THE ROLE OF DEVELOPING NATION TOWARDS COMBATING THE CYBER CRIME

Abhishek Vaish and Satya Prakash,
Indian Institute of Information Technology, Allahabad.

Hon'ble Justice Rajesh Tandon ,
Chairperson, Cyber Appellate Tribunal, Ministry of Communication and I.T., Govt. of India.

Abstract:

In the era of internet there is no boundary for the cyber criminals to sabotage the critical services and important data for any individual, organization and for entire nation. With the advancement in the information and communication technology, everyone is managing and developing web presence in order to utilize the potential and benefit of this innovative technology. On the other hand, the anti social elements of the society are taking it as a platform to create group and execute a crime in much organized way without a fear of getting caught by the law enforcement agencies. Almost every nation across the globe are struggling hard and developing man power with sophisticated technologies to control it. In this paper we are proposing a model that can highlights the requirement for the developing nation to address the menace of the cyber crime like the legal need, technological need, man power capacity building and intelligence system development.

Introduction:

In the edge of Information Technology, the whole world is now being in touch within one click. As fast as technology is growing simultaneously cyber crime is also increasing day by day. Now a days terrorist are using internet as a weapons called cyber weapons against the countries. Cyber war and cyber terrorism are matters of serious concern to all countries. Cyber warfare is a relatively new type of weapon with various effects on the target. It doesn't have any limitations of use and can achieve most of the goals set [1].

As hackers of all the parts of world is now targeting to the developing nation for stealing the critical data of military zones & government data and sell critical and confidential data to the terrorist and other peoples whoever is indulging in unfair means. After 26/11 attack, India tightened the security in respect of border security, intelligence system, Information assets etc.

Highlights on the recent trends:

A report of Indian computer Emergency Response Team (CERT-IN) shows that more than 2500 incidents were registered and handled in the year 2008. The types of incidents handled were mostly of phishing, malicious code, website compromise & propagation of malware and network scanning & probing [2].

The statistic of incidents reported and handle by the CERT–In during the year 2004 to 2008 is as below:

Phishing incidents reported in the year 2004 was 3, in year 2005 was 101, in year 2006 was 339, in year 2007 was 392 and in year 2008 was 604. This statistic shows the incidents increased in each year.

Network scanning & probing incidents reported in the year 2004 was 11, in the year 2005 was 40, in the year 2006 was 177, in the year 2007 was 223 and in the year 2008 was 265.

Virus & malicious code incidents reported in the year of 2004 was 5, in the year 2005 was 95, in the year 2006 was 19, in the year of 2007 was 358 and in the year 2008 was 408.There is only fall in the year 2006 and rest of the year reported inclination of incidents.

Spam incidents reported only in the year 2008 that was 305. No any incident reported during the period of 2004 to 2007.

Denial of service attack incidents reported only in the year 2008 was 54. No any incidents found during rest year.

Others security incidents reported in the year 2004 was 4, in the year 2005 was 18, in the year 2006 was 17, in the year 2007 was 264 and in the year 2008 was 94. This means that other incidents increased except the year 2006 and 2008.

835 incidents of Website compromise & malware propagation reported only in the year 2008. No any incidents found during the period of 2004 to 2007.

Above statistics clearly shows that India is more careful and aware about their sensitive and confidential data. Also provide the solution and training of such incidents.

Issues and challenges:

