at 50% discount, if they are purchased for personal use by individual police officers

# INTERNATIONAL TERRORISM FINANCING

KK Attri  
Dr GD Pandey

## INTRODUCTION

Conventional acts of terror may not cost much. However, many of the most feared forms of terrorism, the so-called weapons of mass destruction - biological, chemical and nuclear - can be very expensive to produce and deliver. For example, Aum Shinrikyo, a Japanese cult, put about 30 people and an estimated \$30m into producing the chemical Sarin that was released in the Tokyo subway in 1995. It is for this end that the terrorist organizations devise methods of financing the terror networks.

The ever increasing alliances between terrorist and criminal organizations are posing serious threat to global peace and stability. Neil Pollard, Director of the US-based Terrorism Research Center, describes the extent of

this threat: "If terrorist interaction with transnational crime syndicates is successful enough - especially with narcotics traffickers - the infrastructures of these interactions might be robust enough to provide terrorists with real opportunities for WMD [weapons of mass destruction] proliferation, including the introduction of a weapon of mass destruction into the United States. The implications of such an infrastructure are obvious".<sup>1</sup>

## PART-A

### TERRORISM FINANCING Origins of Financial Support

Terrorist groups co-mingle illicit revenues with legitimate funds drawn from profits from commercial enterprises and donations from willing and unwilling

sympathizers. They tap a range of sources for their financial support. Terrorist groups differ from other criminal networks in the motive behind their crimes. While drug traffickers and organized crime groups primarily seek monetary gain, terrorist groups usually seek non-financial goals, such as publicity for recognition and political influence. Terrorism is a means to these ends. While terrorists do not seek financial gain as a sole end, they need money to attract adherents and to support their activities. Some terrorist organizations also need funds for media campaigns, to buy political influence and to undertake social projects aimed at maintaining membership and attracting sympathetic supporters.

At the outset, difference in the terrorist financing (dealt in part A) and the money laundering (dealt in part B) may be understood. Terrorist financing differs from money laundering in many respects. Ordinarily, criminal activity produces the funds and other proceeds that money launderers disguise so that the funds can be used for legitimate or criminal purposes. Funds that support terrorist activity are generated primarily through fund raising - often through legal non-profit entities, although terrorist groups often obtain some funds from criminal activities as well. Because terrorist activity requires very little money (the September 9/11 attacks on the World Trade Center, the Pentagon and the Indian Parliament are estimated to have cost some half a million dollars and few thousand rupees), the amounts of money that individual terrorist cells or their members seek to disguise is substantially less compared to that laundered by organized crime and drug kingpins. And it is the latter for which anti-money laundering tools were initially created which may not be sufficient in detecting terrorist financing demanding modification of existing laws and regulations. The investigation of terrorism is requiring law enforcement and regulatory officials to use existing

anti-money laundering laws in altogether new ways. It will require stronger international anti-money laundering enforcement regimes in the years to come.

Terrorists typically derive only relatively small sums from the proceeds of traditional illegal activities like robbery, kidnapping for ransom, drug trafficking, extortion, document forgery, currency and merchandise counterfeiting and smuggling. A substantial portion of the terrorists' funding comes from contributors, some of whom know the intended purpose of their contribution and some of whom do not. In this key respect, terrorism financing contrasts with the financing of a drug trafficking network, which obtains virtually all of its funding from illegal activities.

The origins of financial support to the terrorism can be broadly categorized as under:

1. **Illegal trafficking in the drugs** - has emerged as the single easiest and substantial source of the money supply to the terrorist organizations the world over.
2. **Legitimate Commercial Enterprises** - Terrorist groups earn profits from businesses they own (Osama Bin Laden). They also secure donations from sympathetic entrepreneurs.
3. **Social and Religious Organizations** - Since the early 1990s, terrorist groups have relied increasingly on substantial donations from knowing and the unknowing social and religious organizations for financial support. In this key respect the *terrorism financing* contrasts with the financing of a drug trafficking network which obtains virtually all of its money from the illegal activities.

4. **State Sponsors** - Several rogue nations like Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria and Pakistan -have provided material assistance, financial support and other resources to terrorists.

5. **Coercion, kidnappings, protection money and toll taxes in affected areas** - In India North East in particular, Jammu & Kashmir, and Punjab and in the Latin American countries terrorist organizations have thrived on these.

### Indicators of Terrorist Financing

Law enforcement agencies indicate certain activities which could be linked to terrorism. These are:

1. Use of multiple personal and business accounts to collect and funnel funds to a small number of foreign beneficiaries;
2. Deposits are followed within a short period of time by wire transfers of funds;
3. Beneficiaries are located in a problematic foreign jurisdiction.
4. Structuring of cash deposits in small amounts in an apparent attempt to circumvent Currency Transaction Report requirements;
5. Mixing of cash deposits and monetary instruments;
6. Deposits of a combination of monetary instruments atypical of legitimate business activity (business checks, payroll checks and social security checks);
7. Stated occupations of those engaging in transactions that are not commensurate with the level of activity (e.g. student, unemployed, self-employed);

8. Large currency withdrawals from a business account not normally associated with cash transactions;
9. Movement of funds through a “non-cooperative country territory” and
10. Involvement of multiple individuals from the same country or community.

Attempts by governments, therefore, focus to limit the financing of terrorist organizations generally by

1. Eliminating sources of financing, and
2. Reducing the capacity of terrorists to keep, move and launder money around the globe.

### Generation of Terrorism Money

In many developing countries<sup>2</sup> surpluses are generated abroad for the system of compensatory payments to operate. This is done mainly through:

1. Over/under invoicing of imports/ exports whereby the excess foreign exchange released is retained abroad.
2. Bogus imports, false imports, whereby the foreign exchange released is retained abroad for a non-existent import.
3. Through crime, mainly drug trafficking, as the source area, say for opiates lie in the developing countries of Asia.
4. Through commissions or bribes in the context of developing countries. It is seen that when it comes to exports, the commission agents in both the private and government sector are operating on much higher commission levels, say 10 per cent. However, when it comes to imports the commission agents are operating at the level of half a per cent, the balance of the commissions is retained abroad by these commission agents.

5. Through the black market in hard currencies, involving transportation of hard currency. In countries where exchange controls are very stringent the hard currency purchased on the black market generally goes to pay for tourist travels abroad.
6. Through encashment of airline tickets after performing a short leg of the journey. In this case the ticket purchased in local currency is subsequently encashed in the foreign currency.
7. Through tourists whose local expenses are assured and the hard currencies retained abroad by the tour operators.
8. Through other forms of organized crime such as smuggling of antiques, precious stones or trafficking in women, which would lead to the generation of hard currencies that can be retained abroad.
9. Extortions from the local corrupt elements also constitutes an element of terrorist funding. Quite a few sympathizers of the terrorists in Jammu and Kashmir, especially in the Valley, contribute to the terrorist kitty. Jammu and Kashmir banks have also played a fairly dubious role in channeling terrorist funding there.

### WEALTH FOR TERRORIST CRIMES

#### I. Drug trafficking -The Value for Terrorist and Criminal Organizations:

There is an undeniable link between terror groups and illicit drugs. Terrorist organizations in almost 30 countries now finance their activities, to a greater or lesser extent, through illegal drug trafficking. Terror and drug trafficking organizations are linked mutually beneficially by money, tactics, geography and politics and in many instances even by coercion. Drug trafficking has, throughout this century, been an international enterprise and an

international problem. The ever increasing scale of the traffic, the apparent efficiency of organization and sophistication, the fast sums of money involved and the increasing links with transnational organized crime and terrorist organizations constitute a threat which is increasingly serious in both its nature and extent. Illicit drug trafficking now threatens peace and security at both national and international levels. It affects the sovereignty of some states, the right of self-determination and democratic government, economic, social and political stability and the enjoyment of human rights.

Illicit drugs are terrorists favourite tool on three counters.<sup>4</sup>

1. To finance their activity, providing necessary funds, for weapons, explosives and corrupting officials.
2. To undermine the political, economic and social health of the targeted countries/ populations.
3. To use the above factors as examples of social degeneration which warrants necessity of destruction thus allowing new recruits to their ranks.

Internationally, drugs form an important part of the financial infrastructure of terrorist outfits with terrorist outfits extensively involving in following activities; **I. Trafficking** -Al Qaeda, Hizbollah, Basque Fatherland and Liberty, Islamic Movement of Uzbekistan, Kurdistan Workers Party, Palestinian Islamic Jihad **2. Growing** -Abu All Sayyaf Group Couriers -LTTE **3. All aspects expect International Movement**- National Liberation Army, Revolutionary Armed Forces of Colombia, Peruvian Shinning Path, United Self-Defense Forces of Colombia **4. Drug money made available by Government agencies**.- Kashmiri terrorist organizations through Pakistan ISI.

## 2. Factors promoting global drug trafficking

Some of the most important factors are:

1. Endemic corruption and lack of transparency and accountability in the developing countries. Corruption makes it possible for terrorism, drug trafficking and criminal organizations to flourish.
2. Individuals rights'- permissive society - youngsters getting independent financially at much younger age - lack of social taboos and family ties facilitate drug abuse.
3. At the end of the Cold War and weakening of the State-sponsored terrorism in the West, terrorist groups were forced to find alternative means of financing, e.g., Angola, Columbia, Afghanistan, etc. The FARC ( left-wing guerilla group in Colombia) is estimated to generate between \$400 and \$600 million of tax free dollars a year for its coffers through drug trafficking.<sup>5</sup> In Kashmir, the terrorist organizations are getting funded through the Pakistan ISI Controlled narcotic smugglers to the tune of estimated Rs.250 Crores annually.<sup>6</sup>
4. The collapsing communist regimes caused new conflicts in Former Yugoslavia, Azerbaijan - Armenia, Georgia, Chechnya, and Tazakistan, etc. which have led to development of drug trafficking by Central Asian Criminal Organizations.
5. Funded by drug trafficking, the terrorist organizations gain the resources, routes and network to engage in a whole series of criminal activity including illicit arms trade, possible proliferation of chemical and nuclear weapons.<sup>7</sup>

## 3. India and the drugs-trafficking

India is the world's largest producer of the legal opium for pharmaceutical purposes, some of which is reportedly diverted for heroin production. Opium is produced in the states of Madhya Pradesh, Rajasthan and Uttar Pradesh. India serves as a major route for the drugs produced in Afghanistan, Pakistan, Myanmar. The smuggling of acetic anhydride to Pakistan and from the North-Eastern states to Myanmar has been recorded. India, nonetheless, receives the major illicit supplies of the drugs from Pakistan, Myanmar and from Nepal. Most of the heroin transiting through India sells in Europe. The spillover of the drugs 'in transit' has started showing alarming proportions in Manipur and Nagaland, the North Eastern states where it has contributed to alarming spread of the AIDS. India has estimated 1.2 million heroin and 4.5 million opium addicts.<sup>8</sup>

The Narcotic Control Bureau created in 1986 to coordinate among various drug law enforcement agencies of the Central Government and the state Governments also functions as an independent drug law enforcement agency. It also implements the provisions of the International conventions including 1961 Single Convention, the 1971 Convention against Psychotropic Substances and the 1988 Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.<sup>9</sup>

India has bilateral agreements relating to the narcotics with the USA, the UK, the UAE, Pakistan, Afghanistan, Mauritius, Zambia and the Russian Federation.<sup>10</sup> India's anti narcotic efforts are, however, hampered by lack of budgetary support and infrastructure in drug prohibition areas and corruption among police, Government officials and the politicians. India stands on the annual list of US counter-narcotics assistance's major illicit drug producing countries to get the US foreign aid.

## 4. Drug Trafficking-Global Volumes, Price Tags and Profitability

The value of the global trade in illegal drugs is difficult to determine. However, the **United Nations Office of Drug Control and Crime Prevention (UNODC)** estimates that the retail value of the illegal market is \$400 billion *per year*, which would put it ahead of the entire US petroleum industry. *The Economist* magazine suggests that global retail sales are less, probably around \$150 billion annually (In comparison, Canada's annual real gross domestic product for 2001 is about \$650 billion, and the US Department of Defense budget request for 2001 was about \$290 billion). Royal Canadian Mounted Police(RCMP),Criminal Intelligence Directorate Report(1999) estimated illegal drug trade proceeds in excess of 4 billion US Dollars at whole sale and 18 billion US dollars at street level".<sup>11</sup>

UN officials believed that 2,800 tonnes of opium, convertible into 280 tonnes of heroin, was in the hands of the Taliban, the al-Qaeda network of Islamic militants and other Afghan and Pakistani drug lords. On the wholesale market in Pakistan, this harvest could be worth \$1.4 billion. On the streets of London and Milan, processed into white powder, its ultimate value is estimated by Interpol and UN officials at between \$40 - \$80 billion (the annual retail turnover of the European heroin trade is estimated at \$20 billion). UN officials estimate Afghan stockpile as enough to keep every addict in Europe supplied for three years and to allow the Taliban and their allies to dominate the European, Russian and much of the Asian market for another two years. In the Indian subcontinent, the Pakistani narcotic smuggling trade was valued at \$2.5 billion during 1999.<sup>12</sup>

The drug users pay greatly inflated prices (often several thousand percent more) than their cost of



production presenting significant opportunities for terrorist groups to profit from their production or sale.

According to the **United Nations Office for Drug Control and Crime Prevention (UNODC)** value of many drugs at different stages of production and sales in countries of origin and consumption varies from 175 to 1300 times: <sup>13</sup> ( Table )

**5. Illegal Drug Trafficking and International Security**

Narcotics *supply*, has been a subject of diplomacy and international law at least since the Opium Wars between Great Britain and China in 1839 and 1858. In modern times the established links between organized crime, terrorist organizations and their financial prowess, arms dealing and drug trafficking compound the risks to security in individual countries and to the international community. According to the **United Nations International Drug Control Programme, (UNDCP)** “in situations of armed conflict, illicit drug revenues—or the drugs themselves—are regularly exchanged for arms”

The huge profits of illicit drug trafficking “do more to corrupt social systems, damage economies and weaken moral and ethical values than the combined effects of all other forms of corruption. The corrupting reach into government officials, politicians and the business community further endangers the stability of societies and governmental processes, and ultimately threaten political stability and even world order”. If security is defined not only as dealing with external military threats but as addressing challenges to the effective functioning of society, then drug trafficking is much more menacing than many issues that have traditionally been seen as hazardous to security. It poses risks to security at three levels: the individual, the state and the international system of states. This threat is more substantial for “source” states, and “transit” countries, than for consumer countries, but it exists to some degree for all three. The threat is insidious rather than direct: it is not usually a threat to the military strength of the state, but to the governance prerogatives of the Sovereigns that are an integral part of statehood. <sup>14</sup>

**5(1) Narcotics and security in source countries:** The drug trade has serious national security implications for both source and the consumer countries. Countries as Colombia, Mexico, Malaysia and the West Indian have framed their national security doctrines, taking in view the factors of : 1. Political security, 2. Military security, 3. Economic security, 4. Societal security and 5. Environmental security. No such effort has been made in Afghanistan, the world’s largest producer of illicit opium.

**5(2) Narcotics and the political security of states:** Narcotics production and trafficking pose substantial *political* problems in source country governments and states, which are mostly **less developed countries (LDCs)** and possess fragile political, economic and social systems of contested legitimacy. The primary threat to these states is internal arising from development of autonomous producer/trafficker power and authority, which stems from non-political financial and paramilitary power, parallel to and independent of that of the state. In Peru, Colombia, Bolivia and Mexico, rival parallel states exist.

On many occasions, increasing trafficker power in producer/transit states has led to the actual assumption of formal governmental power by the traffickers. Such narcocracies existed in Bolivia between 1980 and 1981 and Panama under Noriega .The regime of Dzhokhar Dudayev with criminal syndicates in Chechnya which controlled the smuggling of most contrabands including Central Asian opium and hashish in the CIS is yet another example. Drug-related corruption has penetrated bureaucratic and political leaderships in both source and transit countries. The best-known cases are Colombia and Mexico. Mexico has been termed a “narco- democracy” by some.

The security threats posed for producer countries by the continuation of the drug trade do not necessarily lead to the enactment of counter narcotics

<b>Opium (All figures in \$ US)</b>	
Farm gate price <i>per gram</i> (Afghanistan)	3.00 to 7.00
Retail price <i>per gram</i> (in Canada)	39.00
Multiple of retail to farm gate price	550 to 1300
<b>Heroin (All figures in \$ US)</b>	
Wholesale price <i>per Kg</i> (Afghanistan: 1996)	2,700
Wholesale price <i>per Kg</i> (W Europe: 1996)	60,000 (22 times Afghan wholesale price)
Wholesale price <i>per Kg</i> (US: 1999)	107,000 ( 40 times Afghan wholesale price)
Retail price <i>per Kg</i> (US: 1999)	475,000 (175 times Afghan wholesale price)
<b>Cocaine (All figures in \$ US)</b>	
Wholesale price <i>per Kg</i> \$400-600,	
Retail price <i>per Kg</i> (US Streets)	110,000(180 to 275 times cost of the coca leaves)

policies by their governments. There are substantial national security risks involved in a vigorous pursuit of a counter-narcotics policy as well. The implicated regimes in Sofia and Managua no longer exist. The US State Department accused Vietnam in the past of involvement in the drug trade. The North Korean regime has been trafficking in narcotics, mainly opium and heroin, since, at least, 1976 when it defaulted on repayment of billions of dollars in international loans. Links between Cuba and Colombian drug barons apparently date back to the 1970s.

**5(3) Territorial Autonomy** - Narcotics producers and traffickers in many source countries have achieved a “state-within-a-state,” affording sanctuary to the illegal drug trade for local strongmen who effectively block the central government from enforcing its writ. Such a situation exists in many regions of the Andes and Amazonia, in the remote border regions of the Southeast Asian “**Golden Triangle**” and the Southwest Asian “**Golden Crescent**”. In Pakistan, opium and heroin production are concentrated in the tribal areas of the remote, mountainous Northwest Frontier Province, where, until recently (1995), local leaders were virtually a law unto themselves, since the government was unwilling to press them for fear of pushing them into open resistance to Islamabad.

**5(4) Narcotics and the external political relations of producer states** - Association with narcotics can seriously tarnish the image of a source country in the international arena. The US, since 1986, by congressional legislation certifies major drug-producing and transit countries as having cooperated “to the maximum extent possible” with its narcotics reduction goals. On the multilateral level, the 1988 UN Convention mandates the application of sanctions for any activity carried out with the intention of participating in drug trafficking.

## **6. Narcotics and the Military security of states**

A major security problem for the governments of source countries is the proliferation of sophisticated arms, communication equipment and ancillary equipment in the hands of narcotics organizations. A growing number of indigenous revolutionary organizations, terrorist groups and insurgents have obtained funds and other assets, arms and military technology, through illegal drug-related activities. Both trafficker and insurgent/terrorist organizations function primarily in remote areas where government control is weak. The extensive collocation of areas of insurgency and those of narcotics production usually provides an incentive to both sides to pursue policies of cooperation, and coexistence. In Southeast Asian ‘**Golden Triangle**’ areas of Burma, northern Thailand, eastern Laos and the southern Yunnan province of China, the insurgents and the traffickers are one and the same. The control of trafficking by the insurgents and the Chinese in the ‘**Golden Triangle**’ is much more direct than in almost all other regions with functional integration. In Southwest Asia, illicit opium cultivation in India is concentrated in the states of Jammu & Kashmir and Uttar Pradesh, where active separatist organizations and political disturbances hamper effective law enforcement. Tamil separatists in Sri Lanka are apparently funding their separatist struggle by trafficking heroin through compatriot networks in Europe and Canada. In Latin America, the operative model for relations between insurgents/terrorists and traffickers is of cooperation. In Eastern Europe traffickers and insurgents in the former Yugoslavia have developed a nexus and the Albanian separatists control up to 70% of the heroin market in the Switzerland, in order to buy arms and support terrorist activity against Serbian authorities in Kosovo and Metohija. Croat nationalists were involved in drug trafficking before achieving independence.

## **7. Narcotics and the economic security of the states**

Drug production and trafficking pose two types of economic threats to source countries. First are those posed by over-dependence for export earnings and foreign currency on commodities whose production and marketing are illegal in most source countries.

## **8. Narcotics and the societal security of the states**

While drug abuse is widely viewed in producer countries as primarily a problem of the “consuming” countries it has become clear that domestic drug abuse has also seriously affected producer and transit countries alike affecting the urban poor, the middle and upper classes.

## **9. Narcotics and the environmental security of the states**

Drug production, and attempts to control it through crop eradication, has caused substantial damage to the environment in producer countries. This is doubly serious, since most drug cultivation occurs in largely underdeveloped, ecologically unique and fragile regions, especially rain forests in South America and Southeast Asia.

## **10. Appropriate Responses and Solutions to the Drug Trafficking**

1. Traditional measures to suppress the production and trade in drugs-crop substitution, money laundering legislation, demand reduction (education and treatment), supply reduction (policing and crop eradication programs), may reduce the flow of drug money to terrorists. For many reasons, programs of crop substitution - encouraging farmers to grow alternative crops and crop eradication with herbicides, etc., have not elicited adequate response.

2. Reducing the supply of drugs through policing has an important role to play. In India, a unique system of Government controlled opium production and processing units exists where all area under illicit cultivation is measured, repeatedly checked till the crop maturity, any surpluses destroyed and the defaulting cultivators dealt under law. Due to this, there are no incidents of Indian origin opium getting caught in any other country.

The United States has a success rate of stopping around 10% of the drugs coming into the country from abroad.<sup>15</sup> The Associated Press reports that the goal of United States was to stop 18 % of the illegal drugs destined for its shores in 2002. The Canadian Customs and Revenue Agency suggested before a Commons committee their enforcement was able to stop about 10% of the \$C7 billion to \$C10 billion annual trade in illegal drugs in Canada.<sup>16,17</sup>

3. Money-laundering legislations have great potential if enforced with vigour. To date, these legislations have not fully succeeded in curtailing the flow of illicit funds to criminal and terrorist organizations. The effectiveness of such measures is often impaired due to corruption in various institutions.
4. Many significant financial transactions do not occur through the banking system and largely remain untouched by money-laundering legislations. *Hawala*, for example, popular in the Middle East and South Asia, moves huge sums of money without leaving a paper or electronic trail.

## PART B INTERNATIONAL TERRORISM FINANCING-LEGITIMATE BUSINESS SOCIO RELIGIOUS ORGANISATIONS AND STATE SPONSORSHIP

The terrorist financing in these broad categories is being widely resorted to by the Islamic world to foster terrorism in the Middle East and the Kashmir. In the past few years there has been a shift of Islamic terrorist influence from the Middle East to Central and Southern Asia. This shift is the result of several factors including fall of the Soviet Union, the Soviet defeat in Afghanistan, the Oslo Accord, and the reconciliation between Israel and the Palestinians to name a few. All this has caused a reentering of Islamic terrorist activity from the Middle East to Balkans-Bosnia, Albania, Kosovo; towards Caucasus-Chechnya and Dagestan and lastly toward Asia-Uzbekistan, Kashmir Afghanistan and the Philippines. The Islamist culture of terrorism spreads from the Middle East and has recently given rise to the '**Suicide terrorism**' in Chechnya and Kashmir.<sup>18</sup>

Exploiting the religious element which is most important in financing of the Islamic terrorist groups and widespread support to Islamic movements and political organizations on political, social and religious issues, the '**Pan Islamic Activism**' now exhibits itself in 'Armed Jihad' in Kashmir and the Chechnya.

The countries such as Pakistan, Iran, Saudi Arabia, Kuwait and Sudan give directly or through official and un official foundations and companies enormous amounts of money to Islamic movements many of which serve as the front organizations for terrorism. In Saudi Arabia and other Middle East countries huge private donations land up with terrorist organizations. The financial transactions cover a variety including direct transfer in the accounts, special couriers, and the financing of a wide

range of institutions for social and educational projects, hospitals, orphans and other humanitarian goals.<sup>18</sup>

### 1. MOVING TERRORIST MONEY- MONEYLAUNDERING

**Laundering the proceeds of crime** - In today's global economy, organized criminals generate huge sums of money from drug trafficking and financial crimes. The efforts of the criminals to disguise the illegal profits of the large scale crime without their being compromised is termed '**Money Laundering**'.

Left unchecked, the money laundering can erode a nation's economy by largely increasing the demand for cash, making interest and exchange rates and by causing high inflation in countries where criminals are doing the business. The siphoning of billions of rupees from the normal economic growth poses a real danger at a time when the financial health of each and every country affects the stability of the global markets.

