4

CYBER CRIME A STRATEGY FOR BATTLING THE MENACE

*Varun Kapoor, IPS**

The human race has undergone a number of changes and developments over the ages. These changes have all aided in the progress of the race as a whole into a more cohesive, collective & progressive unit of existence. The **Agricultural Revolution** which started 12,000 years ago, ushered in the first big leap in human development (not evolution). It leads to settled communities coming into being and the concept of village and community living, with all its advantages, coming into practice.

The next big leap came with the construction of the power looms and the setting up of large units of production in Manchester, England. This was the era of the **Industrial Revolution**. It started around 250 years ago. The concept of cities and urbanization came into vogue. Yes, there were some disadvantages in the springing up of urban conglomerates, but these were far outweighed by the numerous advantages that this brought in its wake.

Something momentous again happened around 50 years ago; this once again has enabled mankind to take a giant leap forward on the development index. This was the invention of the integrated circuit or the computer chip. These chips have revolutionized our lives, running our appliances, providing calculators, computers and other electronic devices to control our world. The era of the **Information Revolution** is here and we are living in it. Noted scientist Castellas (2000) has proposed an analysis "that highlights a networking logic as a distinctive characteristic of information societies", the ones in which we exist today.

* IGP & Director PRTS & PITI, Indore (MP)

Today we are living in "Exponential Times". The main factors that have contributed to this are as under:

1. **Cell Phone Revolution:** Cellular technology and its continuous up-gradation has ensured that the use of mobile communication devises has multiplied exponentially. Today there are 6.8 billion cell phone subscribers the world over. Out of this nearly 1 billion (905 million) are in India! Only China with 1.2 billion subscribers is ahead of India in usage.

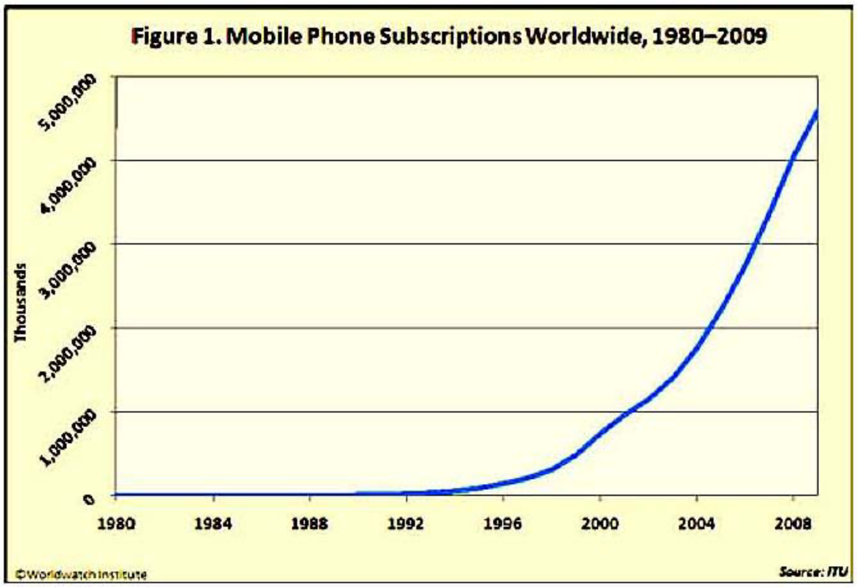


Figure 1. Mobile Phone Subscriptions Worldwide, 1980–2009

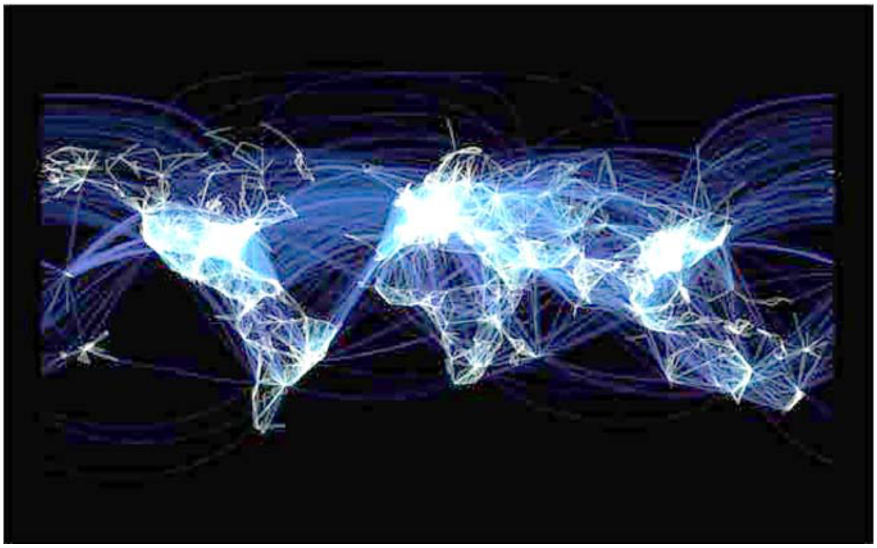
Source: ITU

This graphical representation clearly indicates how cell phone use has "taken off" since the mid-nineties. This has ensured that communication is possible today at lightning speed. What, Where, When, How of any situation is available with huge sections of the population within the "blink of an eyelid". The community is now not only better informed but sometimes even "over-informed". This is the information age society.