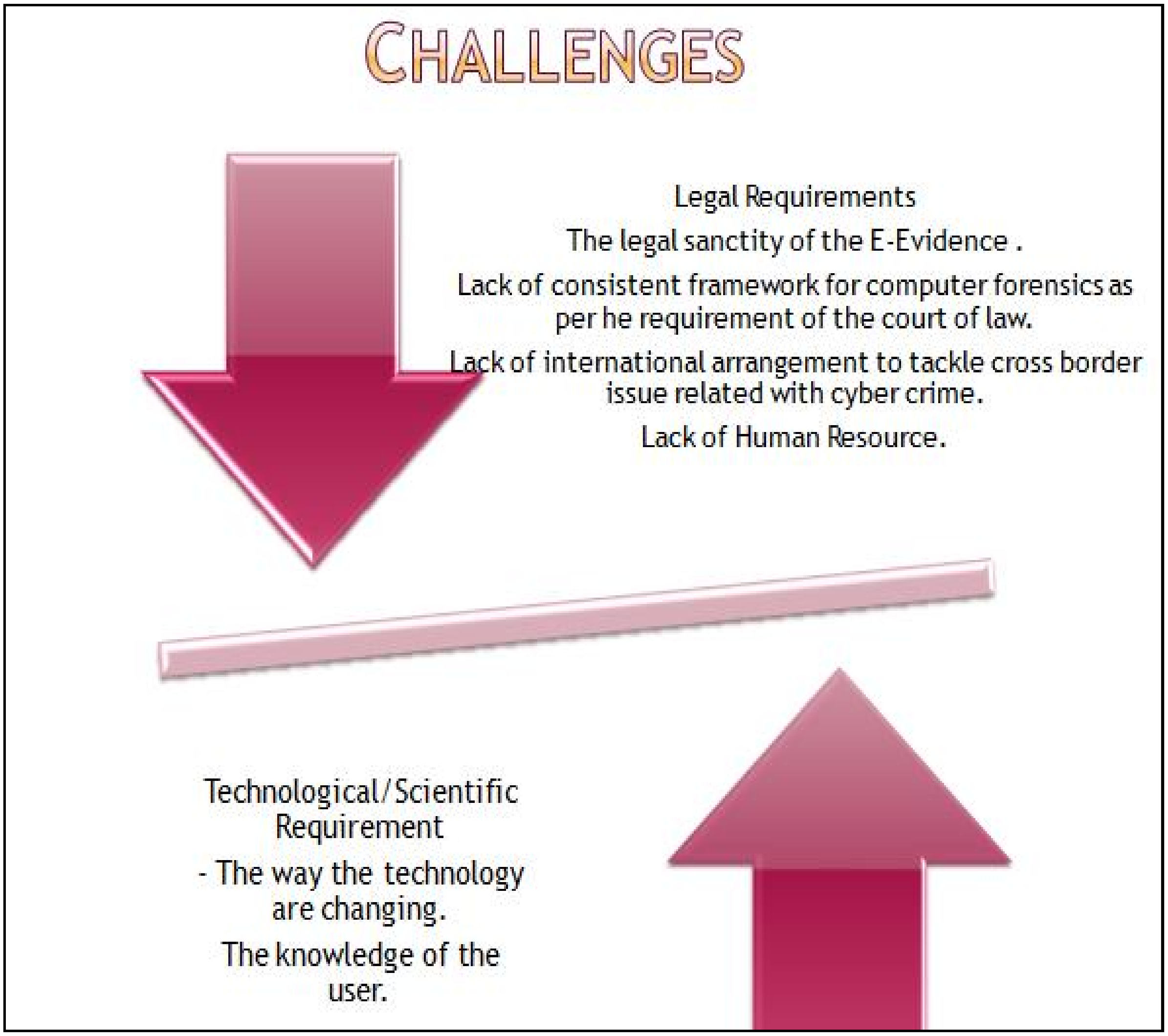
Cyber crimes are relatively a new kind of crime and therefore the challenges associate with it are also new. The field posses challenges to the scientific and legal community because the nature of crime are technical and the adjudicating system is procedural. Therefore, we have clubbed the challenges in two fields:

- Scientific
- Legislative
- Socioeconomic

Scientific: the problem associated with this community is lack of scientific and homogenous framework for the collection of evidence. With the rapid advancement of the technology and the very less life cycle of the technology it becomes hard for investigator to mine the information from the system. Additionally, the anti social elements are becoming smarter and smarter everyday and the technology are giving enough room to misuse the technology and making it difficult for the investigator for e.g., the NTFS file system which has the privilege create fake bad cluster and the information. The same attributes were not available in the older file system.

Legislative: The nature of cyber crimes are boundary less and requires international level framework at various level i.e., at the legal enforcement level, at investigative and at the law adjudication level. The lack of framework in this area is making it vulnerable for the wrong does and hence requires immediate attention. The biggest threat for the developed nations are posed by the country those doesn't have any cyber law because those countries work like a launching pad for cyber terrorism and cyber crimes.

Socio-Economic: Economy and social set-up plays big challenges in cyber space. Poor economy like unemployment of IT skilled people is contributing toward more reported incident year after year. Contrary to this, countries those are sentimental with religion and social dogmas are prone to cyber crime because the rumors are very easily and widely spread over internet. The aspect that plays encouraging roles is the feel of anonymity and a feel that the traces are difficult to find.



CHALLENGES

Legal Requirements

The legal sanctity of the E-Evidence .

Lack of consistent framework for computer forensics as per he requirement of the court of law.

Lack of international arrangement to tackle cross border issue related with cyber crime.

Lack of Human Resource.

Technological/Scientific Requirement

- The way the technology are changing.

The knowledge of the user.

Fig 1, balance of scientific and legislative challenges.

Parameter that governs the intensity of the attack

As the field of cyber crime is very sophisticated and distributed it becomes challenging to evaluate the intensity of the crime done and this makes the most of the potential evidence go undetected and finally makes the judicial process ineffective. Hence, it is imperative to develop the network of the crime and this topology is governed with the following parameters shown in figure 2 .