Tracking terrorist financial transactions is more difficult than following the money trails of mainstream criminal groups. While many organized crime groups are adept at concealing their wealth and cash flows for long periods of time, their involvement in the physical trade of illicit drugs, arms and other commodities often exposes the revenues and expenditures connected to these illegal dealings. In contrast, terrorist actions generally are comparatively inexpensive and their financing is often overshadowed by the larger financial resources allocated for the group's political and social activities. Making it more difficult to uncover the illicit nexus.

Terrorist groups use a variety of means to move and launder their funds including :

1. **Currency Transport** - Cash couriered by operatives is difficult to track because there is no paper trail.

2. **Traditional Financial Institutions** - The international nature of most foreign terrorist groups forces them to rely on banks and other financial institutions.
3. **Islamic Banks** - Banks that operate in line with Islamic law, which prohibits the payment of interest and certain other activities, have proliferated throughout Africa, Asia and the Middle East since the mid-1970s. In most instances, these banks are not required to adhere to a wide range of regulations and are not subjected to regulatory and supervisory scrutiny by bank regulators. They do not undergo periodic bank inspections. While these banks may voluntarily comply with banking regulations and in particular, antimoney-laundering guidelines, there is often no control mechanism to ensure such compliances. Some of the largest Islamic financial institutions now operate investment houses in Europe and elsewhere.
4. **Money Changers** - Money changers play a major role in transferring funds in Asia, the Americas, the Middle East and other regions. Their presence is largest in countries where immigrants work to remit funds to families abroad.
5. **Underground Bankers** - Commonly referred to as alternative remittance systems, such as the Hawala or Hundi, underground bankers are prevalent throughout Asia and the Middle East.
6. **The Offshore** - Financial Centers(OFCs): Offshore financial centers are, in the vast majority of cases, segregated from the traditional banking structure of the jurisdiction. OFCs provide beneficial business and

financial planning options for their clients. These include sophisticated trade financing; estate planning for high net worth individuals; tax mitigation for individuals and corporations; avoidance of exchange controls; liability containment for ships and airplanes; sophisticated insurance management options; investment opportunities that transcend home country marketing regulations; preservation of assets; investment of overnight funds; and freedom from certain home country regulatory requirements. Freedom from certain home country regulatory requirements provide opportunities to those with criminal intent. Some OFCs permit the licensing and registration of “shell banks”- that exist on paper only and do not have a physical presence in any jurisdiction. A principal attraction of the OFCs is often the existence of legal frameworks designed to obscure the identity of the beneficial owner, to promote regulatory and supervisory arbitrage, and to provide mitigation or evasion of home-country tax regimes. This lack of transparency and the ability to engage in regulatory arbitrage, coupled with a concomitant reluctance or refusal of many OFCs to cooperate with regulators and law enforcement officials from other jurisdictions, attract those with both legitimate and illegitimate purposes.

Drug traffickers, terrorists, money launderers, tax evaders and other criminals have found the OFCs a particularly inviting venue in which to conduct and conceal their activity. With the advent of the Internet and other technological advances, funds can be transferred around the globe instantaneously, providing further opportunities to engage in the placement and layering of illicitly gained funds.

## 2. MONEY LAUNDERING TRENDS AND TYPOLOGIES

**Alternative Money Remittance Systems or Informal Value Transfer Systems (IVTS)**, are a family of monetary remittance systems that provide for the transfer of value outside of the regulated financial industry. These systems are known by a variety of names reflecting ethnic and national origins, predominantly South Asian and Chinese. They operate throughout the world, especially in countries with large expatriate populations from Africa and Asia. Included, among others, are such systems as hawala (India), hundi (Pakistan), fei ch'ien (China), phoe kuan (Thailand), hui k'uan (Mandarin Chinese), ch'iao hui (Mandarin Chinese) and nging sing kek (Cantonese Chinese). Most of these systems pre-date the emergence of modern banking and other financial institutions. The Colombia Black Market Exchange can also be characterized as a form of alternative remittance system.

**(I)The Hawala System:**<sup>19,20</sup> The hawala continues to be a key factor in money laundering and financial crimes and terrorism associated with South Asia, and now the world. It is used in both the huge “underground” economies of the region and is also widely used in everyday transactions involving legitimate commerce. Hawala has been called “the poor man’s banking system”. Of late, the use of hawala was increasingly noted in terrorist financing investigations. Moreover, because of changing immigration patterns, the use of hawala is no longer confined to South Asia but has spread around the world. Hawala money transactions were recorded in assassination of Rajiv Gandhi, Indian Prime Minister and the 1993 serial blasts in Bombay where hawala operators in UK were involved.

Hawala operates on trust and connections. In fact “trust” is one of several meanings associated with the word hawala. Customers trust hawala operators or “hawaladars” to use their

connections to facilitate money movement or more accurately transfer value around the work. The system is generally much more rapid and inexpensive than traditional banking. The transactions are often based on the trade of a commodity such as electronics or gold. Fictitious, under-or-over-invoicing are often used to “balance the books”. The actual hawala records often in codes provide little paper trail. Most hawala networks which are based on ethnic and family ties are very difficult for law enforcement to penetrate.

Hawala accounts for more than 30-50 percent of the black economy in the South Asia. Dubai in the United Arab Emirates has often surfaced as the conduit for hawala transfers involving India, Pakistan, Afghanistan, Somalia and other countries in the region. The hawala transactions are almost always associated with money laundering since it provides for effective means of money placement and consequent money layering.

The factors favouring hawala are:

1. Cost effectiveness over other institutional means of remittances of money.
2. Efficiency- Hawala transactions are complete in a day or two compared to the delays in the banking.
3. Reliability - Complex international transactions involving one or more banks/institutions have potential to be problematic.
4. Lack of the Bureaucracy - In hawala, the requirement to go to the banks renders it quite amicable for the client.
5. Lack of proper trail - No records are kept Hence privacy of the transactions is assured.
6. Tax evasion - Hawala provides a security free remittance system meticulously avoiding the authorities.

### **Some additional factors rendering hawala lucrative are:**

Hawala competes with other means of the remittances being integral part of the existing business dealings 2. Hawala has low overhead hence cost effective 3. Hawala operators offer favourable exchange rates luring the customers 4. Hawala has added advantage of trust reassuring the customer of fast and advantageous money delivery.

### **Indicators of hawala**

The complexities of the hawala transactions and variations make it nearly impossible to layout a straightforward guide for spotting hawala. Some indicators, however, are:

1. Most consistent and valid indicator is ‘**significant deposit activity**’ usually in the form of cash/cheques often in the name of primary account holder.
2. Certain businesses are also more likely than others to be involved in hawala. Following is a starting point: Import/Export, Travel and related services, Jewellery (gold, precious stones), Foreign Exchange, Rugs/Carpets, Used Cars, Car Rentals ( usually non-chain or franchise), Telephones/Pagers.

Laws in India, Pakistan and other countries make it difficult to convert foreign currency. Criminal activities in these countries may often involve foreign currency (especially dollars), which pose something of a problem. A ‘solution’ that has been seen to this problem is the shipment of these negotiable instruments from South Asia to the United States. Even though such shipments may violate both courier policies and U.S. law, the money launderers accept these risks rather than try to attempt to place these instruments into their local economies.

Any solution must also address the underlying causes of hawala in South Asia such as severe foreign exchange restrictions, inefficient and costly banking channels, and tax and duty policies.

### **Hawala channel for funding terror**

One of the most important sources of terrorism funding in Kashmir is through the hawala. The hawala route is being used to send money by the ISI and Islamic fundamentalist groups in ‘**Organization of Islamic Countries**’. Hawala funding is done through a network of Hawala dealers which extends all the way to Delhi, Mumbai and other places in India. Many of these hawala dealers have genuine wholesale/retail businesses as fronts or they are using such businesses as fronts to divert money to Jammu and Kashmir militant groups. It has been reported that the Kashmiri carpet dealers are under-invoicing their exports to Islamic countries and the balance of the under invoiced value of the carpets is coming into India through the Hawala route.

Legal over invoiced remittances to educational institutions are another source of terrorist funding. For eg. money received by the Jhelum Medical College where the cost of building was inflated and the differential proceeds were passed off to the terrorist groups.

In the recent past a number of Madrasas have come up in Jammu and Kashmir and in other parts of India, especially in northern UP, receiving legal funding from the ‘**Organization of Islamic Countries**’. Money for terrorists is also coming in through porous Indo-Nepal border.<sup>3</sup>

**Black Market Peso Exchange System:** The Black Market Peso Exchange System (BMPE) is a trade-based system that depends on commercial traffic between the U.S. and Colombia to launder profits from the sale of illegal drugs in the United States. The

BMPE is a significant money-laundering conduit used by Colombian narcotics traffickers in repatriating revenues to Colombia. The BMPE is estimated to launder \$3 - \$6 billion annually in the USA.

To combat the BMPE, the U.S. Department of Treasury instituted an inter-agency working group for enhanced coordination of anti-BMPE investigations and successful prosecutions under **Treasury's outreach programs** and guidelines were issued to help U.S. importers and exporters identify BMPE-related transactions and institute protective measures. In addition to domestic outreach efforts, the United States, Colombia, Panama, Venezuela and Aruba formed an international working group of experts to combat this money laundering system.

The BMPF Multilateral Working Group for Panama, Colombia, and the United States recommended (2001) to improving international cooperation through the design and implementation of standardized recording and reporting of international shipments to facilitate information exchange between governments, screening and regulation of free trade zone merchants and operators, efforts to educate international commerce merchants to the risks of trade-based money laundering and methods to combat it. The Multilateral Group also recommended conducting studies of economic, social, political and/or legal issues to find comprehensive responses to problems. The multilateral Working Group is expected to reconvene in 2003 to review progress in implementing these recommendations.

**Lawyers/Notaries, Accountants and Other Non-Financial Professionals:** United States law enforcement authorities have observed that as money laundering schemes become more complex, the perpetrators

turn to the learned expertise of attorneys, accountants, consultants and agent representatives to aid them in the movement of illegal currency. These professionals, using 'shell' corporations, nominees and fictitious records, devise elaborate paper trails to disguise the true source of illegal income. Similar efforts are required in several other countries.

**The Market for Gold and other Precious Metals :** Gold is known to play a significant role in international money laundering. Gold, just like certain currencies (e.g., the U.S. dollar, Swiss Franc and British pound, the Euro) is a nearly universal commodity for international commerce. Gold has been a key medium of exchange since antiquity and remains nearly immune to the consequences of changing global fortunes.

Gold serves as both a commodity and, to a lesser extent, a medium of exchange in money laundering conducted in Latin America, the United States, Europe and Asia. In this cycle, for example, gold bullion makes its way to Italy via Swiss brokers. There it is made into jewelry, much of which is then shipped to Latin America. In Latin America, this jewelry (or the raw gold from which it was made) then becomes one, if not the most important, of the commodities in the black market peso exchange.

**Use of Traveler's Cheques to Disguise Identities :** Criminals may be using traveller's cheques as a money-laundering tool. Although , traveler's cheques can be the preferred mechanism for conducting large business transactions in some countries, the use of traveler's cheques can offer the opportunity to co-mingle illicit funds with legitimate funds. Mexico, Nigeria, Israel and a number of East Asian countries have been frequently cited as the point of origin or negotiation for instruments involved in this type of activity.

**Pre-paid Telephone Cards as Cover for Money Laundering :** Phone card sale businesses routinely generate significant legitimate cash flow. Information reported by financial institutions to FINCEN shows problematic transactions suggestive of money laundering or other illicit financial activity such as large and unexplained cash flow increases or transactions structured to stay below CTR reporting requirements associated with illegitimate use of these businesses. Additionally, law enforcement information suggests the use of phone cards may be a possible mechanism to launder illicit funds.

## **2. Money Laundering Countermeasures - Institutional Mechanism in USA <sup>21</sup>**

**1. National Money Laundering Strategy:** US Congress passed the Money Laundering and Financial Crimes Strategy Act of 1998 to develop a national strategy for combating money laundering and related financial crimes. The **2001 National Money Laundering Strategy** identified five goals: (1) focus law enforcement efforts on the prosecution of major laundering organizations and systems; (2) measure the effectiveness of anti-money laundering efforts; (3) prevent money laundering through cooperative public-private efforts and necessary regulatory measures; (4) coordinate law enforcement efforts with state and local governments to fight money laundering throughout the United States; and (5) strengthen international cooperation to combat the global problem of money laundering.

**The 2001 Strategy** mandated that the **HIFCA task forces** become operational and conduct investigations designed to result in indictments, convictions, and seizures, rather than focus primarily on intelligence gathering. HIFCA Task Forces are composed of, and draw upon, all relevant federal, state and local agencies. The Departments of

Treasury and Justice jointly supervise the HIFCA Task Forces and the 2001 Strategy primarily tasks the **Federal Law Enforcement Training Center (FLETC)** and **Justice's Asset Forfeiture and Money Laundering Section** to develop and advanced money laundering training program to enhance the HIFCA Task Forces' ability to investigate sophisticated money laundering schemes.

The strategy also seeks USA remove all barriers to foster **international cooperation**, and to review extradition and mutual legal assistance

relationships those are keys for money laundering investigations and prosecutions and to recommend that coverage of money laundering offenses be considered an important objective in assessing US, Government priorities for future treaty negotiations. The 2001 Strategy sets as its goal increased use of the international asset-sharing programme, which provides an incentive for international cooperation. Further, the feasibility of establishing model international financial task forces to plan and coordinate significant multilateral money laundering investigations be examined.

**2. U.S. Suspicious Activity Report System (SARs)** plays a critical role in U.S. anti-money laundering efforts. Similar types of reporting throughout the world are key to global efforts to combat money laundering. US Treasury Department issued final regulations, in December, 2001 mandating that money transmitters, issuers, sellers, and redeemers of money orders and traveler's checks must report suspicious transactions to the Treasury Department. The principal focus will be to ensure that law enforcement fully utilizes reported information. The 2001 Strategy requires that law enforcement agencies using SAR information evaluate the usefulness of this information and provide FinCEN with operational feedback. FinCEN will use the feedback to increase the usefulness of reported information to law enforcement agencies.

The aggregate totals of U.S. SARs help illustrate the nature of illegal proceeds and relative scale of the problem. The following statistics provide aggregate totals for SARs filed by depository institutions (i.e. banks, thrifts, savings and loans, and credit unions) since implementation of the U.S. SAR system in April 1, 1996 to April 30, 2001.

**3. Broker-Dealers in Securities Suspicious Activity Reporting:**

During 2001, Treasury's Financial Crimes Enforcement Network (FinCEN) issued a proposed rule that "leveled the playing field" by requiring securities brokers and dealers to file suspicious activity reports in connection with customer activity that indicates possible violations of the Bank Secrecy Act.

**4. Reduce the threat of money laundering posed by foreign correspondent banks:**

The USA has started implementing the **'International Money Laundering Abatement and Antiterrorist Financing Act - 2001**

<b>SAR Filings</b>						
Number of Filings year wise						
	1996	1997	1998	1999	2000	2001
Subtotal	52,069	81,151	96,521	120,504	162,714	59,866
Total Filings						572,825
Chart 2: Frequency Distribution of SAR Filings Suspicious Activity wise (April 1,1996 -April 30,2001.)						
Violation Type	1996	1997	1998	1999	2000	2001
BSA/Structuring/Money Laundering	21,655	35,625	47,223	60,983	90,606	31,980
Bribery/Gratuity	94	109	92	101	150	60
Check Fraud	9,078	13,245	13,767	16,232	19,637	7,933
Check Kiting	2,902	4,294	4,032	4,058	6,163	2,497
Commercial Loan Fraud	583	960	905	1,080	1,320	393
Computer Intrusion	0	0	0	0	65	62
Computer Loan Fraud	1,190	2,048	2,183	2,548	3,432	1,391
Counterfeit Check	2,405	4,226	5,897	7,392	9,033	3,072
Counterfeit Credit/Debit Card	391	387	182	351	644	378
Counterfeit Instrument (Other)	291	294	263	320	474	171
Credit Card Fraud	3,340	5,075	4,377	4,936	6,275	2,358
Debit Card Fraud	261	612	565	721	1,210	516
Defalcation/Embezzlement	3,286	5,252	5,252	5,178	6,117	2,137
False Statement	1,880	2,200	1,970	2,376	3,051	818
Misuse of Position or Self Dealing	952	1,532	1,640	2,064	2,186	735,
Mysterious Disappearance	1,216	1,765	1,855	1,854	2,225	728
Wire Transfer Fraud	302	509	593	771	972	467
Other	4,836	6,675	8,583	8,739	11,148	4,719
Unknown/Blank	1,539	2,317	2,691	6,961	6,971	2,900

pursuant to the **USA PATRIOT Act (2001)**. The Act concerns how financial institutions could make sure that their correspondent accounts were not being used to move proceeds directly or indirectly from foreign “shell banks.” The IMLAATF Act, has advantages of collective knowledge and expertise of various government agencies and departments, and also facilitates the consultation requirements of the Act itself.

### **5. Evaluation and Accountability:**

The 2001 Strategy seeks to institutionalize systems to measure the success of money laundering enforcement efforts and results to provide law enforcement with an accurate picture of its anti-money laundering programmes. Measured evaluation will allow for the identification of money laundering “hot spots,” indicate areas where law enforcement must enhance or prioritize its investigation and prosecutions and allow law enforcement to articulate measurable goals. Treasury has convened a high-level working group to consider the establishment of standardized reporting procedures for each federal law enforcement agency involved in money laundering investigations and prosecutions.

### **6. Legislation**

An aggressive anti-money laundering attack requires that law enforcement utilize all available statutory authorities to dismantle large-scale criminal enterprises. A variety of anti-money laundering proposals were contained in Title III of the USA PATRIOT Act(2001). The anti-money laundering provisions of the USA PATRIOT Act addressed various deficiencies in current money laundering laws and enhanced criminal money laundering enforcement and asset forfeiture capabilities. A number of inter-agency task forces are working to implement the various provisions of the USA PATRIOT Act.

### **7. International Emergency Economic Powers Act (IEEPA):**

International Emergency Economic Powers Act is the principal tool to study terrorist financing. It authorizes the US President to impose trade and financial sanctions to deal with a threat.

### **8. The Anti-Terrorism Act:**

The US Anti-terrorism Act provides authority for two additional sanctions programs targeting terrorism. It prohibits both material support, such as funds, false identifications and safe houses, to designated foreign terrorist organizations and financial transactions with state sponsors of terrorism.

### **9. United Nations Participation Act :**

The United Nations Participation Act (“UNPA”) gives the President the authority to impose economic sanctions to implement mandatory provisions of UN Security Council Resolutions.

### **10. Bank Secrecy Act:**

This Act now also applies to the non-bank financial sector that may be used by terrorists, informal funds transfer businesses like hawalas are required to register with the Department of the Treasury. All non-bank financial institutions such as brokers and dealers in securities and casinos have been brought under its purview.

### **11. The Foreign Terrorist Asset Tracking: Center (FTAT)**

The center is dedicated to identifying the financial infrastructure of terrorist organizations worldwide and curtailing their ability to move money through the international banking system. It represents a preventative, proactive and strategic approach to using financial data to target and curb terrorist funding worldwide.

### **12. Financial Crime-Free Communities Support Program.** The 2000 Strategy announced the launching of the

Financial Crime-Free Communities Support (C-FIC) Program. The C-FIC program is the result of a legislative mandate to establish a federal grant programme to provide seed capital for emerging state and local anti-money laundering enforcement efforts.

### **3. TREATIES, AGREEMENTS, AND OTHER MECHANISMS FOR INFORMATION EXCHANGE**

**1. Mutual Legal Assistance Treaties (MLATs):** allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners.

To facilitate the ongoing exchange of information to combat money laundering, U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) has fostered information exchange with other financial intelligence units (FIUs) around the globe, as well as, on a case by case basis, with law enforcement and regulatory agencies of foreign governments.

### **2. Asset Sharing**

Pursuant to 18 U.S.C. 981(i), 21 U.S.C. 881 (e) (1) (E), and 31 U.S.C. 970(h) (2), the United States is authorized to share assets with countries that facilitate the forfeiture of criminal proceeds. Under this authority, the Departments of Justice, State and Treasury have aggressively sought to encourage foreign governments to cooperate in joint investigations of drug trafficking and money laundering, offering the possibility of sharing in forfeited assets.

### **Multilateral Activities**

**3. Financial Action Task Force (FATF)** The Financial Action Task Force on Money Laundering (FATF), established at the G-7, is an inter-governmental body is international standard in dealing with



the money laundering with the purpose of development and promotion of policies, both at national and international levels, to combat money laundering.

The Task Force was given the responsibility of examining money-laundering techniques and trends, evaluating counter-money laundering measures and recommending measures still needed. In 1990, (revised in 1996) FATF issued 40 recommendations to fight money laundering. These were designed to prevent proceeds of crime from being utilized in future criminal activities and from affecting legitimate economic activity. The revised recommendations (2001) reflect new trends in money laundering and recommended establishing 3 working groups as below to address those areas considered most crucial:

**Working Group A (Customer Identification)**- This working group addresses all issues relating to customer identification.

**Working Group B (Corporate Vehicle)**- This working group addresses questions relating to the transparency of corporate vehicles such as corporations and trusts.

**Working Group C (Gatekeepers)**- This working group addresses questions.

FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. In performing these activities, FATF collaborates with other international bodies.

In order to combat terrorist financing, after September 11 attacks, FATF expanded its mission beyond money laundering to focus its energy and expertise on the worldwide effort to combat terrorist financing. During its extraordinary plenary meeting in

Washington, DC on October 29-30, FATF agreed to the following Eight Special Recommendations on Terrorist Financing for its members:

1. Take immediate steps to ratify and implement the relevant United Nations instruments.
2. Criminalize the financing of terrorism, terrorist acts and terrorist organizations.
3. Freeze and confiscate terrorist assets.
4. Require financial institutions and other entities subject to anti-money laundering obligations to report suspicious transactions links to terrorism.
5. Provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.
6. Impose anti-money laundering controls on alternative remittances systems.
7. Require customer identification measures on international and domestic wire transfers.
8. Ensure that entities, in particular non-profit organizations, cannot be misused to finance terrorism.

**4. Non-Cooperative Countries and Territories (NCCT)** In response to the G-7 Finance Ministers 1998 Birmingham Summit, FATF formally created the Adhoc Group on Non-Cooperative Countries and Territories (NCCT). In 1999, this group developed 25 criteria by which to determine those jurisdictions undermining the global effort to combat money laundering. These criteria encompass four broad areas:

1. Loopholes in financial regulations,
2. Obstacles raised by other regulatory requirements,
3. Obstacles to international cooperation,
4. Inadequate resources for preventing and detecting money laundering activities.

#### **4. UNITED NATIONS: GLOBAL PROGRAMME AGAINST MONEY LAUNDERING(GPML):**

The United Nations Office for Drug Control and Crime Prevention (ODCCP)<sup>22</sup> created the Global Programme against Money Laundering (GPML) in 1997 in response to the United Nations mandates against money laundering. GPML is the focal point for issues related to money laundering and proceeds of crime, providing technical assistance to States to upgrade countermeasures to meet international standards. GPML is the only technical cooperation body with a global mandate to deal with money laundering. It is an active partner of international organizations working in this field, such as the Financial Action Task Force (FATF), the International Monetary Fund, the World Bank, the Commonwealth Secretariat and Interpol. It also works closely with regional organizations and regional development banks.

The general thrust in the area of technical cooperation is assisting legal, financial and law enforcement authorities in developing the necessary infrastructure to fight money laundering. Specific initiatives are built around awareness-raising, institution-building and training. GPML uses its highly successful mentorship programme to provide sustained assistance over periods ranging from 6 to 12 months. Research activity focuses on adding to the body of information on money laundering issues, the maintenance and improvement of databases, the analysis of specific aspects of money laundering and the provision of logistic support for technical cooperation activities including practitioner tools and training materials.

GPML is also the coordinator of the International Money Laundering Information Network (IMoLIN), which includes global databases of anti-money

laundering registration and analysis. The programme administers IMoLIN on behalf of the United Nations, FATF, Interpol, the Commonwealth Secretariat, the Organization of American States, the Council of Europe and the Asia-Pacific Group on Money Laundering.

Key to GPML assistance of expertise and other assistance in the establishment, development and maintenance of Financial Intelligence Units (FIUs). FIUs are the central national institutions for receiving and analyzing reports of financial transactions linked to criminal activity. The programme does much of this work in conjunction with the Egmont Group, the international umbrella body for FIUs.

To prevent and dismantle the financing of global terrorism, the Interpol works to fill the void in coordination of operational activities and to acquire a proactive role in combating the financial flows linked to terrorism. Interpol is also working to determine the structure and operations related to money laundering. The Interpol General Secretariat, has been recently reorganized creating a **Public Safety and terrorism sub-directorate** as part of the **'specialized crimes directorate'**.