2. **Electronic Gadgetry:** This information explosion has been supported by a host of state-of-the-art gadgetry. These are also continuously being upgraded. Shelf life today of modern gadgets and gizmos is around 3 months. After that time the technology they use gets outdated and something better and newer is available. Off course this is driven by market compulsions of the

manufacturing agencies, but the fact remains that modern gadgets have changed the entire mindset of the population. Be it desk top computers; Lap top Computers; Palm Top devises; iPads; iPhones; iPods; Androids; Smart Phones; CCTV Cameras; Web cameras; Blue Tooth Devices; Spy Cams – the list of devises is endless and ever growing. The availability of these devices and there stepped up use have greatly contributed to the progression of this information revolution era.

3. **Connectivity:** The next great contributor to this explosive growth of information and communication is the surge in the quantum and quality of connectivity available. The development of the fiber optic cable has greatly enhanced the quantum of data that can be pushed down a single strand of optical beam as well as the speed at which it can be transmitted. This capability was first demonstrated by Robert Maurer, Donald Keck and Peter Schultz in 1970.



Today more than 80% of the world's long distance communication traffic is carried over optical fiber cables, 25 million kilometers of the cable first demonstrated by Maurer, Keck & Schultz has been installed worldwide.

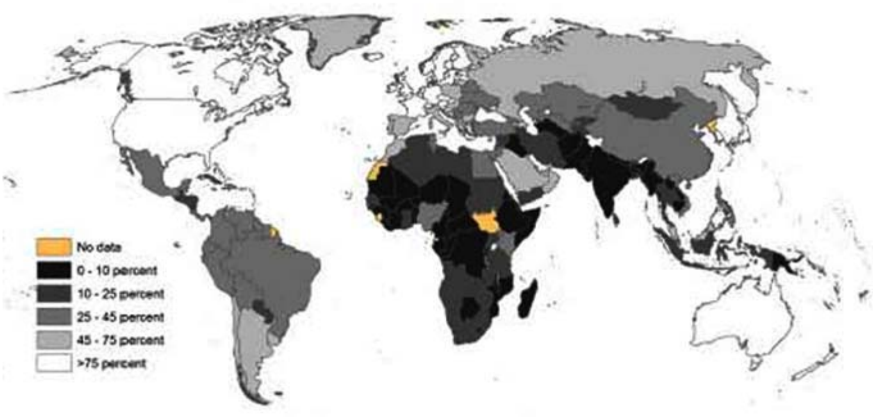
The speed of this connectivity and the quantum of data bearing capacity is also being continuously increased. The mobile communication connectivity has also rapidly developed; 1G Technology – launched in Chicago in the year 1978 – was capable of transmitting voice data at high speed. This was soon followed by the 2G Technology. This was formally launched once again in Chicago in the year 1991. This technology ensured the transmission of text data along with voice transmission at high speed over long distances. In fact, the first SMS message was formally sent in the year 1992 at London, UK. It was in Japan in the year 2001 that the 3G Technology was unveiled. This technology entailed the transmission of the internet along with text and voice communication over long distances. Finally the 4G Technology was introduced in Scandinavia in the year 2009, which vastly enhanced the speed of connectivity. The "buffering time" (or downloading speed) is almost reduced to zero and live images can be obtained without any lag over mobile communication devises. Today a two hour feature film can be downloaded in 8 seconds using 4G Technology.

The Direct To Home (DTH) television connectivity has revolutionized the entire concept of information dissemination to the society at large. Even remote and rural areas are fitted with numerous DTH dishes. Live and happening information is available to the public irrespective of age, gender, caste, community & creed. This has changed the entire mind set of the people.

4. **Internet:** The internet today is the largest factor in the spread and growth of the information revolution to the remotest corners of the globe. The percentage users globally are given below[1] :

[1] Source: World Telecommunication ICT Indicators 2012.

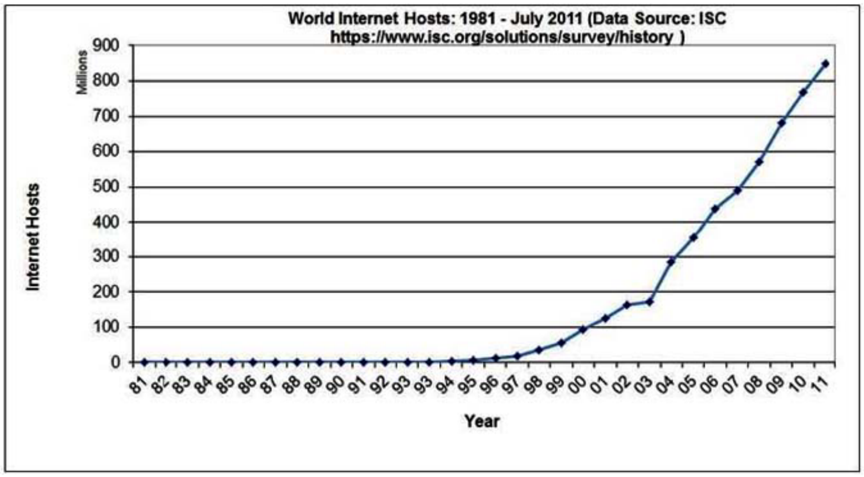
Figure 1.1: Percentage of internet users (2011)



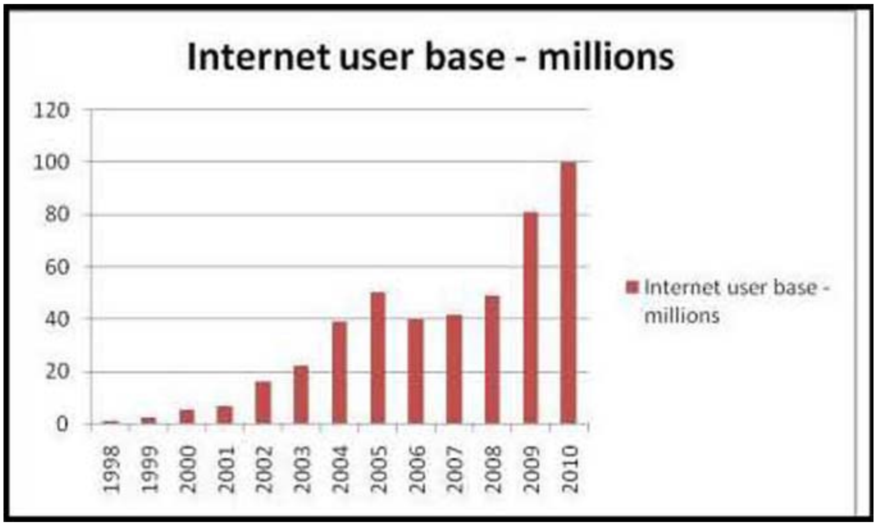
The internet is being primarily used for:

- Surfing
- Downloading
- Commercial Activities
- Social Networking

Global usage of the internet is growing explosively as the graphical representation given below clearly brings out:


World Internet Hosts: 1981 - July 2011 (Data Source: ISC https://www.isc.org/solutions/survey/history)

In India to the use of the internet is multiplying at an extremely rapid rate. This is borne out by the following graphical representation:



The internet has become such a huge medium of information dissemination that every aspect of human existence is being touched in major ways by this phenomenon. This fact can be readily cross checked by applying the "1 Minute Test". In 60 seconds on the internet globally:

- 2.6 Million CD's or 1820 TB of data created.
- 1400 Discs are rented online (online movie rental service).
- 950+ purchases on e-Bay.
- $219,000 payment on Pay Pal.
- 11 Million conversations on Instant Messengers.
- $75,000 added to Google Revenues.
- 2,500 ink cartridges sold.
- 4,000 USB devices sold.
- 38 tons e-waste generated.
- 232 Computers infected with Malware.
- 12 websites got hacked – 416 attempts.
- 11,000+ hour's music streaming on Pandora.
- 12,000+ new ads posted on Craigslist.

- 370,000+ minutes calls on Skype.
- 98,000+ Tweets – 320+ New accounts.
- 100+ New LinkedIn Accounts.
- 695,000+ Face book Status Updates.
- 168 Million E-mails sent.
- 11,000+ iPhone applications download.
- 70+ Domains registered.
- 600+ New video uploaded on You Tube.[2]

These figures are indeed mind boggling. All these activities going on in cyber space courtesy the internet and that too in 60 seconds, defies all reasonable logic. It goes to amply & definitively prove that the internet has been the real engine that has driven the information revolution to the present day dizzying heights.

It is time now to analyze the effects that the information revolution has brought about on the society in general. There are manifold effects of this revolution but a few stand out like beacons and need to be explored in detail:

1. Global village concept has taken shape. This concept was first introduced by Marshall McLuhan of the Boston Consulting Group. Rapid advances in communication technology have ensured that distances today are no barriers to speedy and effective communication and contact. We feel as if we are living in a large "Global village".
2. Greater than ever opportunities have emerged. Today there are opportunities in numerous fields be it IT, telecommunication, travel, tourism, financial markets, commercial activities, service industry etc. These are all fuelled and driven by the incessant march of the information revolution.
3. There has been a virtual information explosion. People are extremely well informed today and it is well neigh impossible to hide any facts or situations from public scrutiny. This new dimension has changed the entire thought process of the human race and molded it in the direction of "perfection at all cost" & "individualistic existence". Today vast majority of the populace (especially the youth & urban dwellers), physically live in large

[2] All figures provided by Go-Globe.com

communities but exist individually. It appears that the circle of existence has come a full round as a result of this information revolution. The agricultural revolution broke down the individual existence and promoted community living whereas the information revolution is pushing the human race to move from community living back, into the folds of individual existence in the physical form, all over again.