Anti-money laundering is a dynamic field, with changing techniques, technology, jurisprudence and policy approaches at the national and international level. GPML activities will continue to be structured to take into account current circumstances, thus remaining responsive to the changing needs of Member States and the international community.

## CONCLUSION

**G**lobal terrorism is now funded differently as compared to its funding mechanism 25 years ago. Terrorists now use complicated networks which are not specific to them only. Globalization and other new technologies have created

beneficial opportunities for them as well. In addition, completely legal donors can fund terrorist groups through perfectly legitimate looking charity donations that ultimately reach terrorist hands.

The real obstacle in way of targeting the terrorist financing is the lack of international cooperation. The 'UN International Convention for Suppression of the Financing of Terrorism' is signed only by 25 countries including India. With the international decline in the state sponsored terrorism (barring Pakistan), the international cooperation should be easier to come since national political interests and considerations towards certain states no longer exist. Terrorism is global in nature; international cooperation is an essential component of any enforcement strategy. After Sept 11 attacks 27 countries have taken steps to implement US led anti terrorist actions, while another 27 are acting on UN Security Council Resolution 1333. USA is working closely with other G-7 countries in the fight against the financing of terrorism.

In addition to role played by the G-7 countries, efforts are also afoot to implement multiphase action plan to combat terrorist financing in China, Russia, India, Saudi Arabia, Pakistan, Indonesia, Egypt, the Netherlands, the Philippines, Spain, Argentina, Brazil, Bahrain and Kuwait under the auspices of the UNO.

## BIBLIOGRAPHY AND NOTES

1. Neal A. Pollard, "Terrorism and Transnational Organized Crime: Implications of Convergence," (Terrorism Research Center). Website: <http://www.terrorism.com/terrorism/crimes/html>.
2. Jyoti Trehan, "Underground and parallel Banking Systems", *Journal of Financial Crime*, 76-84, vol 10(1), 2002.
3. Jyoti Trehan, "Terrorism and the funding of terrorism in Kashmir", *Journal of Financial Crime*, 201-11, vol 9(3), 2002.
4. Dr. Rachel Ehrenfeld, *Center for Study of Corruption and the Rule of Law, Manhattan, New York in "Narcoterrorism"*, (2001) website.
5. Ralf Mutschke, "The Threat Posed by the Convergence of Organized Crime, Drug Trafficking and Terrorism", statement before a hearing of the US House of Representatives Committee on the Judiciary Subcommittee on Crime, December 13, 2000. Mr. Mutschke is the Assistant Director, Criminal Intelligence Directorate, International Criminal Police Organization- Interpol-General-Secretariat. website. <http://www.house.gov/judiciary/muts1213.htm>.
6. Jyoti Trehan, in "Peace in the New Millennium", ed. Air Commodore Jasjit Singh, pp83- 9(2001), Knowledge World, 5A/12, Ansari Road, Daryaganj, Delhi.
7. Raphael F. Perl, "Organized Crime, Drug Trafficking and Terrorism in a Changing Global Environment," Statement before the US House of Representatives Judiciary Committee, Subcommittee on Crime, December 13, 2000. Mr. Perl is a Specialist in International Affairs with the Foreign Affairs, Defence and Trade Division, Congressional Research Service. Website: <http://www.house.gov/Judiciary/per11213.htm>.
8. Congressional Research Service, - CRS web
9. Drug Law Enforcement Training Compendium, Vol I Narcotics Control Bureau, India, PP 19-21 (1997).
10. *ibid*, P2.
11. "Survey: Illegal Drugs: Stumbling in the dark," *The Economist*, July 28, 2001.
12. "Another powder trail", *The Economist*, October 20, 2001.
13. *Global Illicit Drug Trends, 2001*, pp210-11
14. Joshua S. Krasna, "Narcotics and the National Security of producer States", web site

15. "Caribbean Drug Traffic up 25%, US Says", "Baltimore Sun", October 20, 2001.
16. House of Commons Special Committee on Non-Medical Use of Drugs, testimony of Mr. Mark Connolly, the Director General of Contraband and Intelligence Services Directorate, Customs Branch, Canada Customs and Revenue Agency, October 1, 2001.
17. "Getting to them through their money," *The Economist*, September 27, 2001: "Some money generated by criminal activities, notably drug trafficking, has been grabbed by the authorities. The amounts, though, are tiny in comparison with all the world's illicit money. The International Monetary Fund reckons that the amount of dirty money being washed through the financial system is huge: between \$500 billion and \$1.5 trillion a year - equivalent to up to 5% of gross world product."
18. Reuven Paz, "Targetting Terrorism Financing" Paper presented in the International Conference on Countering Terrorism through enhanced International Cooperation", Courmayeur, Mont Blanc, Italy, 22-24 September, 2000.
19. Patrick M Jost and Harjit Singh, "The Hawala alternative remittance System and it's role: Interpol website, also, Patrick M. Jost "Black Hawala, Financial Crimes and the World drug trade" in Jayasurya, Indian Law Institute/UNDCP International Conference on Global Drugs Law, New Delhi, 20th February (1997).
20. Malhotra Angelina, "India's underground bankers", Asia Inc., Online/Asia, Inc.
21. International Narcotics Control Strategy Report-2001, Bureau of International Narcotics and the Law Enforcement Affairs, March 2002, US Dept of State. **Category Designations on the Offshore Financial Services: Offshore Banks:** Mostly the "shell banks" having no physical presence in any jurisdiction. **Trust and Management Companies:** These are companies that provide fiduciary services, as well as serving as marketing agents, representatives, lawyers, accountants, trustees, nominee shareholders, directors, and officers of international business companies. **International**
- Business Companies (IBCs) & Restricted Companies:** Numbers are significantly underreported. **Bearer Shares:** Share certificates can be issued without the name of the beneficial owner **Asset Protection Trust (APTs):** Trusts that protect assets from civil judgment. **Insurance and Re-Insurance Company Formation:** Sells "Economic Citizenship" A practice well advertised on the internet, if improperly controlled can enable bad elements to purchase citizenship in an OFC jurisdiction that may not have an extradition agreement with the purchaser's original home country. **Internet Gaming:** Licenses granted by jurisdictions that enable grantees to establish "virtual casinos" on the Internet, in which customers can pay via credit card. **membership in International Organizations** may exist in fictitious names.
- +22. UNDCPP- Countering Money Laundering (2002), website

## **Believe in Yourself**

**Once there were two friends, a mynah and an elephant. One day the elephant said: "You know, all my life I have wanted to fly. I have always dreamt of what fun it would be to fly over the village and look down at the houses and people, to glide over the river and jungle. Do you think I can fly?" "Sure you can", said the mynah. Reaching back with his beak, he pulled a feather from his tail. "Here", he said, "take this feather and hold it firmly in your mouth. Then flap your ears as hard as you can and you will fly."**

**The elephant did as he was told. He put the feather in his mouth, flapped his ears as hard as he could and, lo and behold he began to fly. Holding the feather tight in his mouth, he flew over the village. He looked down at the people, he glided over the river and over the trees. He did things he had never done, saw things as he had never seen before.**

**When at last he glided back to earth, he ran to meet his friend, guarding the feather carefully with his trunk. "Mynah, you've changed my whole life," he said, "I really can't thank you enough for this feather."**

**"That feather?" said the Mynah. You didn't NEED that. I just gave you something to BELIEVE in. It was your flapping of your ears that did it, NOT the feather !**

from the collections of **pullela murali mohan**

# CRIMINAL ABUSE OF THE INTERNET & SOFTWARE PIRACY

Dr SC Agarwal

## OF INTERNET ADDICTIONS AND CYBER AFFAIRS

**I**n the last five years, the growth of Internet connections, Cyber-Cafes and usage patterns among Indians have increased manifold. More and more surfers spend about 8 – 12 hours in the “**Net Space**” (**Cyber World**) as against the “**Meat – Space**” (**Real World**) and these people are called “**Net – Junkies**” “**Internauts**” and even “**Cyber-Maniacs**”.

This Internet addicts, spend increasing number of hours surfing and spend decreasing number of hours for work, family, etc. The American Psychiatric Association calls this as **Internet Addiction Disorder (IAD)** and **IAD** is now recognized as a **Diagnosable**

**Physio-Psychological Disorder**. These Cyber addicts give up sleep, marriage, social life and almost anything, in order to be with the Internet surfing, engaging in Cyber Chats in varied Chat Rooms where some are called “**married and flirting**”, etc. They speak a different language, have absolutely no social life, families find them strange and friends feel they are different. This virtual infidelity makes men to ignore wives, thereby, making them ‘**Cyber-Widows**’.

One interesting aspect is that, Internet addicts go through the same process of any other addiction, like alcoholism or drug addiction. When removed from ‘Internet’ they suffer “**withdrawal symptoms**” like drug addicts have distress, pre-occupation, anxiety, fantasy, etc. They again use the net to avoid withdrawal symptoms.

In order to come out of IAD, there are Online Cyber Psychologists and even Online De-addiction Clinics [eg. Ksy@netaddiction.com].

## **INTERNET FRAUD**

**I**nternet fraud is an emerging threat that will increase significantly in the coming years, albeit from a low base. The huge growth in the Internet population and e-commerce will provide for fraud, with sharp pushing being a particularly simple and effective means of defrauding innocent investors and making large sums of money. Compared with the totality of fraud, however, the significance of Internet fraud should not be over-stated. Poorly designed and controlled electronic payment systems would pose a serious risk to law enforcement efforts to counter money-laundering operations. Software piracy is a boom business. The experience of the Software industry is likely to be a harbinger of the troubles ahead for the phonographic and video industries. E-mail harassment will increase as Internet usage grows. Paedophiles are using the Internet to disseminate child pornography, to market videos and magazines for commercial sale, to promote opinions seeking to rationalize and legitimize sexual fantasies about children and sexual encounters with them, and to solicit children.

However, certain threats are emerging and there is merit in taking suitable preventive steps now to avoid having to deal with a greater problem at a later date. Government, law enforcement, industry and users all have a roll to play in ensuring that the 'Information Highways' do not become a seductive environment for criminals.

Widespread use of secure encryption will curtail opportunities for certain kinds of 'Computer Crime' – it can be used for secure storage of information (anti-hacking), to protect intellectual property (anti-piracy), and to prevent defrauding of firms and

individuals. Unfortunately, secure encryption will also help organized crime, paedophile rings and other criminals to communicate without risk of detection.

Internet based attacks on e-commerce sites provide a 'wake-up' call to the Forensic Scientists. Unidentified attackers, many a times, have demonstrated the fragility of the system and (quite possibly) our digital infrastructure by crashing major sites. The message therefore is simple: it's time to be enlightened. There is no such thing as fool proof computer and information security. The computer based proprietary information is vulnerable to loss and theft, even our most guarded Atomic secrets might have been compromised. It is simple use of readily downloadable software programmes designed to ambush any on-line site on the Internet; simply point and click and the user can transmit a tidal wave of data aimed at a particular site, which will cause it to crash. Using certain basic techniques, it is possible to even to identify of the attacker.

## **CONSUMER FRAUD & INTERNET FRAUD**

**I**n general, the same types of fraud schemes that have victimized consumers and investors for many years before the proliferation of Internet use are now appearing on-line. We may find many fraud schemes in chat rooms, e-mail, message boards, or on Web Sites.

## **TELEMARKETING FRAUD**

**F**raudulent telemarketers typically use false and misleading statements, representations, and promises when offering you goods and services, investments, or asking you to donate funds to charitable causes.

## **IDENTITY THEFT AND FRAUD**

**I**dentify theft and identity fraud are crimes in which someone obtains and

uses another person's personal information in some way that involves fraud or deception, typically for economic gain.

Internet has 65 million subscribers around the world, and the membership is daily growing. It has created instant person-to-person and organization-to-organization communication across national frontiers. It brings information, education and entertainment into homes and work-places. It has vastly facilitated business and financial transactions, fostered advertising, and helped businessmen, banks and financial institutions to serve customers anytime anywhere. As a result, firms, companies, banks and corporate houses; retailers and wholesalers; government, public and private organizations; and individuals are registering sites on the WWW (WORLD WIDE WEB), the multimedia part of the NET.

NET, as part of the Information Technology, promises to be a powerful engine for economic growth in the 21<sup>st</sup> century; and to enrich an average man's life by improving its quality dramatically. However, most people see only this bright, beneficial side of the INTERNET. Few know, or care to know, its baneful aspects.

## **CYBER CRIME IN INDIA**

**C**yber Crimes have become a reality in India, too. Indian Airlines was defrauded to several lakhs of rupees, by tampering with the Computerised booking records. In the arms drop case of Purulia, the main players used Internet for the International communication, planning and logistics. Computer hackers have also got into the Bhaba Atomic Research Centre (BARC) Computer and pulled out data. Some Computer professionals who prepared the Software for M. B. B.S. Examination altered the data and gave an upward revision to some students in return for a hefty fee.

A sample of few other cases being investigated in India include the following: A loss of 1.39 crores to a nationalised bank where the Computer records were manipulated to create false debts and credits; a loss of 2.5 lakhs due to computerised creation of false bank accounts in another nationalised bank. In another case, a MTNL official manipulated Computer terminals by reversing the electronic telephone meter systems, thereby allowing some companies to make overseas calls without charges.

Technology empowers and does so universally. The benefits of such empowerment reaches criminals too. Cyberia (or) Cyberspace can be defined as a system made up of millions of people who communicate with one another through computers. It is just not the people who make up the Cyberspace but it includes the information stored on millions of Computers world wide accessible to others through telephone lines and other communication channels, that make up Cyberspace.

The Cyberspace or the Internet is a complexity in itself and the most identifiable part is the World Wide Web [WWW]. This consists of web pages which can be used with a web browser. E- mail is another component which is a user-friendly communication device. Internet Relay Chat room (IRC) is another component, which allows real time chatting among thousands of people. The Internet also comprises the Gophel, similar to the W W W, but more for an academic purpose. The File Transfer Protocol (FTP) allows the transfer of files from one Computer to another. According to the available statistics, the number of Personal Computers (PCs) per thousand persons in India is about 2 .8. In the year 2002, it is estimated to be about 10 per thousand.

The table given below gives details of the various types of crimes

concerned with computers and Internet, that happened globally, in 1998.

TABLE

S.No.	Type	Percentage
1.	Virus contamination	27.0 %
2.	Notebook theft	24.0 %
3.	Insider Abuse of Net Access	12.8 %
4.	Telecom Fraud	6.9 %
5.	Unauthorised Access by insider	6.7 %
6.	Theft of Proprietary Information	5.8 %
7.	Financial Fraud	5.3 %
8.	Sabotage	4.5 %
9.	System Penetration by outsider	3.5 %
10.	Spoofing	1.0 %
11.	Active wire tapping	1.4 %
12.	Telecom eves dropping	1.1 5

Since India has the best software professionals, Computer experts feel that, India will also have the best hackers. In due course of time, it is probable that frustrated programmers who realise that they cannot earn good money in writing programmes will slowly shift into hacking.

CYBERCRIME is largely an unexplored frontier for the police in India. Either they are unaware of, or apathetic to, this menace looming on our horizons. However, the threat is already at our doorsteps and is likely to become the biggest white-collar crime in the 21st century. In the USA, the computer crime is increasing at 35% annually and the cost is estimated to be \$3.5 billion.

CYBERCRIME is largely an unexplored frontier for the police in India. The author has described several types of crimes committed on the INTERNET. The Indian Police is not trained and equipped to detect and investigate the cyber crime. Therefore, the police personnel should be familiarized with

these new white collar-crimes. An active liaison between major software firms and police would be mutually beneficial. Policemen can acquire computer literacy through these firms, whereas the latter would learn from the police. The details of reported cyber crimes thereby refining their counter-action strategy and tactics.

### SPECIFIC TYPES OF CYBER CRIMES

The types of cybercrime noticed so far are :

- Financial fraud
- Breach of security of the State, and of Government and private organisations
- Pornography and public indecency
- Paedophilia and enticement of youth
- Harassment and intimidation
- Gambling
- System /data damage
- Virus contamination

### FINANCIAL FRAUD

Defrauding financial institutions and banks is a major cybercrime. It is estimated that, in the USA, an average bank robbery by means of computer yield \$560,000, whereas a robbery by traditional bank hold-up costs \$19,000. The Times of India reported (November 4th, 1995) that the Securities & Exchange Commission of the USA had got frozen the assets of a woman, Renate Haag, who was running a racket of selling bogus securities via the INTERNET, in which people had invested over \$1 million. In 1996, a gang armed with a laptop computer broke into the security code of a US-based City Bank in St. Petersburg, Florida, and moved more than \$10 million to overseas accounts. The crime was detected before the money was lost (The Hindu, April 21st, 1996).

Bank and financial institutions move huge amounts of cash each day electronically, and the biggest fear is that criminals may use the INTERNET's E-cash facility to commit fraud and amass wealth. The INTERNET also holds a great lure for money launderers. This developing threat is causing concern to law-enforcement agencies in the USA and other developed countries, as it would render obsolete the traditional methods of tracking tainted money that rely mainly on the policing of bank transactions. The enormous potential of this crime could be gauged from the fact that the annual turnover of money earned by criminals through illicit drug trade, prostitution, financial fraud, gambling and other criminal activity is an estimated \$500 billion.

#### **BREACH OF SECURITY OF STATE AND OF GOVERNMENT, PUBLIC AND PRIVATE ORGANISATIONS**

Studies show that terrorists or other adversaries could seize control of defence information systems and seriously degrade the nation's ability to deploy and sustain military forces. Since then, the threat has escalated. The Wall Street Journal (February 27th, 1998) reports that the FBI is investigating a "fairly heavy" series of attempts to break into US Military computer systems.

Breach of computer security in the private sector, too, deserves attention. In a recently published book, 'Computer Crime', the British National Computer was quoted as observing that 80% of British private organisations had suffered breaches of computer security in the past ten years, and each security breach cost a company \$20,000. How a high-tech prowler can damage the security of an organisation through the INTERNET was dramatically revealed in the court case against Kevin Mitnick, who in 1994 broke into the well-guarded personal computer of Tsutomu Shimomura, a computer security expert at the San Diego Supercomputer Centre in California. With Shimomura's help, the

FBI eventually caught Mitnick, who is now serving a 22-month jail term. Shimomura revealed that the thief electronically controlled his computer for an entire day and stole a number of his security programmes. The Reader's Digest (January 1998) has published a fascinating account of this crime. Mitnick will soon face another trial on various charges, including possession of unauthorised passwords, computer fraud and illegal interception of wire communications.

#### **PORNOGRAPHY AND PUBLIC INDECENCY**

Today, one can access on the INTERNET smutty photographs, films, and sounds; order a variety of sex toys; engage in lewd and erotic chat; and fix appointment with willing partners. A study was conducted in 1995 by a research team of the Carnegie Mellon University, Pittsburgh, Pennsylvania. Titled "Marketing Pornography" on the Information Superhighway, it reported that, in a 18-month research, it found on the INTERNET, 9,17,410 sexually explicit pictures, descriptions, stories and films of naked women, paedophilia, hebephilia, sadomasochism, urination, defecation and sex with animals. TIME magazine cited (July 3rd, 1995) the case of a 10-year old boy in new York, who, while surfing the INTERNET, got a file in the E-mail with instructions on how to download it. Not able to understand its content, he called his mother, who was horrified to see on the computer screen smutty pictures of sex, including lesbianism and sodomy. Rober Thoman, a youth operating an on-line pornographic service in California, was jailed in 1995 for three years for transmitting obscene images by computer, including those of incest and women having sex with animals. The Mumbai police registered an offence in 1997, when Star Dust magazine published a nude picture of actress Pooja Bhat, which had been downloaded from the INTERNET. The biggest danger is that

these 3-D images, pictures and films are being projected to kids and teenagers, who, being emotionally immature, can develop perversions and unhealthy desire for obscenity and smut. The INTERNET is an even more dangerous medium than the television, as it brings into homes the interactive presence of voices and images, depicting humans engaging in explicit or perverted sex or erotic conversation. An article in The New York Times calls the INTERNET "a garbage heap of pornography, of lewd exchanges of crazy ranting." (The Asian Age, October 18th, 1997). The USA has been so alarmed over cyberporn that the US Congress enacted the Communications Decency Act last year, which prohibited the posting of "indecent" material over the INTERNET. The Act was, however, overturned by the Supreme Court on grounds of violating freedom of expression.

#### **PAEDOPHILIA & ENTICEMENT OF YOUTH**

Paedophilia, transmission of child-pornography images and making sexual assignations are a particularly alarming online activity. Newsweek reported (July 3rd, 1995) the case of a 13-year old Kentucky girl found in Los Angeles after being lured by a cyberpal. Middy, a Mumbai daily, reported (July 23rd, 1995) that, of the 8,00,000 children reported missing in the USA in 1994, abduction was facilitated in about a dozen cases by computer. After investigating child pornography on America On-line, a major computer service on the INTERNET, the FBI raided numerous places and arrested several persons in September, 1995. The FBI probe found that Online computer networks were rapidly facilitating individuals to share child-pornography or entice children into illegal sexual relationship. The Asian Age (February 12th, 1998) reports the arrest of a man in the USA, who would post on the INTERNET photographs of having sex with his own daughter. The accused has

been charged with sexual exploitation of a child and child pornography.

## **HARASSMENT AND INTIMIDATION**

**T**he INTERNET is exploitable for violating privacy and facilitates personal harassment. Once a person registers a Web-site, his privacy can be invaded. A sender of obscene E-mail letter can identify female recipients by the first names figuring in e-mail address. The Indian Express (February 10th, 1995) reproduced an article from the Independent, London, detailing this problem faced by women in England. In an article titled Invasion of Privacy in Time Magazine (October 13th, 1997), the writer described how a hacker seized his telephone line through the NET and invaded his privacy for six months. He writes: "He could have sabotaged my credit rating. He could have eavesdropped on my telephone conversations or siphoned off E-mail. He could have called in my mortgage, discontinued my health insurance or obliterated my Social Security number".

## **GAMBLING**

**C**yper-gambling is a growing on-line activity. As the INTERNET transcends national boundaries, gambling laws can be evaded by setting up computer operations in a neighbouring country without such laws or tolerant of their transgressions. For instance, a Canadian has opened a site, INTERNET casinos in the Caribbean islands, where the FBI can not get him. His casinos take bets from hundreds of clients from Asia and Latin America. An online gambling company, Global Sports Connection, is run by some Americans from San Jose, Costa Rica. An estimated 130 cyber-gambling sites are at present in operation outside the USA in the Caribbean and Central America. As the INTERNET reaches millions of people around the world, cyber-gambling can enormously enrich somebody overnight.

On-line gambling is estimated to emerge as a \$ 10 billion industry in near future. Representatives Frank Lobiondo and Bob Goodlatte have sponsored a bill in the House aimed at empowering the states in the USA to outlaw cyber-gambling.

## **SYSTEM/DATA DAMAGE**

**W**ire trapping is a common technique for damaging a computer system or its database. This is done by inserting unauthorised signals on a communication line or data channel either to jam the system or use it for criminal purpose. A few years ago, two New York youths, aged 14 and 17 years, were charged with criminal invasion and disruption of the voice mail box system of the International Data corporation, a firm which publishes computer magazines. The voice-mail system enables the callers to leave their telephonic messages through the modem in an electronic mail-box. The teenagers were angry that the firm had not kept its promise to send them a poster alongwith a paid subscription to a computer-game-magazine. Using their home computer, they discovered the firm's password, logged into the firm's computer system, changed messages left in the mail box by genuine customers, cancelled various orders, and made bomb threats. The firm had to shut down its voice-mail system for 18 days and lost revenue of \$ 2.5 million due to cancelled orders. The miscreants were caught after two months investigation.

## **VIRUS CONTAMINATION**

**T**he INTERNET is causing computer virus to spread more quickly than through the diskettes. Macro viruses - small programmes that can be attached to documents written with Microsoft's Word - are transmitted via the NET. As soon as one opens a file on

a PC connected to the NET, the virus infects the machine. According to the National Computer Security Association (NCSA) in the USA, the most dangerous macro is a virus called Concept. It travels mostly on E-mail and files downloaded from the WORLD WIDE WEB.

## **OTHER COMPUTER CRIMES**

**I**nformation Technology has bred some more high-tech crimes, i.e., software piracy, use of computerised information for committing physical crimes like theft, and theft of hardware. Though the medium of INTERNET is not needed for these criminal deeds, policemen will be increasingly called upon to investigate and detect them.

Video Piracy has severely affected the film, video and music industries. It has assumed the proportion of an organized Crime Industry. This piracy was earlier taken lightly, now it is difficult to control, even with the best of Law and Enforcement machinery. Now joint effort between Industry and Police is being thought of. The same thing applies to the current Software Piracy and Copyright violations. A Special Police Force or enforcement agencies with funds from the Industry say @1% of their profit should be thought of to check this Software Piracy and Copyright Violations.