4. Human networking in the virtual space is taking place as never before. Youth today may have only a couple of friends in the real world but they all will have a couple of hundred in the virtual world! This human networking is to an extent de-humanizing the race but at the same time is promoting the spread of information at lightning speed amongst large swathes of population in an instant. This is resulting in better cooperation & collaboration on issues of importance to the society.

5. The specter of the rapidly growing and uncontrolled cyber crime is an ever present threat. This has fast become a multi-dimensional & multi-national problem and it needs quick address so that it does not damage the entire fabric of the economy and the society.

Definition of Cyber Crime:

Cyber Crime as defined by the Information Technology Act, 2000 is:

- "Any crime committed using a computer."[3]

The definition was modified and expanded under the IT (Amendment) Act, 2008. It now defines Cyber Crime as:

- "Any crime committed using an electronic devise. "[4]

A better and more comprehensive definition is as follows:

- "Any crime committed using the functionality of an electronic device."

Types of Cyber Crime:

Cyber Crimes are of numerous types. In addition new types of cyber crime keep being added all the time and the modus operandi of existing crime keeps changing rather rapidly too. However, cyber crimes can be classified into two broad categories:[5]

[3] Information Technology Act, 2000.

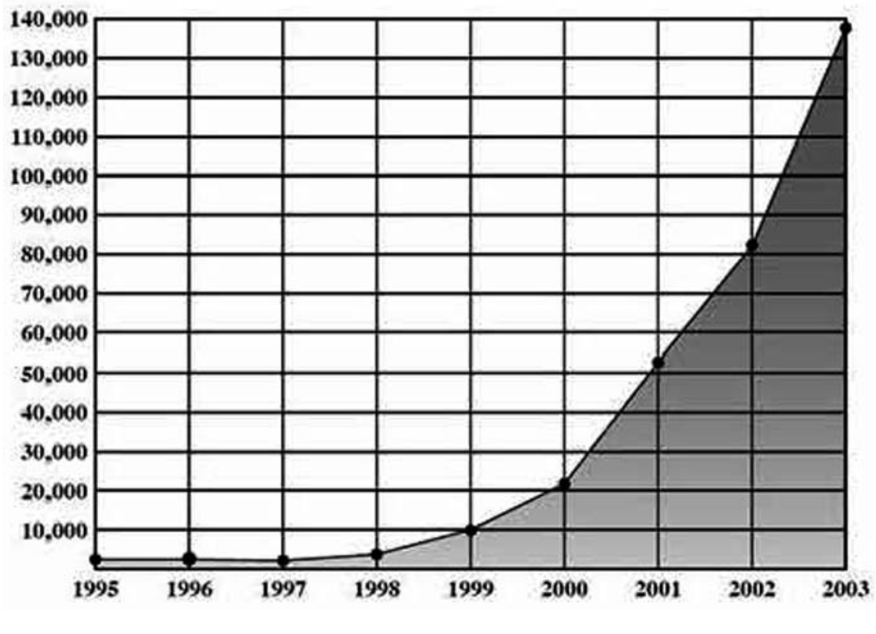
[4] Information Technology (Amendment) Act, 2008.

[5] DSCI: Cyber Crime Investigation Manual.

SNo	Crimes targeting Computers	Crimes using computers as Tools
1	Hacking	Financial Frauds
2	Denial of Service/Distributive Denial of Service Attack	Data Modification
3	Spreading Virus & Malware	Identity Theft
4	Website Defacement	Cyber Bullying
5	Cyber Terrorism	Cyber Stalking
6	Spoofing	Data Theft
7	Skimming	Pornography
8	Pharming	Theft of trade secrets
9	Phishing	Intellectual property thefts
10	Vishing	Espionage on protected systems
11	Spamming	

Growth of Cyber Crime:

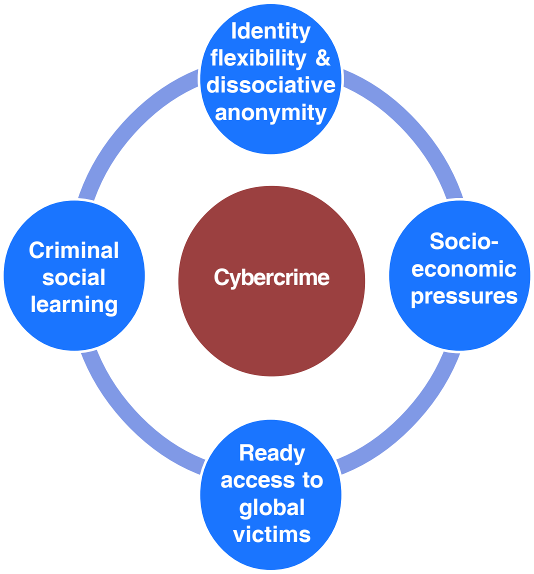
As stated before cyber crime is growing at an alarming rate the world over. A graphical representation of this exponential growth is given below.[6]



[6] Figures supplied by Ohio Supercomputer Center.