## **SOFTWARE PIRACY & OTHER COPYRIGHT VIOLATIONS**

**S**oftware Piracy is a common form of Cyber Crime. Anywhere in the world, Software Piracy refers to illegal copying and sharing of Software by persons, who have not made a proper purchase of the Software, thereby violating Copy Right Act. A recent study by Dataquest, revealed that almost 65% of all the Software sold in India is the pirated variety. About 80% of the user population are aware of Software Piracy. Exorbitant prices, lack of support for



registered users and low cost of Software outside India are some of the reasons, why Software Piracy is common in India. Further, Internet makes it all the more easier for the Software Pirates. With the present day hyper-speed technology, one can copy a Software and transmit it from one continent to another in no time. For example, an illegal Software of US priced at 28, 0000 dollars can be transmitted and sold at Hong Kong for 60 dollars !!

Apart from the Software Piracy, another hottest copy right violation is that of Music. The site *www.mp3.com* is the latest way in which music is distributed. In about 10 minutes time, the music files can be downloaded from mp3 and the music can be enjoyed. The music once downloaded can be copied (Pirated) and even sold. These files can be loaded in a walkman like music system called MP Station (Cost 200 dollars) and music can be heard during mobility. New music can be downloaded at any Internet Cafe for a few rupees.

The Copy Right Act came into force from 1995 and Software has been given special status in this law. With stringent use of this law alone, this crime can be controlled.

In India, software piracy is a cognizable crime punishable under Indian Copyright Act, and Trade Marks Act. On 7th July 1997, a posse of policemen from the Intellectual Property Cell of Delhi Police's elite Crime Branch cracked down on major computer software pirates operating in the Capital and seized hundreds of CDs with illegal software worth crores of rupees. Amongst the seizures the police was astounded to discover pirated copies of the very latest programmes including expensive packages like Autocad. The raid was a success but no one, even the exuberant cops could deny that it represented no more than a drop in the ocean, considering the fact that over 82%

of all softwares used in India are pirated or illegal.

The simplest way to define software piracy is that it is a copyright infringement on computer software programmes. These programmes are intellectual properties. Technically, computer software is not owned; it is licensed to the person who pays for it for use on a single computer. Software is not the property of its licensee and cannot be loaned or given to another user and if it is installed on another computer it is supposed to be removed from the first one.

Software piracy is today an international phenomenon and the losses caused due to software piracy are astronomical. According to one estimate a staggering US \$12-15 billion are lost annually due to this illegal activity.

Software piracy is rampant all over the world and ranges from an incredible 98% in China and Commonwealth of independent States to 35% in USA. Software piracy is well above 55% in most European countries. In neighbouring Pakistan the incidence of software piracy is 96%. Losses in dollar terms were, however, due to the larger absolute usage in the developed countries. In absolute terms the largest losses occurred in US (\$ 2.8 million), Japan (\$2.1 million), Germany (\$1.9 million), France (\$.77 million), Brazil, UK, Korea Russian Federation and China (about \$0.5 million each). In dollar terms the losses in India due to piracy are estimated at \$ 0.13 million.

#### **DIFFERENT TYPES OF PIRACY**

Software piracy is of different types. Soft Lifting or the purchase of a single copy which is loaded on more than one computer is prevalent all over the world and is difficult to check unless some reliable informers divulge inside information.

Hard disc loading or the loading of unauthorised software onto computers that are sold by dealers is now a well established marketing strategy even by vendors selling hardware of leading brands like HP, Compaq, etc. One of the copy of the PC Zone, for example, a Compaq Pressario 4760 is offered with preloaded Windows 95, MS Works, Corel Draw and several other leading softwares. Almost all the hardware advertised can be pre-loaded with software of the buyers' choice.

By far the most damaging piracies are software counterfeiting and downloading through Internet. Counterfeiting software is more prevalent in China where the piracy rate is estimated to be as high as 98%. It is common knowledge that more than 25 factories, mainly around the Schenzen province in Southern China produce 75 million counterfeit CDs annually, of which 5 million are locally sold and the rest is exported. It was in this context that the New York Times wrote that piracy is not just a problem, it is a fundamentally ingrained part of China's economic plan (NYT 27/2/96). A CD had substantial storage capacity (600MB) as compared to a floppy (1.44MB), and using sophisticated Philips equipment several software programmes can be 'hot-pressed' onto a single CD. The racket operates so efficiently that pirated versions are often available in all the markets within a couple of days of release of the formal software. These CDs are illegally exported to all Asian countries particularly to Hong Kong, Thailand and India where there is a ready market. Thus you are offered master-pieces like Autocad (regular price Rs.1.30 lacs), MS Office (Rs.20,000), Corel Draw (Rs. 20,000), Tally (Rs.27,000) and many other programmes at a fraction of the listed price. At the infamous Golden Arcade in Hong Kong, buyers from all over the world converge to buy such counterfeit CDs. One can buy a CD-ROM containing nearly 70 software titles, including the latest Microsoft releases

for US \$ 50, the total market value of the programmes being well over \$30,000. Customer profile includes persons from Canada, USA and South Africa who find it economical to make a trip all the way to Hong Kong to shop for illegal CDs.

The advent of the Internet has made the already serious problem of software piracy much worse as any and all of the 20 million Internet users can illegally download software onto their computers with just as much effort as it takes to press a few keys. Inexpensive CD-ROM copying devices and increasing use of Internet will make large scale counterfeiting of software a common occurrence.

Undoubtedly, software piracy has numerous, alarming effects as it kills creativity and originality in software manufacturers, stunts development of the software industry, deprives the programmers and others engaged in the production of original software of their just returns, robs the government of revenue and fuels parallel economy.

Several factors are responsible for the proliferation of software for the proliferation of software piracy. The exorbitant cost of original software makes the dirt cheap, pirated version (which works just as well) an affordable, easy and relatively safe option.

Statistically, the odds are against the ultimate user being prosecuted. Second, each PC user has all the equipment he requires to make perfect copies of the original. In many instances there is an erroneous belief that purchase of software includes the right to reproduce it whereas, in fact, the buyer is merely a licensee who is authorised to use the software for his own, personal use. Many people do not realise that they break the law when they loan their floppies to their friends to copy the software. Third, enforcement action has not been taken on such a scale as to act as an effective deterrent. Only three

complaints have been made to the police in the past few months in Delhi and none in these cases so far has yet been convicted. Most serious, however, appears to be the ineffectiveness of the law to redress the problem. "None of our laws were written with the Internet in mind" - observed a Los Angeles attorney who prosecuted Captain Blood, one of the most notorious software pirates brought to book in the US in recent times. It is difficult to apply existing laws to emerging technologies even in advanced countries, not to talk of the scenario that prevails in India. There is a quantitative difference in the perception level of investigating and prosecuting officers and magistracy. The conventional laws of evidence and rules of criminal procedure governing, for instance, those relating to property case and physical evidences collected during investigation are areas where the present wherewithal is hopelessly inadequate to meet the requirement.

Offence of Software Piracy is a cognizable crime punishable under section 63 of the Indian Copyright Act, 1957, which was amended in 1994 to make it more proactive towards checking piracy, and sections 78 and 79 of the Trade Marks Act. In the 1994 amendment, the definition clauses were modified to specifically include computer programmes within the scope of the Act. All forms of software piracy now fall within the ambit of the Act. The law now prescribes a minimum punishment of seven days imprisonment, which may extend upto three years and a substantial fine up to Rs. 50,000/- for such offences. There is a provision for enhanced punishment with higher fines for second and subsequent offences. On being convicted on the second and subsequent occasions, the offender faces a minimum sentence of one year, and which may extend to three years and at least a Rs. 1 lakh fine which extend up to two lakhs. However, very few prosecutions have been launched as there seems to be more emphasis on education and creation of awareness

both amongst the general users and the enforcement personnel.

Software piracy has assumed drastic proportions. The singleness of purpose and resoluteness of will required to meet this challenge is sadly missing.

Three interesting, albeit controversial, arguments about the situation relating to software piracy may be mentioned, which have come up in discussions on more than one occasion. The first concerns the marketing strategy of software manufacturers and the second concerns the pricing of the software and the last concerns ethics; whose interest are we protecting and at whose cost.

While calculating estimated losses incurred by Software manufacturers through software piracy, the accuracy of such figures themselves were questioned as these calculations assumed that those who purchased pirated copies would have purchased legitimate copies, had the illegal versions not being available. It may be that the software manufacturers have realised that such assumptions are certainly unrealistic and have devised their marketing strategy with those very thoughts in mind. What this implies is that, even if all pirated copies were non-existent, some software manufacturers may realise that they may not gain a significant amount of business. As a result, therefore, for the time being, they may wish not to pursue actions to attempt to combat piracy, and instead deliberately allow such activities to take place, in the hope that their software may become widely used and established as industry standard, thereby becoming a necessity in many organisations. When such a time does arrive, the software manufacturers would then intervene to help to stop piracy, and as the users have become so ingrained with the software they are then reliant on the legitimate vendors for any future developments and revisions.

The second point concerns the pricing policies of the software manufacturers. It is quite obvious from browsing through many of the American computing magazines that legitimate copies of the same software are retailing in US at price around 20% cheaper than what it would cost to purchase them outside the US. Thus, customers outside the US are paying a premium in order to obtain legitimate copies of software because the software manufacturers have decided for various reasons, to sell their products, significantly more expensive than they would in the US. The rationale for such policies are unclear, but what is certain is that the effect of selling legitimate software at inflated prices coupled with the prices of pirated copies does not conform to the best environment for combating piracy.

The third and most pertinent question to many is whose interests are we serving anyway by enforcing the copyright laws. Certainly in a poor country like India there are strong grounds to take a soft view. Many law enforcers and trade members feel that the unrealistically exorbitant prices of legitimate software is the root cause of the problem and laws are being framed to serve the vested interests of powerful multinational companies whose primary objective is to maximise their profits. India, particularly, appears to have been pushed into amending its legislation under severe pressure from the US.

The stringent legislation and its effective enforcement should have been bargained for availability of legitimate copies of software at a price affordable to the Indian user. The higher volume sales would have offset the loss due to lower price. Though not legally a justified argument, there is strong resentment against the position presently taken by Indian legislature in the matter.

Software Piracy is on the rise. The global losses from illicit duplication and

distribution on computer programmes, video tapes, cassettes and compact discs are estimated to be \$ 12 billion annually. Europe's software industry loses \$ 6 billion a year, and the USA is also a major loser from software bootlegging within the USA and in China. Macau has between 60 and 80 illicit factories and Hong Kong, another 40-50. A notorious Hong Kong based gang, Wah Ching, whose traditional activities are murder, extortion, narcotics and gambling, has gone into this immensely profitable business of software piracy. In India too, this crime is occurring. One case was reported in 1996 and 1997 each in Mumbai.

### **USE OF COMPUTERISED INFORMATION FOR COMMITTING PHYSICAL CRIMES**

The book "Computer Crimes" by Rakesh M Goyal and Manohar S Pawar, details a burglary of a small town travel agency in Germany. Twice its office was burgled, but nothing physical was stolen. Then suddenly there were a series of thefts in its vicinity, where rich people lived. The thefts occurred when the residents were away from their homes on vacation. The police compared the addresses of the burgled residences with the list in the agency's customer file on the computer. They found that all victims had booked expensive vacations through this travel agency. The customer database had become a thief's guide.

### **THEFT OF HARDWARE**

Three cases of this crime were reported in Mumbai in 1997. In two cases, PCs were stolen and the third related to theft of two printers.

### **TECHNIQUES OF COMPUTER CRIME**

As would be clear from the foregoing, the modus operandi of Cyber-

criminals consists of: (i) manipulating authorised input information; (ii) entering unauthorised information in a computer; (iii) disregarding safety precautions while using files and records; (iv) creating unauthorised files; (v) stealing computer time, software information or equipment; and (vi) introducing virus. The computer crime leads to loss of money, goodwill, image, quality of service, competitive edge and credibility.

### **CYBER LAW IN INDIA**

Any person who, without the permission of the person in-charge of the Computer System, accesses, downloads any data, introduces Computer viruses or causes denial of access, will be liable to a penalty up to Rs. 1 crore (Section 43 of Chapter IX of the Act).

Whoever tampers with Computer source documents knowingly or intentionally conceals, destroys or alters any Computer source code, or causes another to do the same, shall be punishable with imprisonment up to three years or a fine which may extend up to Rs. 2 lakh, or both (Chapter XI under Section 65).

Any person who destroys or deletes or alters any information residing in a Computer resource, or diminishes its value or utility by any means, commits hacking shall be punished with imprisonment up to three years or with fine which may extend to Rs.2 lakh, or both (Section 66).

In the area of electronic pornography, whoever publishes or transmits or causes to be published in the electronic form any material which is "lascivious or appeals to the prurient interest or its effect is such as to tend to deprave and corrupt persons" shall be punished on first conviction with imprisonment which may extend to five

years and with a fine which may extend to Rs. 1 lakh. For a repeat conviction, the imprisonment may go up to 10 years and the fine to Rs. 2 lakh (Section 67).

### **ACHIEVEMENTS OF THE ACT**

**T**he IT Act sought to create a legal framework for electronic commerce and electronic governance in order to extend the laws on oral and paper transactions to Cyberspace. The Act recognises and validates transactions carried out through the electronic medium. It also recognises and protects electronic records and digital signatures. It has provided On-line contracts with evidential value in the court of law by introducing a new section in the Evidence Act. The IT Act and amended provisions of the Evidence Act and the Indian Penal Code provide the contracting parties in an electronic transaction with safeguards regarding digital signatures, misuse of user name/ passwords or login IDs and the like. The Act also proposes the establishment of a legal and administrative framework for e-commerce, through the office of a Cyber Controller. The Act gives statutory recognition to e-governance. It would facilitate electronic filing of documents with Government agencies. It clothes electronic commerce and electronic governance with a legal framework, seeking to curb Cyber Crimes in a more organised and rational way. The Act has extra-territorial jurisdiction to cover any offence committed outside the country by any person.

### **LOOPHOLES IN THE ACT**

**T**he Act has not addressed the following Grey areas: Cyber squatting or stealing of domain name from its legal owner, controlling the conduct of Cyber Cafes; Net pornography hosted by web sites of foreign origin, taxation of e-commerce transaction; spamming or the sending of unsolicited commercial e-mails that amounts to breach of individuals' right to privacy on the Net;

crimes committed by web sites of foreign origin; lack of enforceability of provisions relating to e-governance; jurisdiction (of courts and electronic contracts) in Cyberspace; stamp duty of electronic contracts; Cyber stalking; credit card fraud; Cyber defamation; Internet hour theft, etc. Accordingly, these provisions of the law. For instance, Cyber defamation is dealt with by the regular provisions of the Indian Penal Code and Cyber squatting is dealt with by the Trade Marks Act.

The Act also contains a draconian provision, Section 80, which specifies that only an officer of the rank of Dy SP and above, or an equal senior official will exercise the power of raiding any premises and arresting any person found therein without warrant, who is reasonably suspected of having committed or of committing any offence under this Act. The Section even states that it will have an overriding effect on all other laws in force for the time being. The question is, how can one suspect that an offence is about to be committed somewhere under this Act. This provision came under severe criticism from different quarters.

### **CYBER SQUATTING:**

**C**yber squatting refers to the widely prevalent act of stealing or assuming by a dotcom, of a domain name belonging to an established company. The domain name holds immense importance, since it identifies a Computer or special network of Computers on the Internet. The IT Act, 2000, has maintained complete silence on this issue. The issue of Cyber squatting is presently being dealt with by the provisions of the Trade and Merchandise Marks Act 1958 and the Trade Marks Act, 1999.

### **REMEDIAL MEASURES SUGGESTED**

**T**he foremost requirement is to enhance awareness of the variety and

scale of cybercrime. Banks and financial institutions; government, public and private organisations; business and corporate houses must be sensitised to this threat, for they would be the major victims. The public at large should also become aware, as more and more individuals and families are joining the INTERNET and are exposed to invasion of privacy, harassment intimidation, blackmail pornography, obscenity and smut. Representatives of banks, financial institutions and business houses revealed that they were largely ignorant of this criminal threat. It is, thus, obvious that people want to know more about cybercrime, when realise that it touches their personal lives and threatens their business. Software firms, NGOs and universities should take the lead in organising public awareness programmes. In the USA, an organisation called the Computer Emergency Response Team, financed by the government and based at Carnegie Mellon University, Pittsburgh, has been posting advisories on the INTERNET, alerting computer users to attacks and urging them to take a variety of protective measures involving software and hardware security mechanisms. The London School of Economics has a computer security research centre, which advises banks, companies and governments on how to improve computer security .

Second, NGOs and Software firms should help in detecting software piracy. The London-based Business Software Alliance (BSA), whose members include software giants like Microsoft, Lotus and Novel, detects use of illegal software by firms. It alerts the police, obtains a search-and-seizure order and examines the suspected firm's computers.

Third, software companies should develop or import programmes which can block access to smut and pornography. Western countries have developed programmes like Net Nanny Pro Cybersnoop, which enable parents to monitor and filter everything passing

through a computer. Cybersitter, a programme marketed by a Christian group in the USA, is said to screen out all references to sex and gays. A new Web-site, <http://www.smartparent.com>, offers a crash course for parents about the dangerous side of the INTERNET.

Fourth, the government should create tools, including laws and specialised police units, to patrol and police the electronic airwaves. For instance, the Singapore government has licensed only two Internet services linking individuals' computers with the outside world. It has extended anti-pornography and libel laws to electronic transmissions, providing jail terms and fines for the offenders. Singapore also has a watchdog committee to monitor the electronic transmissions via the INTERNET and the INTERNET surfers have been officially asked by it to

report whether any Internet subscriber is indulging in anti-social behaviour. The Government should also consider enacting a law to combat virus contamination. The Israeli Knesset has passed legislation providing upto 5 years imprisonment for those spreading virus, either by writing destructive virus programmes or introducing virus in computer systems and also for those who transmit or store in computers fraudulent information. The British Government has strengthened the Video Recording Act, enhancing penalties for intellectual piracy.

The main responsibility of detecting and investigating cyber crime in India will, however, be of the police, which is not trained and equipped to discharge it. The first requirement is to familiarise police personnel with this new world of white-collar crime. An active

liaison between major software firms and police would be mutually beneficial. Policemen can acquire computer literacy through these firms, whereas the latter would learn from the police the details of reported cyber crime, thereby refining their counteraction strategy and tactics. Microsoft in the USA trains police officers for combating this crime. Special cells should be established at the state police headquarters to combat INTERNET crime. The USA has a National Computer Crime Squad. Italy has set up a computer Crime Unit in its force.

The police in India should now regard CYBERSPACE as their latest beat, which needs to be patrolled with hi-tech expertise. Otherwise, they would be overtaken by cyber crime before they are ready to meet it.

*The difference between  
coarse and refined abuse  
is the difference between  
being bruised by a club  
and wounded by  
a poisoned arrow*

**Johnson**

## **INDIAN POLICE SERVICE: A SERVICE TURNED TOPSY-TURVY**

Balwinder Singh

**I**t is common among senior Indian Administrative Service (IAS) and Indian Police Service (IPS) officers to very excitedly talk about their 'achievements' during their postings as District Magistrates, Collectors, District Superintendent of Police, etc. They talk of how they handled various agitations, election arrangements or developmental activities or how they 'managed' many crooked and not so 'crooked' politicians. It is very rarely that these officers talk about their other assignments with the same enthusiasm. Why is it so? The simple answer is that most of other jobs which IAS and IPS officers do in their long career spanning 35 to 38 years are not comparable with their district assignments in terms of challenges and responsibilities. In earlier times, IPS officers used to spend a major part of their first 25 years of service in the field postings as District SsP and Range DIsG.

Now thanks to quick promotions they are in the state capital, on an average, after putting in 10 to 12 years of service. A major part of their remaining career, they work as 'Babus' in the State Headquarters. As such, a large number of officers have to be accommodated in the state capital. The existing jobs at police headquarters are bifurcated, trifurcated and so on with the result there is hardly any job content left in vast majority of the jobs from DIG to Additional DGP level. A large number of jobs are only sinecures. Half the IPS officers are leading lives which can be called preparatory to retirement. Unfortunately, it happens when they are at their most productive stage in their career in their late 40s and early 50s. They are highly energetic and experienced but due to a skewed system, this vast pool of experienced competent officers are highly under utilized.

The problem has originated out of a mind set in all organized higher civil services which are competing with each other for 'quick promotions'. In reality there is no real 'promotion'. There is hardly any increase in the official responsibilities, job content or even increase in perks except a nominal increase in salaries. Rather in the case of IPS there is a steep fall in the job content after the level of SP/ Senior SP.

IPS as a cadre does not like to 'lag behind' the IAS cadre. Moreover, different state cadres are competing with each other for quicker promotion. The paradigm of low job content is almost the same in the IAS. There are many departments in the state governments having one or four principal secretaries. Many times even one of them may not have enough work as there is shrinking of the role of Government in departments like industries. But as 'turf' for IPS is relatively limited the problem is more acute. The job of District Police Chief which is the most critical job for IPS cadre is historically designated as District Superintendent of Police. With quick promotions in the last two decades, a situation has arisen where the officers of seniority upto 12 or 13 years get promoted as DIsG. This has resulted in a situation where while junior officers are holding most important jobs with majority of the senior IPS officers at DIG, IG, and Additional DG level officers having jobs which in terms of job content are fraction of the job of District Police Chief. Now the challenge is how to improve the job content of the senior IPS officers so that they can contribute to their optimum capacity. To an extent some southern and western states have found a partial solution by establishing commissionerates of police in major urban areas. But this is a very limited solution because commissionerates can be established only in metropolitan areas where urban population exceeds 10 lakhs. Such areas are very few. Moreover, there is bound to be resistance from the IAS cadre in a big way. For example, a district

like Kanpur in UP with nearly 9000 police force is headed by a senior SP when more experienced officers are holding far less important jobs. There are large number of districts like Kanpur which are headed by district Superintendent of Police but are far more important from policing point of view than many Commissionerates of Police. For example, in Andhra Pradesh, Guntur, East Godavari, Nellore, Warangal, Kurnool, Chittor and many other districts are far more populous and complex from policing point of view than Commissionerates of police of Visakhapatnam and Vijayawada. Most of the above mentioned districts cannot be converted into commissionerates because they are not having big enough urban areas. A district like Guntur in Andhra Pradesh has a population of more than Hyderabad city. Though this district has more than a dozen municipal towns but no one town has population of 10 lakhs to meet the criterion of converting it into a commissionerate.

The solution lies in de-linking the post of District Police Chief from the rank of Superintendent/Senior Superintendent of Police. When more than a century ago British administrators designed the policing system, the district as a unit though vast in area had very limited policing work when compared to the present situation. The policing workload has expanded manifold both in quantity and complexity due to vast increases in population, urbanization, political activity, increased social tensions, organized crime, growth of terrorism, etc. Though a precise comparison between British and Indian Police is not feasible because the systems are different and British police has only one level of entry into police service, still a rough comparison can be useful. We notice that most of our districts are bigger and more complex than British counties on almost all parameters, i.e., size of police force, population, area, magnitude and complexity of crime, social and political tensions, etc. A typical British County has a police chief who can be roughly

treated equivalent of our DGP with a number of Superintendents of Police working with him in various functional and territorial divisions. An officer of the level Superintendent of Police is not adequately experienced to properly manage a district police unit in most of the districts in India today. With just 5 to 12 years of service out of which more than 2 ½ years are spent on training they do not have adequate experience of multifold responsibilities they are expected to handle. They become heads of the district police without acquiring adequate experience in managing crime, law and order, personnel and financial matters. This results in a situation where the focus is on somehow managing the law and order situation and have good public relations, with the result that policing has been reduced to fire fighting and systematic improvements are not taking place. A few young SsP bring about some cosmetic improvements here and there but they fail to take roots and disappear with the transfer of officers.

There is need to have more experienced district police chiefs in at least the big and complicated districts. The designation of SP may be changed to District Police Chief. Smaller districts can be headed by Officers of the level of Senior SP, bigger districts by DIsG/ IsG. These big districts which will be under the control of IsG/DIsG can directly report to the DGP, as Commissioners of Police are doing today, and district SsP can report through DIsG/IsG. The big districts can have SsP assisting the DIG/ IG as is the position in the cities under the charge of Commissioner of Police today.

A typical case of a Career Progression for IPS should be as follows:

We can visualize some of the objections to the scheme as suggested above. It may be argued by some that there are not enough number of willing senior officers to work in the districts. This argument is not sustainable as there

Training	2½	
Sub Divisional charge as Asstt. Suptd. of Police	2½	7 1/2 years
Addl Suptd. of Police ( Admn.& Personnel)	1 year	—
Addl Suptd. of Police ( Crime ) /Naxalite/ Terrorist Operations/ Addl. Suptd. of Police (Operations)	1 ½ Year	—
Suptd. of Police/Deputy Commissioner of Police working under a Commissioner of Police or working under District Police Chief of Inspector General/ Deputy Inspector General level Or Commandant of a Battalion		— 1 1/2 years
Dist. Suptd. of Police Incharge of Smaller Districts		2 to 3 years
As Suptd. of Police in the CID/ Intelligence / Anti-Corruption-Bureau		— 1 to 2 years
Promoted as Deputy Inspector General of Police		13 <sup>th</sup> year of service
Promoted as Inspector General of Police		17 to 18 years of service
Range Inspector General/ Head of District Police as Inspector General / Commissioner of Police / Inspector General in Headquarters/ CID/ Intelligence/ Anti-Corruption Bureau etc.		— 7 to 9 years
Promoted as Addl Director General of Police :		— 26 to 28 years of service

is always a beeline of senior officers with seniority ranging from 15 to 25 years who want to be posted as range/zonal DIsG and IsG. The places where senior officers are likely to be posted will normally be well developed districts, for example, in Andhra Pradesh the districts like Guntur, Kurnool, East Godavari, Nellore, etc. Another objection which can be made is about relationship between District Magistrate and District Police Chief. This equation should not make us continue with a distorted system. In my view when senior IPS officers get posted as District Police Chiefs, the IAS cadre will understand this logic and fall in line by posting senior officers in the district as Collectors/ District Magistrates/Deputy Commissioners and Commissioners.

Another argument which can be made against this scheme is that young officers are more enthusiastic and thus more suitable for field work. While it is

true to some extent but the career progression suggested above will bring a blend of youth and maturity and channelise their creative energies.

The likely resistance to this scheme of things can come from young ambitious officers in seniority of 8 to 13 years who will find that such a system will deprive them of powerful positions in near future and they will have to wait for long. Resistance may also come from some powerful Addl. DGsP/ IsG who find manipulating young SsP easier.

However, taken up in a phased manner this resistance can easily be met. The scheme suggested above is in the interests of better policing and governance and it is also in the long term interests of the Indian Police Service cadre. It is a win-win solution for both the IPS cadre as well as public on the whole.

If establishment finds it difficult to counter the resistance, then go in a phased manner- ( a few districts can first go to DsIG/IsG) say Guntur, East Godavari , Kurnool, Warangal, Chittoor, etc.

Given a limited exposure, I would not venture to suggest a remedy for all AIS service officers and would limit myself to the IPS. My comments are of direct relevance to AP, the cadre I belongs to but should be equally relevant to other state cadres.

1. Reduce the cadre strength -by removing or reducing the leave and Training reserve, because this reserve is practically not used to that extent if more reserve districts cannot be created.

Create smaller police districts – today, with computerization, it is possible to do it without substantially increasing the establishment cost as it is possible to create DPOs with half the strength of Ministerial Staff. (The system is completely distorted).

## LIKELY OBJECTIONS

### I. Young officers are more enthusiastic.

Agreed

You can create a blend of youth and maturity

### II. There may not be enough number of willing senior officers

Not true

Places like Guntur, Kurnool, East Godavari, Nellore

Till an officer is 45 years of age their children are still in school and most of these district headquarters have good schools.

### III. Relationship of DM and SPs :

You would shortly find IAS will understand this logic of fall in line by posting senior people in the district.



# COMMUNITY POLICING: A COMPARATIVE PERSPECTIVE

Meeran Chadha Borwankar

**D**uring my Humphrey Fellowship 2001-02 at the University of Minnesota, I got the opportunity to study some of law enforcement systems in US. I did an internship with the SAFE community-policing unit of Minneapolis and also interacted with St. Paul police during my stay of about ten months. During the course of my travels around that country, I interacted with various law enforcement agencies at all levels, e.g., an Indian American tribe, the Mille Lacs, Sheriffs and staff of Rice County and Fillmore County in Minnesota, Ware County in Georgia, police organisations of Atlanta, Seattle, Chicago and Way Cross in Georgia.

I chose the topic of community policing. I have been curious to know

what it exactly means and whether it is a new jargon for the age-old policing methods that we have been using.

As per Upper Midwest Community Policing Institute, St. Paul, State of Minnesota. "Community Policing is an organisation wide philosophy and management approach that promotes community, government and police partnerships; proactive problem solving; and community engagement to address the causes of crime, fear of crime and other community issues. Community policing has two core equally important components: Community Partnership and Problem Solving." I agree with the above definition. In practice I would prefer more specific focus than the general issue of 'crime and fear of crime', e.g.,

as the paper below shall show, some of the police organisations have taken up topics like drug abuse and 'crime impact statements' for the specific purpose of community policing.

This concept envisages a police officer as a problem solver whose mission is to address grass root level crime related issues and to bring average citizens together as neighbourhood groups. 'He does not react to a crime but encourages the local community to deter the crime happening in their streets. He is the catalyst. Being a professional, he can guide the community in preventing the decay of their area, which in the context of US may mean drug abuse in streets and in the Indian context it may be the 'Road Romeos' teasing young girls. At the cost of repetition I would like to emphasise that a community police officer is not expected to 'take on' all the problems of the community but to empower it to do so itself. In their article 'The basics of Community Policing' Robert Trojanowicz and Bonnie Bucqueroux (Christian Science Monitor, June 18th 1992) mention that "this decentralised and personalised form of policing breaks down the anonymity that plagues traditional police efforts. ...While community police officers are full fledged police officers, their performance is judged on how well they solve the problem, not on how many arrests they make. ..Community policing gives them the autonomy to tailor the response to local needs and resources, the chance to see whether the ideas work and the opportunity to tinker and try again if they do not". And so the cop is back in the community he belongs to. I used my interaction with various police organisations across US to understand how successfully has this concept been put to practice.

The main issues, I want to deal with in this paper are as below-

Is community policing any different than the traditional policing?

- Is this concept popular at the leadership level or has it percolated down to the grassroots level police officers?
- Does community policing mean soft public relation exercise or is it a genuine problem solving approach with the community and police pooling their resources together?
- Are the Communities genuinely empowered?
- Do they participate actively in this collaborative effort?

After reading a lot of literature provided by various police agencies in US and through my interaction with police officers of all levels, I have a glimpse of what I think is the concept of 'Community Policing', and how it is being put to use in US and in India. In my paper below I shall deal with the subject; wherever possible I shall compare the methods being followed by the Indian police (with particular reference to the State of Maharashtra) and those I observed in US. **I am writing this paper mainly for the police officers in India for sharing my experiences and observations during the course of a yearlong dialogue with the police organisations of US.**

Two main issues that distinguish the working environments of police of India and US are - **the magnitude of drug abuse and the culture of guns in US.** It has not been my point that the two countries or their systems of law enforcement have many things in common. On the contrary, I am very aware that India being a developing country is facing challenges that are quite different. But human nature being the same and law enforcement dealing mostly with the darker side of it, I thought I would find a number of similarities. Response of the professional agencies could vary mainly in technology or speed, but strong

tradition of democracy is common to both the countries. I found myself right about the human nature part of it but that drugs and guns would have such a strong impact on the crime scenario in US came as a surprise, a very unpleasant one indeed.

## **BROAD STRUCTURAL DIFFERENCES**

The system of law enforcement continues to evolve in both the countries but it is truly decentralised in US. Each tribe, county, city and state has total autonomy in developing its own system. The chiefs and the sheriffs are directly accountable to the elected representatives and not to a department as it happens in India, e.g., the chief of a city police in India is appointed on the basis of the recommendation of the Director General of state police. The Chief Minister, i.e., the elected head of the state approves the same but local elected officials of the city do not have much hand in picking up their police chief. Of late, they do influence the appointments but it is not built in the system, which empowers the state police chief to recommend. On the other hand, city and county elected officials have a very direct role in not only the appointment of the police chiefs in US but also in influencing the strategies he/she shall follow for law enforcement. The main reason is, of-course, the finances. As the local Govt. pays for the local police, they also hold them totally accountable. In his farewell address as recorded by The New York Times, 27th Dec. 01, the then Mayor Rudolph Giuliani, spoke about policing in New York city, in a way that it makes it very clear about who was calling the shots. "It seemed to me that we had to change the way in which we did policing in New York City. We had to make it accountable. We had to make it responsible..." he does not elaborate on what methods he actually employed to make the New York police more accountable but every one knows that he provided the vision.

The credit for doing so is of course then taken by the elected representatives. While in India, it is mainly the responsibility of the local unit in-charge to provide the vision as well as the strategies. Elected representatives are important but in police related functions in a district, in periphery. If the district police chief were a strong person, they would lie low and bounce back if he/she happens to be weak. Since the funds for police are provided from the kitty at the state level, local monitoring is not as lethal as in US. Mayors in India do not directly select/appoint the police chiefs though they can and do influence the selection. Infact, 'political interference' is looked upon as undesirable by both citizens and the media. During the current Hindu-Muslim riots in the state of Gujrat, while police has come under severe criticism for being unprofessional and biased, most citizens think that it was at the behest of local political leaders that the situation was permitted to take such an ugly turn.

While a direct role of the elected representatives in US may have its down side, but it has ensured a very positive impact of bringing the communities close to the working of the law enforcement agencies. This, to my mind, is the main factor responsible for the universal theme of community policing in US. During 1993, when Chicago police decided to introduce CAPS program, i.e., Chicago Alternative Policing Strategy, the then Mayor, Richard M. Daley talked of "forging new partnerships among residents, business owners, community leaders, the police and the city services to solve long range community problems." ('Together We Can' - Oct. 1993, Chicago Police Department Publication). As is well known, it has been a very successful program. One of its main features has been the ability of the successive mayors to pool in all the city resources, e.g., if an apartment building is afflicted with drug problem,

all the city departments work in collaboration to improve the lighting, remove garbage, dismantle the old neighbouring structure, book the offenders, etc. In India, co-ordinated approach is pursued but as the elected representatives are not so directly involved in policing, it is generally various civil servants who co-ordinate with different rates of success e.g. 'Hawkers' on the public roads are a big problem in Mumbai from the point of view of traffic as well as nuisance to the local residents. Despite the efforts of police and the Mumbai Municipal Corporation, the menace continues because of lack of political co-ordination by different agencies. This co-ordination, whenever seen, is mild and ad-hoc in nature. Political leaders have played a direct role; being dependent on these 'vote banks' they have in a way protected the 'hawkers'. Dragging the issue to the courts has further confounded the problem. In most of the places that I have visited in US and interacted with, the elected representatives have provided the umbrella for city/county services to work in co-ordination with each other (including the police department) and to the benefit of citizens. Curiously though the citizens in US continue to distrust the politicians. Within this broad structural framework, police organisations in US have developed their own area specific systems of community policing.

As I did my internship with the **Minneapolis Police**, I am most familiar with this model. The mission statement of Minneapolis Police Department for community policing is as follows -

"To reduce opportunity for crime, to deal effectively with the fear of crime, to increase neighbourhood liveability and to reduce unnecessary police calls for service, we serve neighbourhoods and the business community by helping them to increase community cohesiveness and solve community problems". (Crime Prevention Resource

Manual, Minneapolis Police Department).

The special community police units are called CCP, i.e., Community Crime Prevention or SAFE, i.e., safety for every one. The city has a population of about two hundred thousand (suburbs not included) and it is divided in to five precincts. Each precinct has its CCP/SAFE unit, where a sworn police officer teams up with a trained civilian known as a crime prevention specialist for the purpose of community policing. These teams are given geographical areas for their work. The SAFE unit has a program manager, a post recently abolished due to the budget cuts; a civilian and a sergeant who work as supervisors for the crime prevention specialists and the sworn officers respectively. The overall supervision is by the precinct commander; the lieutenants of the geographical areas interact with the SAFE teams on regular basis.

While the officers on patrol duties respond to the 911 calls, SAFE teams are expected to invest in long-term relationship with the community. They organise block or apartment clubs as their basic units for interaction. Training sessions are held for block leaders and SAFE teams attend some of the functions organised by these clubs for their security-related issues. If the block or apartment club is afflicted with a particular crime, the SAFE teams are expected to assist in solving the same or to liaison with the concerned authority. I did not find many enthusiastic or active clubs during my internship. These teams also carry out special workshops for the security of business areas in their jurisdiction, create Mc Gruff Houses for children, help in National Night Out event, etc. They also undertake to organise good lighting in neighbourhoods, removal of graffiti, crime alerts, and personal security training. The down side of this model is that it is not being effectively used for

information on serious crime like drugs. It is very loosely structured and the staff cannot be held accountable for anything in particular except for organising public relation programs. The sworn officers generally seek to move out after about a year and this high turnover means that there is no long-term relationship between the community and police. The civilian crime prevention specialists, (curiously there are more women) however, are more or less permanent features and redeem the situation to some extent. I found the CCP staff not tapping the resources of the community to handle crime specific issues. It also depends on the lieutenants and the precinct commander on how effectively do they use these resources. My personal impression is that the units could be more focused and integrated with regular police work. Some revamping is underway; as of today they seem to be more geared for public relations and liaison work. During a random survey that I carried out in the University of Minnesota, Twin-Cities campus, 69% of the students did not have even a rudimentary idea about community policing in Minneapolis.

The concept indeed involves a paradigm shift for police officers that are too full of their 'uniforms' and not used to team up with civilians. In India, since 'prevention of crime' has always been considered a crucial part of a policeman's job and beat system has been an integral part, community policing is only a step further. Yet this one step forward can take painfully long time to come by! Tata Institute of Social Sciences, working with the Mumbai police for a long time has been recommending induction of trained social workers in Mumbai police. But there has been no success and one of the reasons as I see is the strong reluctance on the part of police officials to have civilians in police stations; it seems threatening to many. However, the beat system is working and if officers are not hard pressed for time they interact with community. The change

from 'interaction' to involving the community in proactive problem solving as a philosophy is yet to arrive formally. I can see this in certain situations even today e.g. citizens are actively associated with police arrangements during the festivals, processions, religious gatherings, etc.

I also interacted with St. Paul Police that follows a more centralised system called FORCE, i.e., focusing our resources on community empowerment. Established in 1992, it has street level narcotics activities as its focus. Following are the objectives of FORCE "To combine the elements of patrol, the city wide crime prevention program, an environmental housing inspector, our citizens and other related agencies and programs in an effort to successfully interdict street level narcotics activities and inappropriate behaviours. By working closely with our citizens and other city agencies, FORCE will attempt to reduce both the level of crime and the opportunities for such crime". (Web site of St. Paul police Department, sppds08/manual/314-06.htm)

A commander heads the unit and the staff is centrally located with duties being allotted to them as per the need. Its functions include investigation of street level drug abuse, execution of search warrants, to provide public education on crime prevention and to build police- community partnerships to combat crime. For the purpose of partnership with community, FORCE staff organises Neighbourhood Block Clubs if requested, and conduct Neighbourhood Crime Watch programs. It is pertinent that the literature of the unit mentions that it encourages self-reliance among the communities and not to become dependent on police. During my interaction with St. Paul police, I found FORCE to be thin and lean, clear in its focus on street level drug related activities and moving in a well defined though limited direction. On the topic of more elaborate involvement of

community, I was informed that each precinct has to accept the responsibility for community involvement and that a conscious decision had been taken not to have separate units for community policing except FORCE. There are fewer civilians working for community policing at the precinct level than in Minneapolis police. Existing system of citizens district councils are being used for citizens' input. In many ways it is like in India, where citizens' meetings are held under different names. They may be simple tea meetings most of the time but are put to active use at the time of crisis. Most successful police officers in India know the need for maintaining good relations with the community. It is very essential for their survival. They are also associated with problem solving on day-to-day basis though may not be conscious of the terminology. It is in metropolitan cities like Mumbai, Delhi etc., where police officers are under tremendous work load, that they may only respond to calls with hardly any time for working with the community on sustained basis.

Chicago Police performs the task of Community Policing through its well-known program called CAPS, i.e., *Chicago Alternative Police Strategy*. It is well integrated in the beat system just as it is in India. The whole city is divided into 25 police districts, and each district has 9 to 15 police beats there are 279 beats in all. The beat officers are basically responsible for engaging in constant dialogue with their community and to address to their problems. Each police district has a community police office that co-ordinates at the beat level and also provides services to senior citizens. The emphasis is on beat community meetings as the basic forum to identify the problems and possible solutions. The beat officer is not just expected to respond to 911 calls but also to engage in long-term relationship with the citizens in his beat. Chief of police, Terry G. Hillard in the biennial report of the Chicago Police Department - 1999-2000

says, "The Chicago Police Department's mission is to work closely with the residents to build long lasting foundations for safe neighbourhoods. " Besides drugs, gangs and problem of youth, the beat system also pursues 'court advocacy' where it encourages the neighbourhoods to present their grievance in courts for stringent action by the judges, as the city is seriously afflicted with professional gangs crime. Chicago police has claimed that since its inception in 1995, CAPS has contributed to reduction in crime by 25.6%. (Research and Development Division, C.P.D. Jan. 2002). However, during my visit, the police officers admitted that there was a very high turnout of beat officers. Whenever I interacted informally with police officers in US, they admitted that they liked the enforcement duties more. Some of them preferred 911-call duty, as it does not involve much paper work. It appears to me that we are possibly attracting persons with particular personality traits in law enforcement that prefer action to sustained paper work. In India many a times, officers with strong 'community policing' bearings are derogatorily referred to as 'social workers' and in US they are ridiculed as 'Lollicops' or 'grin and wave squads'. The Atlanta police Department consists of six zones and 56 beats. It too thinks of community policing as a philosophy and not as a tactic. It has 24 neighbourhood planning units representing 139 neighbourhoods. Beat officers are responsible for involving the community and there are Citizens Advisory Councils to facilitate citizen input into the police policies and actions. For the purpose of community policing, the Atlanta police have created mini precincts for officer-citizen interaction. The city police have created foot and bicycle patrols for a 'personalised approach'. Police officers volunteer to read to students for 'Reading Patrol Program' and interact on continuous basis with students under 'Junior Achievement Partnership'. The local police have a Citizens' Police Academy, a Junior Citizens' Academy and are very active in truancy

enforcement. The Atlanta Police Athletic League provides educational, recreational and athletic programs for the youth. In fact, most police organisations in US and in India have such programs, but community policing is much more than this.

Seattle Police Department with a strength of about 1300 sworn police officers has four precincts. Each precinct has a number of police officers responsible for community policing. These officers do not respond to 911 calls. They are engaged in a variety of activities in the local community, e.g., in improving the racial relations, controlling the drug abuse in the streets or in 'School Emphasis Team Program' where the officers work directly within the school. One of the main emphases of community policing in Seattle is to keep the youth away from drugs and gangs. The precinct community police officers invest a lot of time and effort in this and in establishing block and apartment clubs. It has a very active Community Policing Action Council (CPAC) consisting of local citizens. Formed in 1992, it formulates strategies and develops programs to enhance positive community/police partnership. Besides attending the monthly meetings, each of the CPAC members serves in one of the three committees: Community Police Academy, Education or Partnership. During the year 2000, CPAC sponsored two community forums, one on Critical Incidents and the other on Hate Crimes. Its members actively team up with police officers to educate citizens on various issues.

Systems of Community policing in rural settings - As in rural India, so also in rural US, population is widely dispersed and generally police officials have more cordial and friendly relations with the community they serve. One of the main reasons is of-course that police is not incident driven and has time to sit back and communicate in real terms.

I visited two county police organisations, i.e. Rice County and Ware County.

Rice County consists of 496 square miles and 58,000 persons. During my interaction with the Sheriff, Richard Cook, he came out as a police official committed to serve his people. In his e-mail to me he further delved on the topic as below-

"Development of a community policing strategy was not difficult because we felt, in essence, that is what we have always done. With only 12 patrol officers it is not practical to assign permanent areas as some departments have. We, at times, have only two officers on duty. We have, although, emphasised patrol visibility throughout the county with a greater emphasis on sharing of information between officers. Our main weakness is shortage of officers.

This strategy has seemed to pay dividends in more than one way. Not only have we seen a decrease in crime and improved apprehension of criminals but we have also heard positive comments from the public about the visibility of squads throughout the county and an improved sense of security.

Community policing, per se, is no magical formula or complex strategy. It is just a buzzword expanding on what we already do and soliciting support and cooperation from the public in a common goal of public safety. It is based on the premise of creating and expanding partnerships with the public, other agencies and departments to deter, prevent and eliminate crime and the conditions that perpetuate the opportunity for crime. We encourage officers to get out from their squads and interact with the public especially in common gathering places. It is essential to have a grassroot relationship with the public starting

from the cradle and ending with the grave. Being a visible integral part of the community is the essence of community policing, where officers and community members alike take ownership of their community together” (Sheriff Richard Cook, Rice County, State of Minnesota, US).

It is a big quote but gives an idea of what community policing is seen as, especially the fact that the Sheriff feels, it is a buzzword today but has been traditionally undertaken in the past. Most feel the same in India, too. It makes me wonder whether rapid urbanisation created the gulf between citizens and law enforcement that we are now trying to bridge through reviving the concept of community policing! One major factor that appears to have taken the cops away from the community in US, is a squad car. Many students in the University told me that they never see a policeman walking by, he is always rushing in his car. Such perceptions confound the situation. Luckily in India, a cop is still seen around and at the most can afford a two-wheeler!

Waycross Police Department in the state of Georgia is feeling proud that it had no case of homicide during the year 2001. The last chief of police served the city for 26 years as The Chief, and knows practically every one by name. The current Chief, James E. Blackburn is a strong believer in the concept of community policing. He “actively solicits and encourages cooperation of all citizens to reduce and limit the opportunity for crime and to facilitate maximum uses of resources”. His organization has received funds for weeding out criminal problems under Weed And Seed program. He thinks it to be the best example of community policing as it brings the community together to solve a particular problem. Each police officer in Waycross city is a community police officer, as besides responding to calls, he is expected to engage in constant dialogue and

problem solving. Special programs called ‘Shop With A Cop’ and ‘Feed the Needy’ during Christmas are undertaken by the local officers. It is quite similar to the attitude of police officials in rural India who are often involved in issues that may have nothing to do with policing! Availability of time and pace of life makes them more approachable and humane.

In Mille Lacs Band of Ojibwe, I noticed the need for a different kind of police structure as the area belongs to a Native American tribe, who are still struggling to come to terms with the ‘White’ culture. Chief of police, Phillip A. Galeo too admits that one of the main tasks before him is to increase the representation of native Indian in his organization, as till date there are only about 18% native Americans in the police organization of the Band. He too is a believer in the concept of Community Policing and mentioned that “In 2000, the Mille Lacs Band Police Department brought in community policing trainers from the COPPS office (US Dept. of Justice) to provide training to both officers and community members in the areas of police/citizen cooperation, problem solving, and communication and listening skills. Following that training program, citizens formed a problem solving team to address emerging gang issues, and trainers were provided by the Department to show community members what gang life and gang investigations are all about... Community Policing efforts work to assuage citizens’ concerns by opening communication between the department and residents. ...The police and the community are now working on several issues, including community violence and juvenile curfew violations and enforcement and officers are developing a computer literacy course at the community youth center. Members of the community, adults, elders, and young people alike, are getting to know one another better by talking about community issues that concern everyone, including the police.

Community policing efforts are different in every jurisdiction - each community must craft a policing model that best reflects its culture and jurisdictional needs. The Mille Lacs Band Tribal Police Department is working diligently, albeit slowly, at building a policing service model that best meets the needs of the reservation, the Tribal government, and the State of Minnesota”.

The tribal police is also holding computer familiarisation classes for kids and teens, through the police volunteers, “to create non threatening and non-formal atmosphere” in police community relationship.

To sum up, I would emphasize that Community Policing is not the only strategy being followed by law enforcement agencies. All police organisations have special crime units that not only detect but also attempt at preventing certain type of crime in communities though their level of interaction with citizens is not high, for e.g., narcotics, homicide, fraud units, etc. New York police achieved great success through its ‘zero tolerance’ to crime and disorder program. There are a variety of similar programs and strategies. Citizens’ perception about the efficiency of local police and their level of satisfaction depends mainly on the handling of serious crime; collaboration between citizens and police cannot reduce crime over night. It is a long-term investment that shall eventually provide better information to the police for prevention of crime and disorder. It shall also help to detect, once a crime has taken place.