The above graph clearly demonstrates that worldwide cyber crime reports grew by almost a whopping **7000%** over a period of **9 years**! This is an absolutely phenomenal increase and no other world crime is growing at this rate. Another definitive fact is that this pace of growth must have accelerated even more with the passage of time. It is really hard to imagine the volume of this crime today and the sheer magnitude of incidents occurring all over the globe. No wonder the world over, law enforcement agencies are overwhelmed by this crime and are struggling to let alone curb or control this crime but to hold its own against this hydra headed monster of a crime.

Globally cyber crime is showing strong trends of increasing at an alarming rate. One theory of the reason for this rapid increase is represented graphically below:


Identity flexibility & dissociative anonymity
Criminal social learning
Cybercrime
Socio-economic pressures
Ready access to global victims

This brings out a fact very strongly; that due to identity flexibility & dissociative anonymity in the cyber world, citizens tend to behave in such manner and take such actions that they normally would not do in the physical world.[7]

[7] UNODC Comprehensive Study on Cyber Crime 2013.

India too is facing an accelerated growth rate in terms of occurrences of cyber crime. NCRB figures for the years 2005-2012 can be studied to clearly understand the extent and pace of the growth of cyber crime in India:

S.no	Year	Cyber Crime Cases	Persons Arrested
1	2005	179	192
2	2006	142	154
3	2007	217	154
4	2008	288	178
5	2009	420	288
6	2010	966	799
7	2011	1791	1184
8	2012	2876	1522

The growth of cyber crime between 2005-2008 was a moderate 61%. But in the period 2009-2012 it has increased at an unbelievable rate of nearly **900%**!!

Norton Cyber Crime Report 2012:

NORTON Anti-virus manufacturing company carried out a comprehensive study of the worldwide cyber crime scenario and brought out their findings in a report in 2012.

This report brought out some very pertinent facts, which are enumerated below:

- TOTAL GLOBAL BILL FOR CYBER CRIME IS **US $ 388 Billion** or INR 21 Lakh Crores.
- Time Lost Cost is **US$ 274 Billion**
- Cash Cost (money actually stolen + spent to repair cyber attacks) is **US$ 114 Billion**.
- Total victims per year are an estimated **431 Million**.
- Daily victims are **+1 Million**.
- This means **14 victims/second**.
- **80%** of adults in emerging economies have been victims as compared to 64% in developed countries. Indicates greater vulnerability for Indian users.
- Second biggest crime in the world after global illicit drug trade,
- Virus and Malware attack is the biggest cyber crime in the world. It constitutes **54%** of all global annual cyber offences.
- In India annual Time Lost cost is **US$ 3.68 Billion**.
- In India annual cash cost is **US$ 4 Billion**.

This report further corroborates the fact that cyber crime is today a grave threat to individuals, economies and governments – the world over. Things have to be done and done fast, to keep the citizens, their property and governments safe and secure against this ever increasing and rapidly multiplying threat. With the increasing use of computerized systems and internet in all spheres of human activity, if things continue to move in this direction without effective check then the day is not far when the very existence of humanity will come under threat due to the scourge known as – "CYBER CRIME".

The situation in developed markets countries with regard to cyber security measures is much better & advanced as compared to emerging market countries like India. In India as more and more citizens take to the use of mobile phones; increase in internet penetration; greater accessing of the internet using mobile devices & phenomenal growth in the reach of social networking the challenges facing the law enforcement agencies in dealing with the problem of exponential growth of cyber crime, are going to be manifold in the times to come. This pictures is absolutely clear and the writing is on the wall for Indian Police agencies regarding control, investigation and prevention of cyber crime – "**adapt and improve or be over-whelmed**".

Challenges Posed by Cyber Crime to Indian Police:

The challenges faced by Indian Law Enforcement Agencies in battling cyber crime effectively arise due to the following factors:

1. Due to the huge amounts of illegal profits involved the number of offenders committing cyber crime is already of unmanageable proportions. Furthermore these numbers are forever increasing.
2. There are a large number of unsuspecting citizens, who due to lack of proper understanding of the existing legal provisions are offending by mistake. This number is also very large as is seen by the age group of offenders in the figures for 2012 released by NCRB. Out of a total of 1522 persons arrested under the IT Act provisions, 65 were below 18 years of age and 928 were between 18-30 years of age. Hence number of arrested persons who were students of Schools/Colleges was almost **65%**. It is then quite clear that most of these offenders are offending by mistake and not by design.
3. Again due to the large amount of money that this organized crime is liable to generate, there is a huge window for systemic corruption. This blunts the efforts at regulating and controlling cyber crime in an effective manner by the police agencies.
4. Cyber Crime by nature is a highly technology intensive sphere of functioning. Most of the police officials (experienced and fresh recruits) by nature are not oriented to work effectively or extensively in this kind of technologically advanced field.
5. The technology itself is forever changing and being upgraded. This presents further problems for an already technologically challenged department and its officials. The shelf life for cyber technology today has shrunk to THREE months. By the time the police officials are oriented towards a particular technology, it becomes outdated and is replaced by something new and more advanced.