In Police quarterly, volume 3, No. 1 March 2000, ‘Cops at the Door’ by Lawrence F. Travis and others, the authors refer to one of the main assumptions of community policing, i.e., the community is more likely than police to assess and understand its needs for public safety. I am of the opinion that

we are at a stage where communities are learning this process. While police organisations are yet to make the quantum jump from mere interaction to empowering the communities, latter are also yet to prepare themselves to accept this active role. And there are miles to go...

## CONCLUSION

The journey through various police organisations in India and US has given me some tentative hypotheses for the issues I raised in the beginning of the paper. They however require further research-

- Community policing is at the nascent conceptual leadership level. It is yet to be percolated down to the grassroots level police officer both in India and US.
- As the local Govt. finance the police organisations in US, the mechanism is more tuned to the thought of Community Policing than in India where the funds come from the state thus putting certain limitations on the 'say' of local representatives.

- Community policing still continues to mean public relation programs. However, cities like Chicago and St. Paul are using it for problem solving with the community and police, pooling their resources together for specific purposes.
- Most communities do not feel genuinely empowered. However, political leaders in both the countries have been empowered. I see a serious problem in this but it needs further study. I am sure Community policing meant empowering the average citizen and am wondering where did we lose him?
- Citizens in both the countries are not familiar with the collaborative theme that underlines the concept of Community Policing. In US they are in awe of uniform while in India they are still scared of it. They have to prepare themselves for an active role and empower themselves.
- 'The basics of Community Policing' Robert Trojanowicz and Bonnie Bucqueroux (Christian Science Monitor, June 18th 1992)
- The New York Times, dt.27th Dec. 2001
- 'Together We Can'- Oct. 1993, Chicago Police Department Publication
- Crime Prevention Resource Manual, Minneapolis Police Department
- Web site of St. Paul police Department; sppds 08/manual/314-06.htm
- Biennial report of the Chicago police department-1999-2000
- Report of Research and Development Division, C.P.D. Jan.2002
- Police quarterly, volume 3, No.1 March 2000, 'Cops at the Door' by Lawrence F. Travis and others

## BIBLIOGRAPHY

- Web site of Upper Midwest Community Policing Institute', St. Paul and State of Minnesota.

All the views expressed by the author of the paper are based on her personal observations.

*Trust not him  
that  
hath once  
broken faith*

**Shakespeare**

# **CYBER CRIME: INVESTIGATION & PREVENTION**

Dr AP Maheshwari

**T**he contagion of crime is like that of the plague. Criminals collected together corrupt each other. Crimes related to the cyber world are of a unique nature in terms of their locus. The rapidity with which information technology has spread its influence is evenly matched by the dexterity with which cyber crimes have pervaded the human environment. It has been rightly said: "It is great cleverness to know how to conceal over cleverness". This shadowy existence of crime, which lies apparently concealed, makes the study of cyber crime interesting as well as challenging.

## **A LOOK THROUGH CYBER CRIME**

**T**he best way to evolve preventive and detective techniques

towards any crime is to first understand the genesis and the modus operandi of the crime. The series of steps involved in the preparation and the commission of the crime provide "detective trails". The thorough audit would simultaneously hint at the plausible domains of crime prevention.

Cyber crime is no more a new phenomenon as it used to be a few years ago. The virtual world of cyber environment has permeated through the various facets of our life. Computer environment is the combination of the physical machine set up of computers, its peripherals and the logical environment built up through the software. Cyber crimes are the deviations from the "permitted cyber-culture" which may take the following shapes:



- Breach of accessibility/diluting the reliability.
- Breach of identity/ tarnish the authenticity.
- Breach of trust and privacy.
- Wrongful loss of information.
- Damage to the data base (sabotage) by outsiders.
- Subversion (by the incharge of the data base).
- Infiltration in the data base through virus or other means.
- Use of improvised programmes or modules to cause wrongful loss.
- Interrupting the transactions on the net.
- Wrongful propaganda on the net.
- Physical loss or damage to the system.

Extending the logic of the real world, as propagated above, the virtual world has categorized the computer crimes as-

1. 'Data diddling', computer fraud by input manipulation.
2. Programme or module manipulation.
3. 'Salami technique', thin slices of financial transactions being moved from one account to the other.
4. Output manipulation through falsified electronic information.
5. Computer oriented forgery.
6. Use of virus, worms or logic bombs through series of computer codes or programmes, which attach themselves to legitimate programmes and later spread out in the system to damage it.
7. Unauthorized access or 'Hacking' for the purpose of sabotage or espionage.

8. Use of 'cracker' programmes for illegitimate encryption or access to any data base.
9. Using "Trapdoor" method for unauthorized access.
10. Software piracy-
  - Hard disk loading by dealers.
  - Softlifting through unauthorized copies of one legitimate copy.
  - Software counterfeiting.
  - Bulletin board piracy through internet.
  - Manipulation of software through rentals.

The functional or the impact oriented classification of the above computer crimes can also be depicted as follows, for better understanding across the traditional classification of crime:

- Economic offences through computer data manipulation or frauds.
- Abuse of electronic mail and stalking.
- Pornography and child abuse.
- Gambling and betting
- Electronic impersonation through spoofing and masquerading.
- Harassment and threats.
- Cyber terrorism through terrorist destructive activities.

### CYBER INVESTIGATIONS

**H**aving understood the basic nature of crime, one can now harp on the investigative techniques, which are basically no different than the detection trails or the general 'audit' procedures adopted in case of any other crimes. Since cyber crimes are specific to a given environment, as defined earlier, certain pre-requisites are to be well understood for proper investigation.

### TECHNICAL KNOWLEDGE

**K**nowledge of the computer hardware and software systems is an essential pre-requisite to develop a vision for an accurate plan of investigation. How the database is created, how the file system is maintained, how the damage or data recovery programmes function, how the data is transferred on computer network of all types - this basic knowledge will help to foresee and develop the detection trail. An investigator ought to know how the system can be accessed to retrieve data, hidden files, duplicate records, data transfer details and so on. Similarly, the machines and records of Internet Service Provider (ISP) can give time-wise details of data transfer or access to the data base on internet.

In order to secure identity and maintain the authenticity, digital signatures have been devised. The uniqueness of such a system is a positive step in investigation. This technical knowledge can be gained either through direct learning or training to investigating officers or by hiring computer experts to assist them.

### LEGAL KNOWLEDGE

**C**omputer crimes have no binding or limitation as to the space. Through networking, the scene of crime can be any input-output terminal on the virtual world or the 'cyber space'. Hence, cyber crimes may have global dimensions. Many countries have come out with the cyber laws including USA, UK and Japan. India promulgated the law on the subject in the year 2000.

Besides the legal provisions, the computer professionals have also been bound by ethical codes and standard practices at the global level by agencies like International Federation for Information Processing (IFIP), and in India by CSI (Computer Society of India).

These codes go a long way as moral checks and also help in knowing the “forbidden acts”.

It may be reiterated that general criminal legislations like IPC, CrPC and Evidence Act would also apply in so far as they are not inconsistent with IT Act 2000. In India, any cyber offence is to be investigated by an officer of the rank of DySP or above.

### ART OF EVIDENCE COLLECTION

This aspect is dependent upon the combinations of technical as well legal dimensions as discussed above. One should be familiar with the specifications of the machines and input-output devices or means of storage so as to understand what not to do and what exactly to do in order to save a device and not commit any act in ignorance so as to destroy the evidence. Legal aspects including the legal presumptions and the interpretation of computer related evidence have been spelt out in the new IT Act of 2000. Electronic document has been made admissible and relevant to prove a fact. The computer filing, loading, copying and back up record keeping, etc., all become relevant as per system specifications and the software usage. They may be further supported by the evidence of experts local witnesses and networking details. The soft copies may also be converted into hard copies and authenticated as supportive evidence.

### BEHAVIOURAL SKILLS

One may have to interrogate the system operators or the administrator. So also the system providers or those who maintain it and upkeep network connections. Besides using legal powers, one has to be dexterous in behavioural skills in order to extract the informational links. The knowledge of cyber functioning provides an advantage in cross-

verification or interrogation on positive lines.

### KNOWLEDGE OF COMPUTER FORENSICS

In order to fully appreciate the investigative procedures, an attempt has been made to depict the dimensions of computer relevant forensics so that the evidences pertaining to cyber crime can be detected and collected properly.

### IMPORTANT STEPS

#### (a) Examining hardware and operating systems of the computer machines:

- Inspection of computer systems and computer networks.
- Making non-functional computer systems operational.
- Cracking passwords.
- Hard disk copying and imaging.
- Backing up data from computer systems at the search or inspection site.
- Examination of audit trails.

#### (b) Data Recovery:

- Examination of various storage media for data.
- Recovering erased data from disks.
- Duplicating or converting data files from multi-user systems.
- Locating hidden files or disguised data.
- Decrypting encrypted data.
- Recovering data from virus-infected files.

#### (c) Data Analysis:

- Understand the information need.
- Group together the files or data.
- Draw logical conclusions.

### SPECIFIC TOOLS

1. Check the system:
  - System information
  - Data tools/recovery modes
  - Desk editor
  - File allocation tables
  - System entitles like unformat or unerase
2. Make use of investigative software:
  - PC-Investigator - it helps in investigating the suspect computer (IBM compatible).
  - Forensic Internet Evidence Recovery and Search Tool - a complete hardware.
  - Software package for evidence retrieval from a personal computer (IBM - compatible).
  - Password Recovery Software-software tool kit for recovering lost passwords.
3. Look for Internet usage:
  - Cookies that could give information on the Internet sites recently visited.
  - Temporary Internet Files that may contain copies of the recent Internet files accessed.
  - History (containing Internet sites visited).
  - E-mail: inbox, outbox and sent box where copies of e-mail exchanged, incoming and outgoing, would be stored in the folders.
  - Recycle Bin that would contain copies of files recently deleted before they are purged from the system.
  - Thus cyber crime Investigation needs proper knowledge. There is nothing great or big

about it. A proper bent of mind would help acquire what is necessary.

## CYBER CRIME PREVENTION

Prevention of any crime is basically dependent on its detection and prosecution. The fear of being caught and really punished is a great deterrent and thus an effective tool for prevention. All other methods, in absence of the above, can only delay the commission or avoid the happening to an extent. The game of wit on either side, i.e., the offender and the system controller prompts constant search for effective methods to browbeat the other.

The domains of cyber crime prevention, besides the detection, fall under the hardware and software arenas of the cyber world. A couple of such techniques can be seen as under:

- Ensuring physical safety of the computer systems.
- Access control through identity verification, password, usage restriction.
- Use of anti-virus software.
- Use of data dictionary for specific interpretations in a given computer system.
- (a) In case of internet usage, make use of site integrity controls like 'firewalls' (hardware and software combinations to protect from hackers or crackers on the net). One may use video-conferencing methods also for surety of the deal on internet.

Non-repudiation alternatives also provide safety measures against deceit or cheating.

(b) Secure electronic transactions through digital signatures and proper encryption techniques, i.e., take confidentiality measures besides ensuring authenticity.

(c) Use of secure socket layer (SSL) protocol architecture for multilayer protection. New clustering technology such as elliptical encryption (EEC) can also be used. Intruder detection systems (IDS) are also available with multi-sensors to check the intruding programmes and kill or neutralise them.

(d) Earlier, voice and fingerprints were thought as secured systems. But in certain cases, they are also not fully secured. Now the biometric technology in form of human iris textures is being developed. No two persons can possess identical iris textures or patterns, claim the scientists.

The increasing use of e-commerce calls for effective net policing. It involves, besides the above, all measures towards the surveillance, i.e., tracking certain known users or look for certain dangerous signals or programmes. Various types of sensors are available to scan the 'robbers' on the net. So also look for sites violating prevalent laws or selling 'objectionable'.

Thus we can see the three-fold dimensions of cyber crime prevention-

1. Detection and conviction.
2. Precautions by netizens.
3. Net policing or surveillance.

The basics are, nevertheless, the same.

## CONCLUSION

The cyber world is highly dynamic. Before one digests the new formats, it gains newer formats. It may be very difficult to be proactive as a 'watchdog' in the virtual world amidst the scenario of rapid change. The virtual world is highly holistic and calls for real time copability. Indian police has procured the hardware and the software but we still lack the proper "thoughtware". We have not yet evolved with the "logical world" provided by the computer systems. One may not like it, but that is a truth. My humble focus would first be on our "thoughtware". Rest will follow suit.

## REFERENCES

1. Joseph Ponnolly "Investigation in a Computerized environment- Searches & seizures", CBI Bulletin, June 1997.
2. Computers Today: . 'Security is never enough', 1-15 Nov'2000, page 54. 'An eye on the security', 16-30 Sept' 2002, page 74. - Identity assured,' 16-31 March, page 92.
3. Dr Sushil Kumar Sharma, 'Threats for Electronic Transactions', Indian Institute of Management, Lucknow, Lecture notes 2000.
4. Web Site - WWW:forensicsdynamics.com.
5. Peter Stephenson- 'Investigating computer related crime', CRC press, Florida, 2002.

# STRESS IN INDIAN POLICE

M Madana Mohan

## INTRODUCTION

**I**t was around 0100 hours of the intervening night of May 23, 1991. I (then a young Additional Superintendent of Police of Agartala city in the North Eastern state of Tripura) was sitting in the chamber of the Station House Officer of East Agartala Police Station discussing the next day's police deployment with the SHO. We suddenly heard a lot of noise of scuffling from the adjoining Duty Officer's room. We immediately rushed there and noticed to our utter horror a constable pointing a loaded and cocked .303 rifle at the temple of a Sub Inspector of Police and about to shoot him. We all intervened and overpowered the Constable. I had known the Constable (in his 40s) for about 3 years. He was a very sober, obedient, sincere, hard working and

honest officer. I was personally shocked at his behaviour. So, I asked the SHO to check up the true reasons for his abnormal behaviour and requested for a feed back that very night. The SHO's feed back was very revealing.

The SHO reported that the Constable was weeping inconsolably after he realized his mistake. He could not comprehend what and how he had done it. It was the fifth continuous day of duty without rest for him. Due to the Parliament Elections, he was being deployed both during days and nights continuously. On May 21 former Indian Prime Minister Rajiv Gandhi was assassinated in Tamilnadu state and curfew was imposed in Agartala city immediately as violence had broken. So, the police had to be continuously deployed without rest or replacement.

The constable was being continuously deployed at a place where he had no place to sit or have even water to drink. So, he requested for a change of post from the Duty Officer who was helpless in obliging due to constraints of the situation. When the request was turned down, the constable reacted in an extreme way. It was the physical and the mental stress that he could not cope with, which were responsible for the reaction and not the original self of the constable. The moot point here is whether any other profession including the army faces such a kind of stress.

The vivid example above is not unique. My police colleagues can narrate 'n' number of their experiences at least in Indian context where stress has been taking its toll not only of the individual concerned but also of his colleagues and the citizens he serves. We are aware of incidents of junior colleagues shooting down senior officers and policemen going on rampage in civilian areas. More than any service or job, the police service has the highest level of stress and maximum consequences. As such it is worth understanding it to manage it well.

## WHAT ARE STRESS AND STRESSORS?

According to Brian Clegg (2000), stress is the impact of a demand on a human being. The source can be external or internal. The demand can be positive or negative.

Selye (1956) defines stress as the body's non-specific response to any demand placed on it, which may ultimately lead to the diseases of adaptation. Ruben calls it a generalized arousal of the psycho-physiological systems, which, if prolonged, can fatigue or damage the systems to the point of malfunction or disease.

Klarreich (1990) defines stress as a non-specific physiological and psychological response to events which

are perceived as a threat to one's well being, and are thus handled ineffectively; and stressors are basically events, situations or changes one encounters either in his life or his personal life.

According to Cox (1978) stress...can only sensibly be defined as perceptual phenomena arising from a comparison between the demand on the person and his ability to cope. An imbalance in this mechanism, when coping is important gives rise to the experience of stress and to stress response. The latter represents attempts at coping with the source of stress. Coping is both psychological (involving cognitive and behavioural strategies) and physiological. If normal coping is ineffective, stress is prolonged and abnormal responses occur.

Stress is normally referred to in the negative connotation. It is perceived as harmful and unhealthy. Stress is associated with distress. We often hear people saying 'Stress Kills'. In fact, stress has both positive and negative aspects. Stress is a driving force in life. The positive stress that is beneficial is called Eustress and it helps us to forge ahead against obstacles (Selye 1974). But beyond a point and at unmanageable levels, it becomes counterproductive.

In the modern day life, stress is an inevitable angel-cum-evil. In police service, it has reached unimaginable proportions. It is believed that the stress levels the Police Officer is exposed to in one year is more than the average person receives in one year. According to Selye, some occupations are more likely to cause stress-related maladies than others. Police work is one such occupation. Unlike most professions, it ranks as one of the most hazardous, even exceeding the formidable stresses and strains of air traffic control. We are concerned with the negative stress that has negative implications for not only the police service but for the whole society. If you cannot avoid it, learn to

live with it. So, it is worth making an attempt to understand what are the various stressors that cause stress in police officers.

## STRESSORS IN POLICE SERVICE

The Police Service is exposed to stressors from various sources. They can be broadly categorized into external and internal stressors. The external stressors can be further categorized into (1) Societal (2) Systemic and (3) Political. The internal stressors are (1) Individual (2) Family (3) Task and (4) Organizational.

### A. EXTERNAL STRESSORS

**Societal Stressors:** The society looks to the Police officer as a messiah and a superman who can do any amount of work and solve any problem of the common man. It expects him to be omnipresent and omnipotent. In the process of its self-interest, the society forgets that the police officer is also an ordinary human being requiring normal rest and having human limitations like anybody. The Police Officer also, according to the Labeling Theory of Sociology, tries to live up to the macho-image imposed upon him. Sometimes, he has limitations of the legal framework in which he has to operate, his original capabilities and the professional training he has received to handle such situations. He cannot always live up to his own expectations or the expectations of his clientele, i.e., the citizens. In the process, he feels guilty and faces stress. It is often seen that a common man or woman comes to the police station with a civil dispute or an offence of non-cognizable nature. When the SHO expresses his inability in the matter, the complainant thinks that the police are in league with the opposite party, which is more powerful.

The 'traditional Indian society in transition' is full of conflicts between traditional values like caste/clan-affinity,

village loyalty, etc., and modern values like objectivity, impartiality, etc. The crowd around him expects him to dole out favours as a matter of right as the policeman is his village-mate or country cousin or of the same caste, etc. But the organizational ethics and legal framework expects him to work rationally and not emotionally. These conflicts act as stressors on police officers. The same society entertains a very negative opinion about the performance and is generally not very cooperative to him in discharge of his duties. This puts a lot of stress on the police officer during his work. The police officer being a member of the same society faces these two opposite pulling pressures viz., macho-expectations and adverse opinion, leading to stress. The status that the society ascribes to a police officer is incompatible with the current pay structure. Trying to match the two by hook or crook, some officers face stress.

**Systemic Stressors:** The system emanates from the society itself. So, the stressors from these two sources tend to overlap. The legal framework guiding the Indian Police, which basically does not trust the police is another stressful factor for police in the Indian context. The evidence of a criminal is accepted in a court of law and not that of a Police Officer. The Indian Police is governed and guided by the Indian Police Act of 1861 and other outdated laws that are a British legacy. The British rulers did not give us the 'democratic model of policing' of Lord Peel that they have adopted in their country. But, they gave us the 'colonial model of policing', i.e., Irish model basically as an agency of social control with an anti-people slant. But the supreme law of the land, the Constitution of India that is one of the most forward-looking documents of the world expects the Indian Police to be an agency of social change. The subsequent enactments of our legislatures aimed at social change have put onerous responsibility on the police. Added to this, the judiciary, the media and the senior officers keep on exhorting

the police officers to enforce the law of the land only and nothing else. But the police tied down by the systemic shackles are unable to live up to not only its own expectations but also those of the founding fathers of the Constitution and the citizens of this nation. This leads to a lot of internal conflicts and stress in the police officer.

Sometimes, some police officers tend to break the systemic shackles and deliver goods in good faith. But the ungrateful system tends to chase that individual once his contribution is forgotten. We have not forgotten the suicide in frustration by a Punjab Police Officer, a Senior Superintendent of Police (late) Sidhu, who was acclaimed as one of the best officers during the fight against the Punjab extremism. After normalcy was restored in Punjab, Sidhu-like officers were chased by the system, which was nonfunctional in Punjab when there was war like situation there.

**Political Stressors:** The Indian democracy, which is more than 50 years old, is still to mature fully. The present political masters like their British predecessors still expect the police to serve their political ends even at the cost of the large societal interests. More often than not, police officer faces demands from the political executive, which in a democratic society is supposed to represent the popular will, that come into conflict with the charter of duties laid down by the laws of the land and the expectations of the citizens. This perceived or real political intervention with a potential career discomfort in the event of the political executive being unhappy gives a lot of stress to the police officer.

## B. INTERNAL STRESSORS

**Individual Stressors:** The perception of stress is highly individual. What is stressful to A may not produce stress in B. It depends on the person's previous experiences, emotional/psychological

state and his evaluation of the situation. The Type A personality officers in police service face more stress in a given situation compared to Type B personality officers. The level of stress also depends on his success to keep his official and personal life separate and the ability to rationalize the contradictions in his job. In view of the grave security situation that the police officer faces every day, he is concerned about his own security leading to constant undercurrent of stress. Whenever he operates in extremist or insurgency situations he is up against an enemy who employs guerilla tactics. The police officer has to succeed always and the extremist has to succeed only once that will cost the former's life. The element of surprise always lies with the extremist. It is easy to talk of the supreme sacrifice at the altar of duty for the motherland. But I am sure all police officers are also employees who have joined to earn a livelihood. Every one of them always indulges in wishful thinking that the extremist bullets will not hit them. But the professional in him always keeps indicating that 'it' can happen to him. This undercurrent/subterranean feeling of insecurity coupled with the uncertain future of his family in case of any eventuality while discharging the onerous responsibilities is a constant stressor. Other stressor is the concern about his own ability and the doubts about the adequacy of his training to cope with the emerging complex security challenges.

**Family Stressors:** The demands of the family and the job demands of a police officer tend to conflict most of the time. Like any family, the police family expects him to devote enough time for them. But the Indian Police Officer at the lower level works on an average for about 13 hours and is available on call round the clock (BPR&D, 1999), where as, the world over the police officers work in 8 hourly shifts. As a result, the Indian Police Officer is unable to do justice to his family and consequently faces stress. This is mainly due to the role conflict, i.e., the conflict

between various roles of the police officer at the same time – police officer, father, husband, son, friend, etc. Some of the families tend to put unreasonable demands and prod the police officer to resort to undesirable ways in the job to earn more and compensate for the ‘extra time’ he puts in the job. This leads to a conflict within the police officer leading to a lot of stress.

**Task Stressors:** Terry (1981) talked of exposure to violent situations, witnessing distressing events and seeing victims of child abuse as some of the task related stressors. Indian police officer is often exposed to the above types of situations in the course of discharge of his duties and gets stress as a result. The changing security situation in the country has thrown very complicated situations before the police officer. The various insurgent groups in the North East India, the terrorist activities in Kashmir, the Left wing extremist activities in more than 10 states, the Pak ISI sponsored anti-national activities and the ever-increasing underworld operations have been offering new professional challenges to the Indian Police Officer. The Police officer at one level is expected to operate computers and at the other level is to handle decomposed dead bodies. He is supposed to know all kinds of law, all techniques of public relations, every aspect of field craft and tactics to handle extremist operations, principles of VVIP security, intelligence trade craft, effective management of politicians and bosses and what not? Any thing and every thing that concerns other departments and that does not concern other departments is a baby of the police. A child falls into a ditch, the policeman is called. There is flood, he is called. Police is expected to be a panacea. Is it humanly possible for one person to know every thing of every thing? So, the ill equipped and ill trained police officer especially at the lower level feels very frustrated and thus faces a lot of stress.

**Organizational Stressors:** The very nature of police organization gives birth to many stressors. There are **Routine/Operational Stressors** like attending to a scene of death, violent confrontation, grappling with a chaotic traffic jam, work overload, fear of attack any time during police operations, etc; **Traumatic Stressors** like an ambush/ encounter/being taken hostage; and **Structural Stressors** like suppression of creativity/initiative in the name of discipline, lack of personal recognition, frustrated ambition, autocratic management, etc. Stagnation in a particular rank for a long time is a great stressor. This is more pronounced at the lower ranks. Incompatible boss in a hierarchical and highly disciplined organization like police service is a great stressor. A boss whose basic values are at great variance with those of the concerned police officer, especially on core issues like integrity, moral values and Human Rights causes a lot of stress. There are instances of officers getting blood pressure, diabetes, etc, with such bosses. Brown and Campbell (1994) listed out 3 classes of ‘**Traumatic Incident Stressors**’- (1) Criminal injury or violence to self and others (2) Dealing with disasters, accidents, mutilations and fatalities and (3) Public Order situations like policing demonstrations, crowd control (managing huge political meetings/*kumbh melas* with millions of people) and keeping order.