6. Availability of reliable private resources to augment police officers in cyber security work is also fraught with dangers. Thus the idea of recruiting "ethical hackers" to supplant cyber security trained police professionals is a plan that will inevitably raise questions regarding secrecy, impartiality and commitment.
7. All over the country Cyber Cells have been established to tackle this problem. However these Cells are being inundated with a flood of complaints regarding violation of cyber law and are finding it increasingly difficult to cope up keeping in view the fact that they too are severely understaffed and underequipped.
8. Cyber Crime has mistakenly been considered as a specialized area of police operation like Anti-terrorist cell; Anti-naxalite unit or Anti-corruption bureau. On the contrary Cyber Crime is a whole field of policing and it deserves to be treated as such. Just like there is a police force to police the real world there should be an entirely different police force to police the virtual world.

Prts Model for Battling Cyber Crime:

Police Radio Training School at Indore has come with a new model using which cyber crime may be more effectively tackled and the challenges posed by it addressed. The theory of recruiting & employing a virtual army of ethical hackers to aid the police is an unreliable and impractical method for battling cyber crime. The PRTS has devised an almost ingenious method of battling this menace. This involves educating large swathes of police personnel in basic and advanced features of cyber security as well as generating awareness in the community (especially younger generation) to remain safe and secure while using cyber space.

This is thus a two pronged strategy. It was conceived and designed by the undersigned (**VARUN KAPOOR, IGP PRTS Indore**) and was formally launched in January 2012. Thus it has been in operation for more than two years and the results have been encouraging.

The first hub of this strategy is the-

e-Investigator Development Project (e-IDP):

As stated earlier this project was formally launched in January 2012 with the hosting of the first three day training module on e-Mail Tracing for officers of MP Police. This was based on the idea that field officers should be made tech savvy and provided with skills to combat the emerging threat of cyber crime. District Police officers of the cutting edge level (Sub Inspector – Additional SP) were selected, to be trained under this scheme. This scheme was launched totally with self motivation, self resources and self design. The training programs were designed in a manner that they were "**of short duration but high impact.**"

The idea which had humble beginnings has flowered into a full blown project which has been in operation for the last 2 years. **Forty Five** training programs and 5 seminars have been organized under its aegis. In these technologically loaded courses **1584 officers** have been successfully trained. These officers represent **20** different state police forces; **6** Central Para Military Forces; **Indian Army** & **MP Forest Department** Officers. Today the PRTS organizes cyber security training in **9** different type of training modules and police investigators from all over the country take part in it. The best cyber security experts from across the country provide training in these high quality courses.

This is the **only effort of its kind** in operation anywhere in the country. True, that various state police and central agencies carry out cyber security training for the police agencies, but these are just stop gap efforts whereas the e-IDT is definitely the longest running, continuous and sustained effort at providing pointed and all embracing cyber security training to police personnel.

e-MAIL TRACING
Course Series
PRTS Indore

NAVSTAR GPS
GPS HANDLING
Course Series
PRTS Indore

CDR ANALYSIS
Course Series
PRTS Indore

CYBER CRIME SCENE
MANAGEMENT
Course Series
PRTS Indore

3D
3-D MODELING
Course Series
PRTS Indore

CYBER CRIME CAPSULE
COURSES
PRTS Indore

1st National Cyber Crime Training
PROGRAM
(17th – 24th December 2012)
PRTS Indore

2nd National Cyber Crime Training
PROGRAM
(2nd - 13th September 2013)
PRTS Indore

3rd National Cyber Crime Training
PROGRAM
(1st – 13th October 2013)
PRTS Indore

4th National Cyber Crime Training
PROGRAM
(10th - 22nd Februory 2013)
PRTS Indore

α
Θ
FORENSIC HYPNOSIS
Course Series
PRTS Indore

Sno	Name of Course	Collaborator	No. of Courses	Officers Trained
1	e-Mail Tracing		8	153
2	GPS Handling		8	182
3	CDR Analysis		12	228
4	3D Modeling		1	21
5	Cyber Crime Scene Mgt	CERT-in	1	27
6	Cyber Crime Capsule		8	346
7	National Cyber Crime Training Program	BPR&D	4	108
8	Forensic Hypnosis		2	53
9	Advanced Cyber Security		1	20
10	Seminar – Bridging the Digital Divide	KPMG	1	274
11	Seminar – Wildlife Conservation	WWF-India	1	46
12	Seminar – e-Gender Sensitization	BPR&D	1	50
13	Seminar – Cyber Forensics	PwC	1	22
14	Seminar – Anti Human Trafficking (+Online)	BPR&D	1	54
	TOTAL		**50**	**1584**