## EFFECTS OF STRESS

The stress in police has multifarious implications - (1) Individual (2) Familial (3) Interpersonal (4) Organizational and (5) Societal levels.

**1. Individual Level:** At the individual level it has both physiological and psychological effects on the police officer. Due to the factors discussed earlier, a particular police officer may start feeling that he has been a failure on all

fronts – personal, professional and as a family man; and the entire cost has been paid for no gain of any sort – even the society does not recognize his sacrifices. In such a situation, his peer group consisting of colleagues and immediate superiors are the last straw. When he perceives injustice even at their hands, may be real or just perception, the dam of patience/restraint/ discipline breaks leading to ugly incidents like shooting down of colleagues. The pent up frustration finds expression in many more ways. He suffers from sleeplessness, guilt, self doubt, lack of concentration, irritation, drop in morale and performance, etc. Prolonged stress leads to psychosomatic disorders like anxiety neuroticism, depression, stomach upsets, stomach ulcers, cirrhosis, high BP, diabetes, head aches, cardiovascular problems, etc. The individual police officer resorts to escape strategies like drinking, smoking, drugs, etc.

**2. Family Level:** At the family level it has implications for the entire future of the children and wife. Wife beating by police officers is a result of excessive/ prolonged stress. The addictions mentioned above have huge economic costs for the family and the society. Sometimes the stressed police officer commits suicide, which is a catastrophe to the family.

**3. Interpersonal Level:** Sometimes the peers/colleagues of the stressed police officers pay a very heavy price. We keep on hearing incidents of policemen shooting down in frustration his junior or senior colleague. We are also aware of the stressed police officers going on rampage in the neighbourhood.

**4. Organizational Level:** Stress among police officers has taken a heavy toll of the over-all efficiency of the police service to the common man. This has led to poor quality of police investigations, poor image of police in the mind of the general public, organizational indiscipline, poor work culture, etc.

**5. Societal Level:** The Societal implications of Police Stress are very significant. Inhuman behaviour towards the common man by the police officers, custodial violence, Human Rights violations, etc., are a result of stress. The reduced police performance has a long-term impact on the security situation and consequently on the overall development of the society.

**6. Economic Level:** The stress has taken a heavy toll on the economic condition, both at the macro and micro levels. The Police Officer suffering from the effects of stress has to spend a lot of money on the medical front. The coping or escape mechanisms of the stressed police officer

like smoking, drinking, drug addiction, etc., are a big drain on the purse of the family. At the macro economic level, the loss of man-hours and decrease in the efficiency of police officers affects the society.

#### CONCLUSION

**W**e have seen above that the police officers face a lot more stress than any other member of the society. In view of the very crucial nature of duties the police performs in the society, it is in the interest of everybody in the society to ensure that the stress and the stressors among police officers are managed well. Becoming aware of the problem is finding

half the solution. We need to work out strategies to use positive aspects of stress to enhance the performance of police service and handle the ill aspects of stress.

#### REFERENCES

1. "Instant Stress Management" by Brian Clegg (2000)
2. "Stress Management in Police" by Anil K. Saxena (2000)
3. "Thrive on Stress" by Robert Sharpe (1984)

\* Your reactions to this article may kindly be mailed to [madanamadana@yahoo.com](mailto:madanamadana@yahoo.com).

*It is good discretion,  
not to make too much  
of any person at the first,  
because one cannot  
hold out in that proportion*

**Bacon**



# QUALITY AND COST OPTIMIZATION IN POLICE WORKFORCE

Nawal Bajaj

## INTRODUCTION

**P**olicing in India in its current form started after the Penal Law was drafted and written by Lord Macaulay in 1861. The format of the police force at that time was drafted in accordance with the requirements of the British Raj to govern a foreign colony. Since safeguarding the commercial and financial interests of the British Government took the top-most priority, the structure of the police force was formulated accordingly. Bulk of the force (almost 99%) consisted of the lowly-paid native constabulary working under the “bourgeoisie” British officers. This accomplished the dual tasks of firstly, maintaining complete control over the country by using a minimum number of Englishmen in the service and secondly, cutting on expenditure by employing the large native work-force at a pittance.

Obviously the social and economic growth of the native people and the country was not a priority and thus suffered a major setback.

Post independence, with the local government taking over, the priorities of the government metamorphosed to adopting a more progressive and welfare oriented outlook. The rationale behind the working of the police force also underwent a change, effectively transforming the “Police Force” into a “Police Service”. Over the past 55 years the efficacy and “Quality of Policing” has raised many a question which need to be addressed. Also, while working within the parameters of the ground reality, it has to be kept in mind that this much required enhancement in “Service Quality” has to be done within the, available finances.

## SERVICE QUALITY

The aforementioned historical factors along with the low salary, ensured the poor professional development of the native Indian policemen under the British. In order to have complete and unquestioned control over the Indian masses, the British intentionally popularised the concept of the native work force being incompetent and corrupt and hence not worth of giving any work of responsibility. Therefore, all major powers were retained by the officers which incidentally, consisted of almost 100% British officers.

After independence, we still find that the same structure remains with only a marginal increase in the number of officers (up 5%). The constabulary still works with the same mindset and the same perceived limitations. This has resulted in complete demoralisation of the constabulary over the years under the British as well as the Indian officers. This demoralisation has set in to such an extent that it is now presumed that a constable in the police department suffers with the following:

i) low self esteem, ii) low morale, iii) low motivation, iv) poor leadership qualities, v) poor training, vi) poor personality development, vii) less promotional avenues, viii) low salary, ix) low social recognition, x) less intellectual capacity, etc.

All the above are symptoms of a major illness which ails the constabulary in the police department. With these problems facing the constabulary, it cannot be expected that high quality service is delivered by them. Moreover, this large percentage of constabulary (95%) with its inherent problems, is also resistant to any organizational change in the department, thereby preventing rapid modernization of the force.

## COST-BENEFIT RATIO OF SERVICE

Every service is seen in terms of cost and benefit. Cost-benefit ratio of a service should be in the favourable range. This range is determined by the cost of a particular service, that a country can afford. For e.g. the cost incurred by the Government on a Policeman in England is 20 times higher than that incurred in India. Hence, the state of economy determines what is the "favourable range" and how much the State can afford, to spend to maintain a Police personnel.

Hence, taking all the above factors into consideration, i.e., financial constraints and the basic factors ailing the constabulary, a model is proposed to maximise the quality of service provided, by replacing the entire constabulary by officers in the regular (civil) police duties without any increase in expenditure incurred by the State.

### SCHEME OF THE MODEL

Total workforce of Pune Poice (Annexure-1)

No. of Policeman (Constabulary) = 5668

No. of Officers (PSIs and above ranks) = 465

Total cost incurred per month on the constabulary (5668) of Pune Police during the year 2001 = Rs.5,20,27,965/- (Annexure-2, Annexure-3) (includes pay, allowances, pension, medical and other benefits).

Total cost incurred per month on the officers (465) of Pune Police during the year 2001 = Rs.80,09,969/- (includes pay, allowances, pension, medical and other benefits).

Average cost incurred (gross pay) per officer

$\frac{\text{Total pay of all officers}}{\text{Total No. of officers}} = \frac{\text{Rs}17,295/-}{\text{per month}}$

Hence, keeping the cost incurred on the constabulary the same, the following no. of officers can be recruited to replace the constabulary.

Total monthly pay of the entire constabulary of Pune Police-

Average monthly pay of one officer of Pune Police  $5.20.27.965/- = 3008.17,295/-$

Therefore, the total no. of officers which can be recruited is 3008, (approx.), (after completely replacing 5668 policemen (constabulary).)

Certain areas, especially handling of law & order situations, require specialized training and availability of large manpower. For this, it is proposed that detachments completely dedicated to the local civil police unit should be earmarked from the State Armed Police Force Battalions/Groups already existing (as S.R.P.F in Maharashtra). These armed detachments may be continued with the same organizational structure (i.e., officers and men). These detachments can be kept at the Battalion/Group headquarters or at the local civil police headquarters. The training and development of these units shall be exactly on the lines of the armed reserve police of the state. These units shall be called whenever necessary for handling law & order situations or other problems requiring large manpower/show of force. Apart from this, ready manpower as is available in the form of home-guards/civil defence groups, etc., can also be considered for use. Their strength may be increased at the cost of savings done from the reduction of the constabulary in the civil police force, which is proposed in the model.

For the large number of personnel (additional home-guards/civil defence over and above the already existing) for bandobast and law and order duties, a sum of Rs.21,00,000/- from the total of Rs.5,20,27,965/- is kept aside for

requisitioning 1000 extra home-guards/ civil defence personnel (per month). (calculated on the basis of the existing pay of a home-guard, which is Rs.70/- per day or Rs.2100/- per month).

Therefore, the number of officers which can be recruited is reduced to

Rs.49927965 = 2886 (approx)  
Rs.17295  
(Rs.5,20,27,965/-Rs.21,00,000=Rs.49927965)

## METHODOLOGY

A questionnaire was administered to 55 officers of the rank of Inspectors/Sub-Inspectors/Asst. Police Inspectors working in various Police Stations of Pune city.

The Questionnaire consisted of 21 questions and was prepared to assess the difference in the levels of efficiency (read quality) between the two ranks, i.e., officers and constabulary. The comparison was based on certain key performance parameters.

## PROFESSIONAL PARAMETERS

1) Accessibility, 2) Pro-active behavior, 3) Impartiality, 4) Reaction time, 5) Managing Organizational Change, 6) Innovation at work, 7) Quality of investigation, 8) Handling of law and order, 9) Preventive action, 10) Intelligence collection, 11) Response.

## PERSONAL PARAMETERS

1) Motivation, 2) Courage, 3) Morale, 4) Overall skills, 5) Discipline, 6) Initiative, 7) Training, 8) Self esteem, 9) Personality.

The officers were asked to rate each parameter on a scale of (8) and on that basis, assess work-equivalent (of the no. of constables), that can be done by a single (directly recruited) officer.

The entire set of questionnaire was then analysed statistically using various statistical tools.

## STATISTICAL ANALYSIS AND RESULTS:

The analysis of data was done using the following statistical tools :-

- a) Descriptive Statistics:- Calculation of mean and standard deviation.
- b) Pearson's correlation co-efficient (indicating the inter-relation between items in the questionnaire.)
- c) Reliability analysis of the questionnaire as a whole.
  - i) Alpha.
  - ii) Split half.

(Statistical analysis was carried out using SPSS Windows version).

The results of the statistical analysis are as follows.

- 1) The overall quantification of work equivalent is 1 :3.9388., i.e., one officer is graded equivalent to 3.9388 constables in terms of work output.
- 2) Most of the questions (except 0-3,12 &14) relate strongly to 0-21.

- 3) Reliability of the test is high. Alpha=0.9284  
Split half -Alpha for part-1 = 0.8830. -Alpha for part-2 = 0.8725.
- 4) Parameters indicating quality output, score in the range of 5.5 - 6.0 on the numerical equivalent scale.

## CONCLUSION

From the analysis of the data, it is seen that the Work-Equivalent of 1 Officer = 3.94 Constables, i.e., total work done by one officer is equal to that done by 3.94 constables. Hence, in spite of the reduction in manpower from 5668 to 2886 there is actually an increase in the total work output.

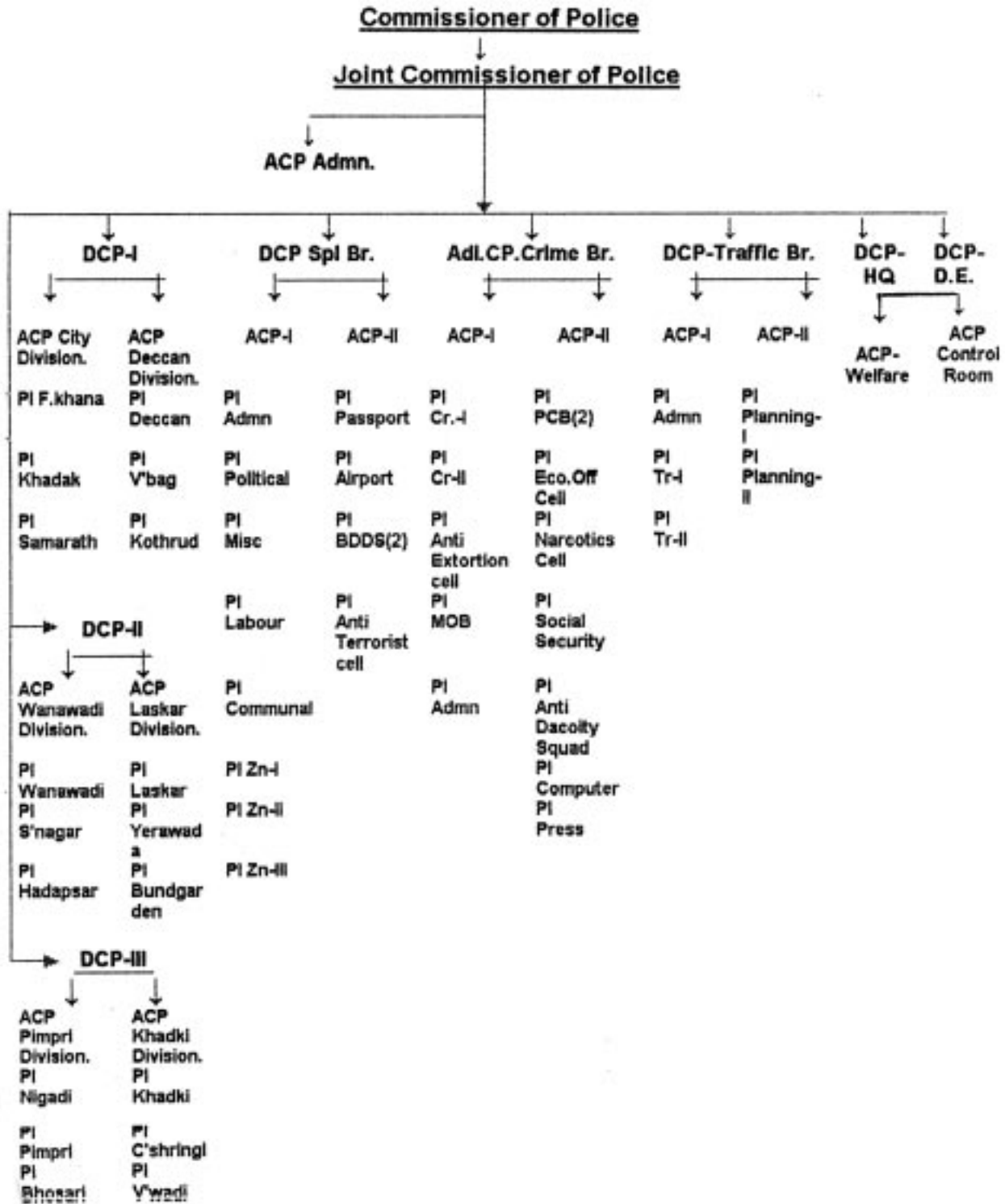
Similarly, analyzing the data on professional and personal performance parameters, it is seen that there is a marked difference in the quality of work done by an officer vis-à-vis a constable. Score of 5.5 - 6.0 on the numerical equivalent scale indicates a vast improvement in the quality of work output in an "all officer police force".

To summarise, if the above model is implemented, there will be both qualitative as well as quantitative improvement in the overall work output, keeping the expenditure constant.

Hence this model would be offering the public "VALUE FOR MONEY" policing.

**Annexure-1**

**Organisational Structure of Pune Police**



**ANNEXURE - 2**

**CALCULATION OF PAY OF POLICE PERSONNEL (RANK WISE)**

No.		No. of Policemen/Officer	Total expenditure per Month on one Policemen/officer	Total expenditure /month
1.	P.C.	3375	8073	27246375
2.	P.N.	786	10544	8287584
3.	H.C.	1088	10544	11471872
4.	A.S.I.	419	11986	5022134
	Total	5668		52027965

Total average expenditure on one policemen (Constabulary)  $52027965 = 9179.24/-$

-----  
5668

1.	PSI=API	358	16200	5799600
2.	PI	83	19601	1626883
3.	A.C.P.	14	23149	324086
4.	D.C.P.	7	25000	175000
5.	Addl.C.P.	1	33800	33800
6.	Jt.C.P.	1	37400	37400
7.	C.P.	1	45800	45800
	Total	465	210350	8042569

Total average expenditure on one officer (PSI & superior ranks)  $8042569 = 17295.847/-$

-----  
465

**ANNEXURE - 3**

**PER PERSONNEL (OF THE POLICE DEPARTMENT) EXPENDITURE INCURRED  
BY GOVT. OF MAHARASHTRA**

No.	Pay & allowances	ACP (P.M.)	PI (P.M.)	AI (P.M.)	PSI (P.M.)	ASI (P.M.)	HC (P.M.)	PN (P.M.)	PC (P.M.)
1	Average Pay	10750	9250	8500	7250	5750	5000	5000	3820
2.	D.A. 44.5%	4784	4116	3783	3226	2559	2225	2225	1700
3.	C.L.A.	240	240	240	240	150	150	150	95
4.	H.R.A. 15%	1613	1388	1275	1088	863	750	750	573
5.	Travelling Allowance	800	400	100	100	100	100	100	100
6.	Total of (1 to 5)	18187	15394	13898	11904	9422	8225	8225	6288
7.	Spl. Duty Allowance	Nil	Nil	Nil	Nil	Nil	20	20	20
8.	Leave Salary @ 11% of Col.6	2001	1693	1529	1309	1036	905	905	692
9.	Pension Contribution @ 10% of Col.6	1819	1539	1390	1190	942	823	823	629
10.	Clothing Allowance	50	50	40	40	20	20	20	20
11.	Supervision Allowance @6% of Col. 6	1091	924	834	714	565	494	494	377
12.	Free Pass Concession	1	1	1	1	1	1	1	1
13.	Cost of Arm & Ammunition	0	0	0	0	0	4	4	4
14.	Arms Allowance	0	0	0	0	0	50	40	40
15.	Accountermnt Allowance	0	0	0	0	0	2	2	2
16.	Total (6 to 15)	23149	19601	17692	15158	11986	10544	10544	8073

(Source :- Maharashtra Govt. G.R.F.D. No. MBV - 1182/9/Seva, dtd.1.4.2002)

# HUMAN RIGHTS & CRIMINAL JUSTICE ADMINISTRATION

AM Bhattacharjee

According to our Ancient Indian Constitutional Law (RAJADHARMA), two of the most important duties of the king (or the state) were (a) to punish the wrong-doer (DUSTASYA DANDAM) and (b) to protect and honour the good people (SUJANASYA PUJA). The system of Criminal Justice Administration was conceived and developed with admirable amplitude and magnitude in ancient India. These principles have very often been referred to, though not quite accurately, as DANDA NEETI, but this expression had also a more comprehensive connotation to mean the principles of governance of the kingdom or the State.

2. In modern India also, as in various other Countries, Criminal Justice Administration has, as its main objects,

adjudication of the cases relating to crimes, i.e., offences punishable by law, punishment of the offenders, prevention of such offences and protection of the people from the onslaught of such crimes or offences.

3. The thesis of Bentham, a Jurist of International standing to the effect that property and law were born together and shall die together is a half-truth. Property may be the root of many of the offences; but even if property, i.e., private property, is abolished, criminal laws would still be direly necessary to deal with various crimes or offences which are wholly unconnected with property. And from that point of view, the view of the ancient Indian Jurists (e.g. Narada, Brihaspati) is more accurate and comprehensive and the

view is that there are two branches of law and adjudication, one arising out of property (Dhana) and the other arising out of violence (Himsa). "Dwipada Vyavaharascaiva. Dhana Himsa Samudbhava".

4. To persons not versed in law the term "Human" in the expression "Human Rights" may be somewhat confusing. Animals do not possess any "Right" in the jurisprudential sense but only some duties have been imposed on us by our laws towards animals. e.g., Prevention of Cruelty to Animals Act. Rights can belong only to natural human beings or to such entities, like corporations or companies, which by law have been endowed with a juridical personality.

5. "Human Rights" are basically those rights of the Individual which are essentially or reasonably necessary for his sustenance, growth and development. The Protection of Human Rights Act, 1993, in Section 2(d), has defined "Human Rights" to mean "the rights relating to Life, liberty, equality and dignity of individual guaranteed by the Constitution or embodied in the International Covenants and enforceable by Courts in India" and the expression "International Covenants" has been defined in Section 2(f) to mean "the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights adopted by the General Assembly of the United Nations on the 16th December, 1966."

6. The real object and reasons behind these grandiloquent Charters including the Universal Declaration of Human Rights, 1948, were not that noble or laudable. When the voice of Marxism began to be heard and the Soviet Union was established and became a great power in and after the Second World War, the Capitalist or the Non-Socialist Block soon realised that they must change their role of mere collecting taxes from the people and arranging for

Defence and Post & Telegraph Communication and the like and must show concern for the people and their welfare. For if they do not, the egalitarian message of Marxism will win over the oppressed and the depressed classes and may finally provoke them to rise up in revolt. So, it was more for their own protection and survival, than for the real welfare of the People, that ruling coteries of the Non-Socialist Block decided to declare these Human Rights in several sonorous International Instruments, like

- (a) Universal Declaration of Human Rights, 1948
- (b) International Covenant of Civil and Political Rights, 1966
- (c) International Covenant of Economic, Social and Cultural Rights, 1966, and waves of other International Parchments started surging on.

7. Rights relating to life, liberty, equality and dignity of individual have been guaranteed as judicially enforceable rights in the Constitution of India in categorical terms and those provisions have over the years been expanded by the Supreme Court with spectacular amplitude and magnitude. Some more facets of these rights have been embodied in the aforesaid two International Conventions of 1966. But those would get the protection of the Protection of Human Rights Act, 1993 provided, as pointed out in Section 2(d), (extracted hereinbefore), they are enforceable by Courts in India. Are the provisions of these International Conventions judicially enforceable in India?

8. The position in India on this point is satisfactorily settled by a series of decisions of the Supreme Court spreading over a period of three decades. Reference in this connection may be made, among others, to the decisions of the Supreme Court in *Maganbhai Iswarbhai*<sup>1</sup> *Gramophone Co.*

of India,<sup>2</sup> *Valsamma Paul*,<sup>3</sup> *C. Masilamani*,<sup>4</sup> *Visakha*,<sup>5</sup> *Apparel Export Promotion Council*,<sup>6</sup> and *Githa Hariharan*<sup>7</sup>. The upshot of all these decisions is that once India is a Party to such an International Instrument, the provisions thereof would be enforceable in and by the Courts in India at the instance of any party aggrieved, provided nothing therein is inconsistent with the Constitution of India and any positive national law.

Therefore, all the provisions of these two International Conventions of 1966, on being ratified by India, became part of the laws of India to the extent those are not incompatible or inconsistent with the Constitution of India or any other national legislation. Those could not obviously be above, but could operate only subject to, our National Charter and could not also outweigh or supplant, any of our national laws, but could fully and efficaciously supplement the relevant provisions of our national laws. But now that these two International Conventions have received the Legislative imprimatur of the Indian Parliament by the Protection of Human Rights Act, 1993, the view has gained ground that the provisions of these two International Conventions, having now been legislatively implemented (as provided in Article 253 of the Constitution), would also outweigh all earlier inconsistent National Legislations.

9. But the efficacy of our Criminal Justice System has been seriously affected by our excessive solicitude for and over-zealous pampering of the individual Human Rights. Most of us are blissfully ignorant of our ancient Indian Criminal Jurisprudence which all along placed the interest of the society, the community or the State above the interest of an individual. For those of us who have obsession for anything occidental or western (and are blissfully ignorant of the wonder that was India), reference may be made to the maxims "Interest



Republicae Suprema Lex”, “Salus Populi Suprema Lex”, which mean that the interest of the State, and the welfare of the People, are the supreme laws. The Roman maxim “Necessitas Publica Major Est Qualm Privata”, meaning that the necessity of the people in general shall prevail over private interest, and “Interest Republicae Ne Maleficia Remaneant Impunita”, meaning that it is a matter of public concern that wrong doings are not left unpunished, may also be referred too. But we have sadly demonstrated our unfortunate failure to apply these principles, so beneficial to the society, in our Criminal Justice Administration. We may illustrate.

(A) “Everyone is to be presumed innocent until his guilt is proved” is trite commonsense. This is also specified in Article 14(2) of the International Convention on Civil and Political Rights of 1966. But the further gloss to the effect that “Guilt must be proved beyond all reasonable doubt.” is unwarranted in Indian Law, though the same has been out-stretched by us morbidly and almost to a breaking point as a result of our erroneous, but dogged, reliance on British precedents.