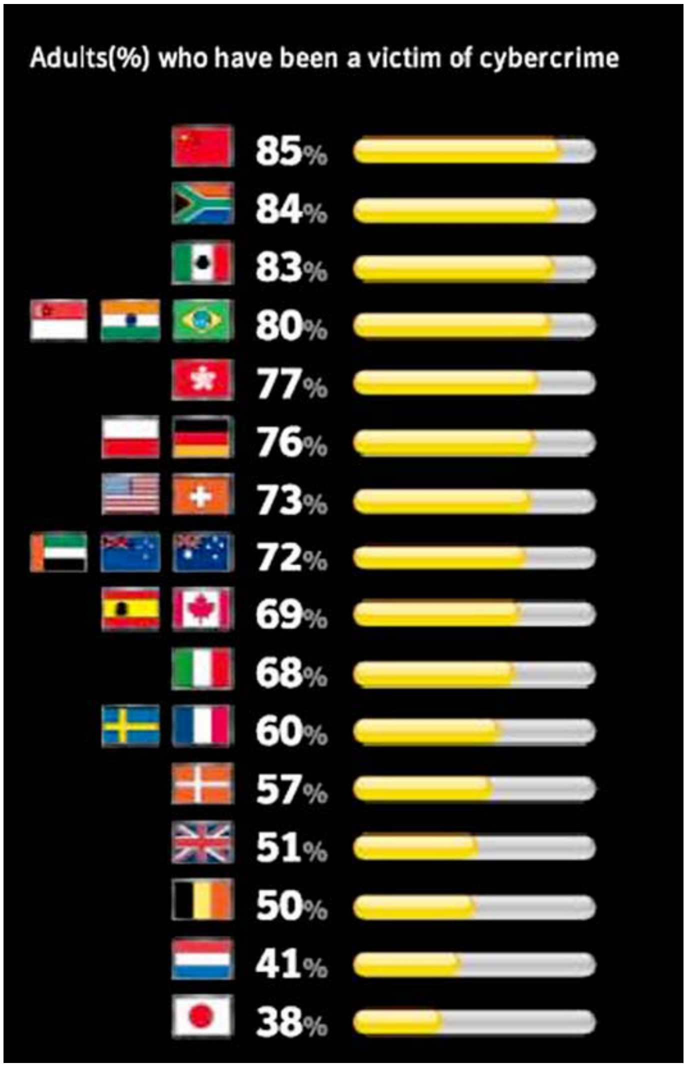
The effect of this huge number of training programs has been that a large chunk of cutting edge level officers including special formations like ATS & STF have been made cyber security aware and equipped. These individual officers not only posses requisite skills to tackle cases relating to cyber crime but also have the necessary contacts with professional and reliable experts in the field of cyber security. These experts they can freely contact for assistance and guidance as and when required. Thus, these PRTS trained officers can truly deliver encouraging results in the field of cyber security and crime detection and prevention.

The second hub of this strategy is the –

Blue Flame Initiative:

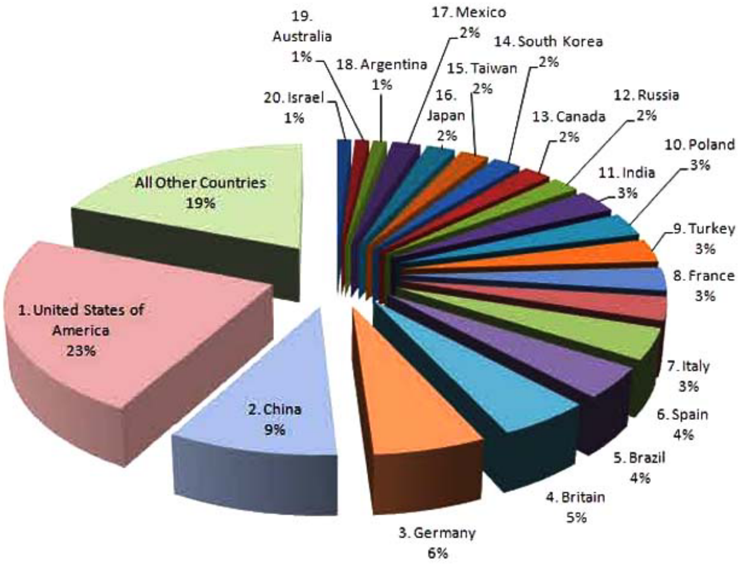
The "Blue Flame Initiative" is designed to spread awareness in the community. This is another initiative taken totally by personal experience and desire to make a change in the way society uses the cyber world and the World Wide Web. The model presented by the USA in this regard is something to be studied and adopted as an excellent strategy at cyber crime prevention.

The following cyber crime incident Hotspots (% adults who have been victims of cyber crime) have been brought forward by the Norton Cyber Crime Report 2012:



It is interesting to note that the top country with highest incidents of cyber crime is china with a rate of 85%. India ranks fourth with cyber crime incidence of 80%. THE 24th ranked country Japan has a cyber crime incidence rate of 38%. In this rather exhaustive list the USA which has the second highest number of internet users, does not figure. That brings out clearly the fact that there is an important reason why the USA does not figure in this list. That reason is greater **AWARENESS** of the citizens in matter of being safe and secure while using the cyber space. Students from 5th grade onwards have cyber security as a part of their curriculum. Thus they learn from an early age the "do's & don'ts" of secure cyber use. It becomes part of their system as a result they do not accidentally become victims or offenders while using the cyber space. Security lessons are in a way internalized by them and become a way of life. This results in the remarkable fact that the incidents of cyber crime are very small as compared to the other major user nations.

The second remarkable statistic with regard to the USA is that even though the incidents of crime are low, whatever crime does occur is fully reported to the concerned authorities.



Cybercrime: Top 20 Countries

This pie chart clearly shows that 23% of all registered cyber crime is in the USA. This is again a result of greater **awareness** in the citizenry regarding the secure web use. High incident reporting ensures more and better investigation. This ultimately results in greater detection and arrest of offenders and that reduces the incidents further. Thus we can say awareness of the citizens **is the key** to reduce and control the menace of cyber crime.

Emulating this experience of the USA in raising cyber security awareness, the PRTS started its "BLUE FLAME INITIATIVE" – the second hub of its two pronged strategy of battling cyber crime.

On 28th November 2013, the PRTS organized the first workshop for making students of Emerald Heights International School, cyber security aware. Almost 100 students and faculty were invited to PRTS center called PRAGITI, for a 3 hour duration workshop in which a number of facts, figures, procedures, laws, tips, films and instructions were given regarding safe and secure use of the cyber space.

This initial effort has developed into a full blown campaign, which has three distinct strategies:

1. SANDESH: For School students. Till date 12 workshops have been held under this Campaign.

2. SANKALP: For College students. Till date 9 workshops have been held under this Campaign.

3. SAMADHAN: For community members and institutions. Till date 4 workshops have been organized under this Campaign.

In a short duration of 3 months 25 workshops have been successfully organized and a huge number of citizens and students have been made cyber security aware. The total number of such individuals exceeds 3500 already. Large numbers of requests are coming in from all corners to organize these workshops for them too. Lack of time is hampering faster spread of this strategy. But efforts are on at war footing to satisfy all demands and spread the net of awareness as far and wide as possible. The DGP of MP has been requested to grant permission to the special PRTS team to travel to different parts of the state to organize such workshops.

This BLUE FLAME INITIATIVE is delivering its purpose is clear from the response of the participants. The questions and responses are so many that it demonstrates the advantage and information that people are obtaining from this effort. This will go a long way in making their internet experience safe and secure and protect them from becoming accidental victims or offenders by mistake or ignorance.

Thus we can say that this two-pronged strategy initiated by the PRTS is the way to go in tackling the ever growing specter of Cyber Crime. The "**BLUE FLAME INITIATIVE**" will bring about the necessary awareness amongst the citizens to remain safe and secure while using the cyber space. Whatever crimes which do occur even after this awareness will be prompt reported and police investigators trained under the "**e-Investigator Development Project**" will be equipped well enough to register, investigate and detect such offences.

ABSTRACT

Theme: Hiring Professional Hackers & Beyond

TITLE:

CYBER CRIME

A Strategy for Battling the Menace

Cyber crime is an ever growing threat to modern day society which relies so heavily on use of technology for all day to day activities. The explosion in the information era has been brought about by the explosive growth in the following sectors:

- Cell Phone use
- Connectivity
- Modern gadgetry
- Internet

This explosive growth has ensured that we now live in "exponential times". These times have brought many advantages in tow, like:

- Global village concept has become a reality.
- Huge opportunities for growth and development.
- Information explosion.
- Human networking like never before

However with these advantages has come a major challenge that threatens to unravel all these advantages – this is the specter of ever increasing and multiplying CYBER CRIME.

The world over this is a major challenge and this is a fact clearly illustrated by the fact that global cyber crime incidents increased by 9000% over a period of 1995-2003. Even in India NCRB data indicates that registered cases of cyber crime increased by nearly 900% between 2009-12. Thus this is a big challenge and conventional policing is not going to be able to deal with this threat. Out of the box ideas like hiring ethical hackers to aid police in battling this menace will not work due to their inherent unreliability. The problem will have to be solved from within and efforts will have to be made by the Police Department itself.

In this regard the Police Radio Training School (PRTS) at Indore, MP has put in place a two pronged strategy to deal with the menace of cyber crime.