The word “PROVED” has been clearly defined in Section 3, Indian Evidence Act, 1872 and the same unmistakably makes it clear that “a fact is said to be proved when after considering the matters before it, the Court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists”. The two expressions, “probable and “supposition”, can leave no manner of doubt that under our statutory Law of Evidence, preponderance of probability justifying a supposition is sufficient for the proof of any matter in any trial, whether civil or criminal. The Evidence Act has not, even remotely, suggested

any different standard of proof for civil and criminal adjudications.

But the glitter of the “Golden Thread” that is said to run throughout the British Criminal Jurisprudence, culminating in the dictum of the House of Lords in Woolmington Vs. Director of Public Prosecution<sup>8</sup> to the effect that, subject to statutory provision and the defence of Insanity, the Prosecution must prove the guilt of the accused beyond all reasonable doubt, has governed the Indian Criminal Jurisprudence also for far too long and has made us oblivious of the stating fact that while the United Kingdom had no statutory Law of Evidence in India, however, the Statutory Law, being the Indian Evidence Act. 1872 has defined the expressions “Proved”, “Disproved” and “Not proved” succinctly and with perfect precision. It would be interesting to note that now in 1970 the Judicial Committee of the British Privy Council has ruled in Jayasena Vs. Reginam<sup>9</sup> that in a case governed by statutory Law of Evidence it would be entirely wrong to be governed by the Woolmington-dicta. It should be noted that the case in Jayasena (Supra) was from Ceylone where the provisions of the Ceylone Evidence Ordinance were in pari materia with those of the Indian Evidence Act. If that is the correct view, and we think it to be so then the Courts in India have all along gone entirely wrong and have gone on acquitting numberless guilty persons by applying a wholly erroneous view as to the proof of guilt in a criminal case. The catchy jargon that “Let thousands guilty escape, but no innocent be punished” has played havoc in our Criminal Justice System. If unmerited conviction is bad, unmerited acquittal may be worse, which goes a very long way to shake the confidence of the community/society in Criminal Justice.

The categorical and bold observations of Justice Krishna Iyer while speaking for a Three-Judge Bench in Shivaji<sup>10</sup>, have not been able to awake

us from the stupor caused by the Ghost of Woolmington<sup>8</sup> which is very unfortunately haunting us even today. The observations are as hereunder:

“Even at this stage we may remind ourselves of a necessary social perspective in criminal cases which suffers from insufficient forensic appreciation. The dangers of exaggerated devotion to the rule of benefit of doubt at the expense of social defence and to the soothing sentiment that all acquittals are always good regardless of justice to the victim and the community, demand special emphasis in the contemporary context of escalating crime and escape... The cherished principles or golden thread of proof beyond reasonable doubt which runs through the web of our law should not be stretched morbidly to embrace every hunch, hesitancy and degree of doubt. The excessive solicitude reflected in the attitude that a thousand guilty men may go, but one innocent martyr shall not suffer is a false dilemma... The evil of acquitting a guilty person light-heartedly, as a learned author has sapiently observed, goes much beyond the simple fact that just one guilty person has gone unpunished.

If unmerited acquittals become general, they tend to lead to a cynical disregard of the law, and this in turn leads to a public demand for harsher legal presumptions against indicted ‘persons’ and more severe punishment of those who are found guilty. Thus, too frequent acquittals of the guilty may lead to a ferocious penal law, eventually eroding the judicial protection of the guiltless. For all these reasons it is true to say, with Viscount Simen, that ‘a miscarriage of justice may arise from the acquittal of the guilty no less than from the conviction of the innocent...’ In short, our jurisprudential enthusiasm for presumed innocence must be moderated by the pragmatic need to make criminal justice potent and realistic.

(B) Our System of Justice has been branded, though in our view erroneously, as “Adversarial System”, where the conduct of the case is to be left virtually at the hands of the parties and/or their Counsel, and the Judge only having the role of deciding the admissibility or otherwise of the evidence sought to be produced and finally to pronounce judgement. We have failed to appreciate the wide and great powers given to the Judge to actively participate in the Trial in order to discover the truth and/or to obtain proper proof of material facts and to take a pro-active role during the Trial of the cases.

Section 165 of the Evidence Act, 1872 empowers the Judge with the right to put “any question he pleases, in any form at any time of any witness or of the parties about any fact relevant or irrelevant and may order the production of any document or thing; and neither the parties nor their agent shall be entitled to make any objection to any such question or order”.

Section 311, Code of Criminal Procedure, 1973 empowers the Court to summon any person as a witness and “the Court shall summon and examine or recall and re-examine any such person if his evidence appears to it to be essential to the just decision of the case”. Section 310 of the Code also empowers any Judge or Magistrate to “visit and inspect any place in which an offence is alleged to have been committed, or any other place which it is in his opinion necessary to view for the purpose of properly appreciating the evidence given at such Inquiry or Trial”. As has been pointed out by a Two-Judge Bench of the Supreme Court in *Ram Chander Vs State of Haryana*<sup>11</sup>.

“The adversary system of trial being what it is, there is an unfortunate tendency for a Judge presiding over a trial to assume the role of a referee or an umpire and to allow the trial to develop into a contest between the prosecution

and the defence with the inevitable distortions flowing from combative and competitive elements entering the trial procedure. If a criminal court is to be an effective instrument in dispensing justice, the presiding Judge must cease to be a spectator and a mere recording machine. He must become a participant in the trial by evincing intelligent active interest by putting questions to witnesses in order to ascertain the truth”.

Looking at the present scenario of escalating crimes putting Human Rights of the victims in severe jeopardy, there should be no doubt that the Courts today must not sit as a mere Umpire or a Referee only to declare as to “who has Won” or “who has Lost” but must take all steps to ensure victory of the party “who ought to have Won”.

(C) Section 24, Evidence Act is good enough to take care and to exclude all confessions caused by inducement, threat or promise. If Confession to Police by any Person is not voluntary, but caused by threat, inducement or promise, it ought to be and cannot but be, excluded. But even if the Court is fully satisfied that a confession is absolutely voluntary, still it must be excluded if it happens to be made to a Police Officer, but not so even if it is made to a debauch, lecher, or one who was convicted of a most heinous offence. This Legislative fiat virtually declares the police to be hoodlums, brutal and unreliable and renders a legislative judgement, so to say, and thereby indelibly, “stigmatise all police personnel horrendously affecting their dignity and thus violating their Human Rights to “Individual Dignity”. If confession to Police, which appears to be voluntary was allowed to go in evidence, there would not have been so many unmerited acquittals. A man commits murder by stabbing and then straightway goes to the Police Station with the blood-stained weapon and surrenders and makes a clear and voluntary confession that he has committed the murder. That would have

been the best possible evidence, but still must be excluded under the categorical mandate of Section 25, Evidence Act. That is not the Law in the United Kingdom, even though the English Law was the basis of the Indian Law. Do we then take it that British Police Officers are Angels, but the Indian Police Officers are Devils?

(D) An interesting point may be noted here to demonstrate as to how and to what extent, excessive and overzealous weightage to individual Human Rights are, or would be, going to affect the effective administration of Criminal Justice. Under Section 64 Indian Penal Code, in every case where the Court imposes a sentence of fine, the Court is also to direct by the sentence that in default of payment of the fine, the offender shall suffer Imprisonment for a certain term; reference in this connection may also be made to the provisions of Section 30, Code of Criminal Procedure, 1973. The American Supreme Court in *Tate Vs. Short*<sup>12</sup> and also in *Williams Vs. Illinois*<sup>13</sup> has held that since in such a case a convict who can afford to pay the fine can purchase his liberty by paying up the amount, but a convict who because of indigence or otherwise cannot pay the amount, would have to suffer imprisonment, the law on the point is squarely violative of the equality clause of the Constitution. This question however, has not yet been raised before the Indian Courts but if such a question is raised, and the Indian Courts readily accept the American view, our Criminal Justice Administration cannot but receive a serious jolt.

It may also be noted in this connection that under Article 23 of the Constitution of India, “Traffic in human being and beggar and other similar forms of forced labour are prohibited and any contravention of this provision shall be an offence punishable in accordance with Law”. There should be no doubt that a sentence of rigorous imprisonment is (as pointed out in Section 53, Indian Penal

Code) imposition of hard labour and, since no accused ever willingly agrees to undergo such rigorous imprisonment, the resultant Hard Labour is obviously forced labour and surely is neither free or voluntary labour. Amendment XIII of the American Constitution has taken proper and particular care to protect such punishment of rigorous imprisonment from the scrutiny of the provisions of the Constitution by using the words “except as a punishment for crime” in that amendment. It is doubtful whether imposition of such hard labour can at all be said to be an imposition of “Compulsory Service for public Purpose” within the meaning of Article 23(2). Such a question was in fact raised before the Indian Supreme Court in *State of Gujarat Vs. High Court of Gujarat*<sup>14</sup> where the Supreme Court however declined to treat the hard labour resulting from a sentence of rigorous imprisonment to be “Forced Labour” within the prohibition of Article 23(1) and has ruled that the expression “Forced Labour” has got to be read *Ejusdem Generis* along with the preceding expressions “traffic in human beings” and “beggar”. The Supreme Court has also pointed out that the convicts putting in “hard labour” under a sentence of rigorous imprisonment are paid at a prescribed rate for such labour, which would go to their advantage and benefit. We find it difficult to understand as to whether an offence or any violation of any mandatory provision is anyhow so solely on the ground that the offender or the violator has dangled out money to the victim. Be that as it may, so long the decision in *State of Gujarat*<sup>14</sup>(Supra) would be holding the field, the provisions for imposition of “Hard Labour” as a part of the sentence of Rigorous Imprisonment would continue to survive Constitutional scrutiny.

(E) The spectacular expansion of the life/liberty clause in Article 21 the Constitution of India as would emerge from the well-known Seven-Judge Bench decision of the Supreme Court in

*Maneka Gandhi*<sup>15</sup> in 1978 may also be said to have given a serious jolt to the law relating to bail under the Code of Criminal Procedure Section 437 of the Code of Criminal Procedure provides that when a person is accused or suspected of the commission of any non-bailable offence, he “shall not be” released on bail, “if there appear reasonable grounds for believing that he has been guilty of an offence punishable with death or imprisonment for life”. It cannot be disputed that “denial of bail” to the Accused would result in deprivation of his “personal liberty”. But the clear mandate in *Maneka Gandhi* (Supra) and in the catena of decisions following the same is that no person can be deprived of personal liberty except according to procedure which is “reasonable, right, just and fair”. Before the commencement of the trial, bail is ordinarily declined solely on the basis of the statements recorded in the First Information Report, the Case-Diary and some such records to which the accused or his Lawyer may not have any access at that stage or at all. Under Section 172, Code of Criminal Procedure, “neither the accused nor his agents shall be entitled to call for... nor... to see” the Case-Diaries. The accused also at that stage has no opportunity to demonstrate his innocence by adducing any evidence or otherwise, and, therefore, the entire procedure would be squarely against and hit by the *Maneka-dicta*.

Even before the decision in *Maneka Gandhi*(Supra), Justice Krishna Iyer in *Gudikanti Narasimhulu*,<sup>16</sup> decided about two months before *Maneka Gandhi* (Supra) observed in connection with a Bail matter that “the significance and sweep of Article 21 make deprivation of liberty a matter of grave concern and permissible only when the law authorising it is reasonable even handed and geared to the goals of community good and State necessity spelt out in Article 19.” This has been reiterated by Justice Krishna Iyer again in *Babu Singh*<sup>17</sup> decided six days after,

but without any reference to *Maneka Gandhi* (Supra), to which Justice Krishna Iyer was a party with a separate but concurring judgement. So whether before or after *Maneka Gandhi* (Supra), acclaimed to be a Landmark judgement making a sea-change in our Constitutional Law relating to Liberties and freedoms, the law on the point was settled to the effect that any law, like the law relating to bail, providing for deprivation of “personal liberty” can be valid only when it is “reasonable” and semantically, or even otherwise, nothing can be “reasonable” unless it is also “right-just and fair”

Some later decisions of the Supreme Court have also affirmed this position with irresistible emphasis. A Three-Judge Bench in *Hussainara Khatoon*<sup>18</sup> and also a Five-Judge Bench in *Gurbaksh Singh*<sup>19</sup> have ruled that no doubt can linger after the decision in *Maneka Gandhi*” that “the law as enacted by the legislature and administered by the Courts must radically change its approach to pre-trial detention and ensure reasonable, just and fair procedure”. In *Motiram*,<sup>20</sup> Justice Krishna Iyer has observed that our Criminal Procedure Code, though re-enacted as late as in 1973, “has largely left untouched ancient provisions on this subject incongruous with the preamble to the Constitution”. It has been urged that while it may be conceded that if an under-trial, accused of an offence punishable with death or life-imprisonment, is refused Bail on the ground that because of the grim prospect of such severe punishment or for other reasons, there appear reasonable grounds for believing that he, if released, would evade justice by abscondence or by jeopardising his own life or is likely to pollute the investigation or trial by tampering with the witnesses by threat, inducement or otherwise, or to endanger public order, his pre-trial or pre-conviction detention may be regarded to be “in the interests of the general public”, who are obviously interested in the proper investigation and

fair trial of offences. But otherwise, that is, if there is no reasonable apprehension of abscondence of or tampering by the under-trial, or of the investigation, or the trial, or the public order being otherwise adversely affected by his being at large, then in view of these decisions noted above, the provisions of Section 437, Code of Criminal Procedure, mandating almost automatic refusal of bail and detention of an under-trial before and during the trial, simply and solely on the ground that from the materials then on record, which at that stage are not expected to be legal evidence, or, at any rate substantive evidence, there appear reasonable grounds for believing that the under-trial is guilty of an offence punishable with death or life-sentence, without anything more, cannot be regarded to be a Law which is sufficiently "reasonable, right, just and fair" to survive the Constitutional scrutiny.

(F) It is also apprehended that another American law-jargon might go to affect our Criminal investigation and trial to a considerable extent. The Exclusionary Rule of Evidence is very much an American product and owes its origin to the IV Amendment and the XIV Amendment of the American Constitution, the former guaranteeing "the right of the people ... against unreasonable searches and seizures" and the latter prohibiting deprivation "of life, liberty and property without due process of Law".. It appears to be the settled Law in the United States that evidence obtained as a result of illegal search and seizure must be excluded from Evidence. The British Common Law rule that "the criminal should not go free because the constable has blundered" was not accepted by the American Courts.

In India, however, a long catena of decisions of the Supreme Court appears to have ruled out the Exclusionary Rule of Evidence. It appears to have been consistently ruled in a series of decisions

of the Supreme Court in *Sunder Singh*,<sup>21</sup> in *Radhakishan*,<sup>22</sup> in *Bai Radha*,<sup>23</sup> in *Shyam Lal*,<sup>24</sup> in *Natwarlal*,<sup>25</sup> that illegality of the search, by itself, would not be a vitiating factor. It has been pointed out that such a search may be resisted by the person aggrieved and that the illegality of the search may lead the court to carefully scrutinise the evidence so obtained; but beyond these two consequences, no further consequence would ensue. But a discordant note has been struck in a Two-Judge Bench decision in *K.L.Subbayya*<sup>26</sup> in 1979, where it appears to have been ruled that if the search is made without complying with the provisions of the relevant statute relating to such searches, it would not only render "the entire search without jurisdiction", but "as a logical corollary, would vitiate the conviction". It appears that this decision has virtually adopted the Exclusionary Rule of Evidence as in the United States, because though 48 bottles of liquor were recovered in the search of the car of the accused, for which the conviction under Section 34 of the Mysore Excise Act could justifiably be sustained. The conviction was nevertheless set aside by the Supreme Court as in its view the search being illegal, the resultant recovery was to be excluded from consideration.

As already pointed out, the English Law on the point was that "if the evidence is relevant, it is admissible and the Court is not concerned with how it was obtained" and that "it matters not how you get it, if you steal it even, it would be admissible" and reference in this connection may be made to *Halsbury's Laws of England*<sup>27</sup> and the decision of the Privy Council in *Kuruma Vs. Reginam*<sup>28</sup> This rule that illegality of search will not affect the admissibility of the materials recovered on such search was also clearly enacted in Section 465 of the Code of Criminal Procedure, 1973, as it was in Section 537 of the preceding Code of Criminal Procedure of 1898 and it may be difficult

to justify the decision in *K.L. Subbayya* (supra) in view of the clear provisions of these Sections. It is, however, apprehended that the *Maneka-dicta* to the effect that no one can be affected in respect of his "Life" or "Personal Liberty" except according to procedure which must be "Reasonable, Right, Just and Fair" would go a long way to support and sustain the adoption of the Exclusionary Rule of Evidence, as done in *K.L. Subbayya* (Supra), on the specious ground that nothing can be regarded to be "Reasonable, Right, Just and Fair" which is done in violation of law.

(G) It was not necessary for us to wait till 1978 for the decision of the Supreme Court in *Sunil Batra*<sup>29</sup> or even till 1974 for the Supreme Court decision in *DBM. Patnaik*<sup>30</sup> to realise that neither the accused nor the convicts are "denuded of their Fundamental Rights and part III of the Constitution does not part company with the prisoner at the prison-gates" nor with the accused, when appearing in the Court or the accused-dock. The position, if we may say with respect, is too obvious, because unless Parliament by law restricts or abrogates any of the Fundamental Rights, which Parliament may under Article 33 of the Constitution in respect of the Armed Forces or the Forces charged with maintenance of Public Order and also persons employed in some other services specified therein, to whom Part III otherwise applies, can be banished out therefrom. An accused or convict is therefore entitled to all those rights, subject only to such modifications, restrictions or abridgements which would legally and necessarily follow from his prosecution or imprisonment.

But even though flood of tears are being shed and overzealous and too anxious concern shown for the accused and the convicts, the Human Rights of the victims have been sadly ignored in our Criminal Justice System.

(H) Under Section 313, Code of Criminal Procedure, the Court must “after the witnesses for the prosecution have been examined and before he is called on for his defence, question him generally on the case”. It has become the settled law that where any evidence or circumstance, though duly brought on record, was not put to the accused while examining him under Section 313, no such evidence or circumstance can be used against him and reference in this connection may be made, among others, to the decision of Supreme Court in Sharad Birdhichand Sharda.<sup>31</sup> As a result, even if strong and reliable evidence against the accused has come on record and the accused through his Counsel has duly cross-examined the witness on the point, yet the same can not be relied on and must be excluded from consideration, if the Trial Judge, through inadvertence or incompetence or otherwise, has not drawn the attention of the accused while examining him under Section 313 of the Code. Thus the protection and enforcement of the Human Rights of the victim have been made very much dependent on the competence or otherwise of the Trial Judge.

This position could have been justified before 1955, when the accused could not depose as a witness on his behalf. But now that after 1955, and also under the present Code of Criminal Procedure, 1973, the accused is fully entitled to enter the witness-box to depose on his behalf, there may not be good and justifying reasons for this Law, except to demonstrate an unreasonably soft heart for the accused. It is generally accepted that if a party, who is conversant with the facts of the case, does not examine himself, the Court is entitled to presume everything; against him and reference, if need be, may be made to the decision of the Privy Council in Sardar Gurdial Singh<sup>32</sup> and to a decision of the Calcutta High Court in Labanya Roy<sup>33</sup>, where many of the leading decisions on the point have

been referred to and relied on. A view is, therefore, gaining ground that the accused being fully entitled to depose on his behalf, the Court may draw adverse presumption against him if he, for no good reason, fails to examine himself as a witness.

10. The Crime scenario of the country is now horrendous and very strong steps have got to be taken to combat such crimes, and to investigate, inquire and to try Criminal Cases. It may be that in doing so, an innocent may, in a given case, become injuriously affected. But, however, unfortunate that may be, this may be inevitable in view of the present scenario of escalating grave offences, including the activities of the militants. It is common knowledge that while dispersing an unruly mob, or dispersing a violent unlawful assembly, or to combat a serious riot, force and even Armed Force may legally be used, and it very often happens, that in doing so, an innocent person may be injuriously affected. But however, regrettable that may be, this is something which cannot be helped.

11. Very recently, the Chief Minister of West Bengal was criticised for asking the Police Forces to “shoot at or down the armed miscreants”. We should remind ourselves that while attempting to arrest a miscreant, a Police Officer or any person may, under Section 46, Code of Criminal Procedure, use all means necessary to effect the arrest and may in such attempt cause even the death of the person if he is ‘accused of an offence punishable with death or imprisonment for life. We must not also forget that under the Indian Penal Code (Section 96-106) every person has a right of private defence not only in respect of his own body or property, but also in respect of the body or property of another person and as provided in Section 100 and Section 103, Penal Code, such right may extend to the causing death also. Therefore, there was nothing inherently

improper or illegal in such statement by the Chief Minister.

But it should however be noted that Section 3 of the Police Act, 1861, vests the power of superintendence over the Police Force in the State Government, while Section 5 vests the power of administration of the Police Forces on the Inspector-General. Under Article 154 of the Constitution, the executive power of the State is vested in the Governor, and as we all know, and as also provided in the General Clauses Act, 1897 which has been made applicable to the interpretation of the Constitution by Article 367, “Governor” would virtually mean “the State Government”. But Article 154(2) nevertheless provides that nothing in this Article shall be deemed “to transfer to the Governor any function conferred by any existing law on any other authority”. Therefore, though the power of over-all superintendence is vested in the Governor or the state Government under Section 3 of the Police Act, which was an “existing law” within the meaning of Article 154(2), the power of administration of the Police Forces is, however, vested in the Inspector-General and therefore the same cannot stand transferred to the Governor or the State Government. The Chief Minister accordingly, in the exercise of power of superintendence, can issue general instructions or lay down a general policy that armed miscreants, wherever found, are to be arrested or apprehended. But how the arrest is to be effected, whether by shooting down or by beating down or otherwise, must be left to the Inspector-General, and no Minister however exalted his position may be, is entitled to issue such specific direction to shoot, or to beat or to pat on the back. Surely it is not for any Chief Minister or any Minister to direct the police to file or not to file any charge-sheet in any particular case.

12. The “Due Process” clause in the V and the XIV Amendments of the American Constitution, providing that no

Person shall “be deprived of life, liberty or property without due process of law” is an invaluable Human Right, which was conceived and enacted with highly laudable and commendable object. But as has been observed by Justice Douglas, a celebrated American Judge, in his Tagore Law Lectures<sup>30</sup> “Due Process” “would have such meaning as Judges from time to time might give it” and that though “that had the advantage of great flexibility” it also had inherent dangers”, “for Due Process, like Natural Law, could come to reflect the individual idiosyncracies of the Judge, his predilections, his favoured economic creed or philosophical theory” and to “the absence of guides or standards might allow Judicial whim or caprice to play havoc with legislative programs.”

Grave apprehensions are being expressed by some legal scholars that the way the ‘Human Rights’ are being expanded and applied with tenacious zeal

and zest, we, in India, may also have to express similar regret.

**REFERENCES:**

1. AIR 1969 SC 783
2. AIR 1984 SC 667
3. (1996) 35.SCC 545
4. (1996) 8 SCC 525
5. (1997) 6 SCC 241
6. AIR 1999 SC 625
7. AIR 1999 5C 1149
8. 1935 AC 462
9. (1970)1 All. ER 219
10. AIR 1973 SC 2622 at 2626/27
11. AIR 1981 SC 1036
12. (1971) 401, US 395 : 28 L.Ed. 2nd. 130
13. (1971), US 235 : 26 L.Ed. 2nd. 586
14. (1998) 7 SCC 3921
15. AIR 1978 SC 597
16. AIR 1978 SC 429 (432)
17. AIR 1978 SC 527 (531)
18. AIR 1979 SC 1360 (1362)
19. AIR 1980 SC 1632 (1646)
20. AIR 1978 SC 1594 (1597)
21. AIR 1956 SC 411
22. AIR 1963 SC 822 (824)
23. AIR 1970 SC 1396 (1397-98)
24. (1972) 1 SCC 764
25. (1980) 4 SCC 669 (673)
26. (1979) 2 SCC 115, 116, 117
27. Laws of England 3rd Edn., Vol. 15, p-266
28. (1995) 1 All ER 236 (239)
29. AIR 1978 SC 1675
30. AIR 1974 SC 2092
31. AIR 1984 SC 1622
32. AIR 1927 PC 230
33. 68 CAT WN 611
34. From Marshall to Mukherjee — Studies in America and Indian Constitutional Law (1956), pages 199-200.

***Conduct  
is the great profession  
Behaviour  
is the peripheral revealing of us  
What a man does  
tells us what he is***

**FD Huntington**