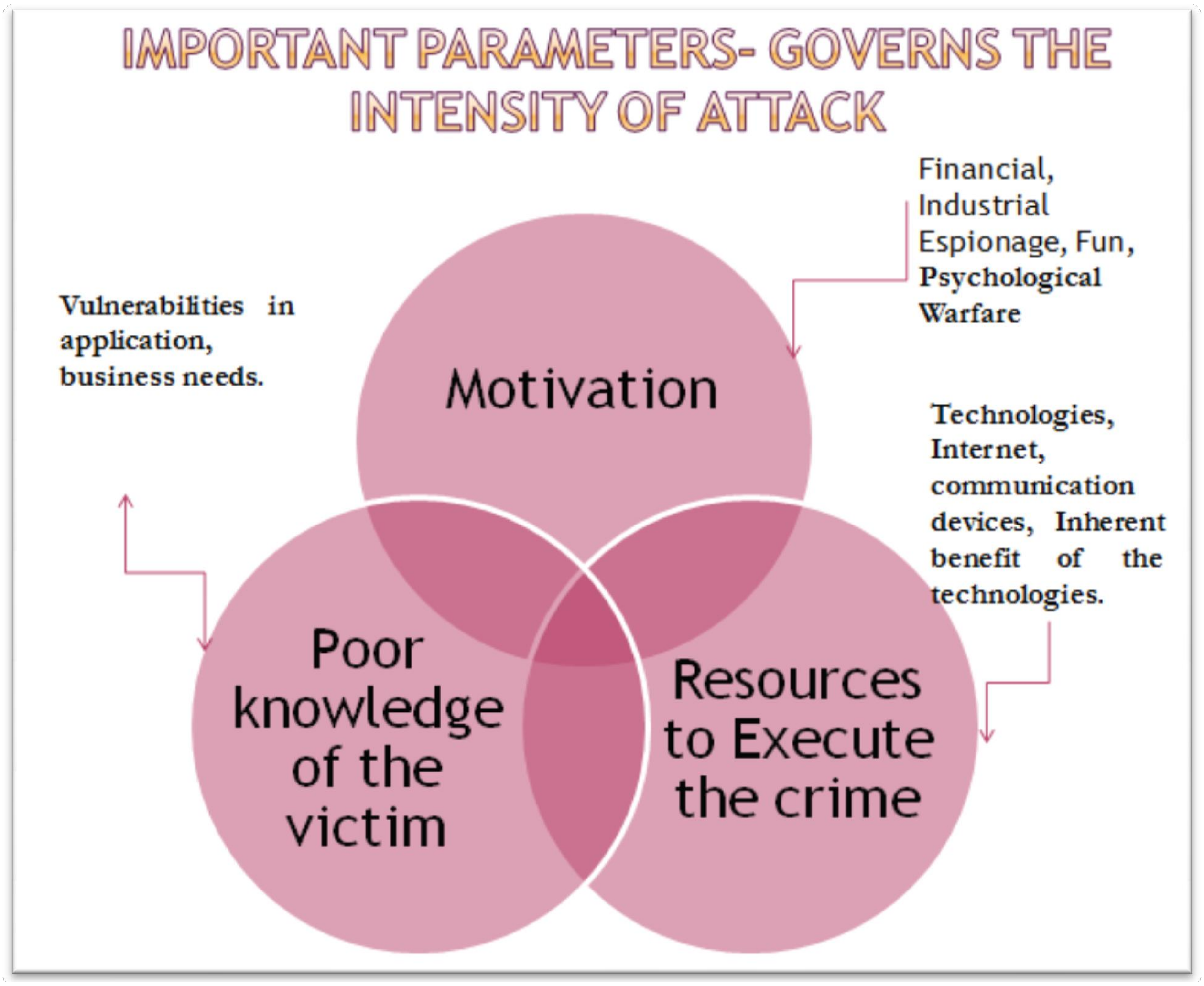

IMPORTANT PARAMETERS- GOVERNS THE INTENSITY OF ATTACK
Financial, Industrial Espionage, Fun, Psychological Warfare
Vulnerabilities in application, business needs.
Motivation
Technologies, Internet, communication devices, Inherent benefit of the technologies.
Poor knowledge of the victim
Resources to Execute the crime

Figure 2

Based on the three important parameter we have evaluate one of the crime that was not consider as cyber crime though had used information and communication devices in a big way to coordinate the incident. Figure 3, is an assumed topology of the Mumbai terrorist attack that took place in26/11, 2008. The incident was an example of a terrorism activity which is universal across whole world but the point worth noticed is the use of the technology to coordinate the incident having a devastating impact. On the contrary, if the handlers were not having the communication devices the impact could have been much lesser or may be a total failure in attempt. If you compare the incident with the three parameter that has been proposed you can it is clearly evident that the impact is associated with the knowledge, resources used and motivation of the anti social elements.

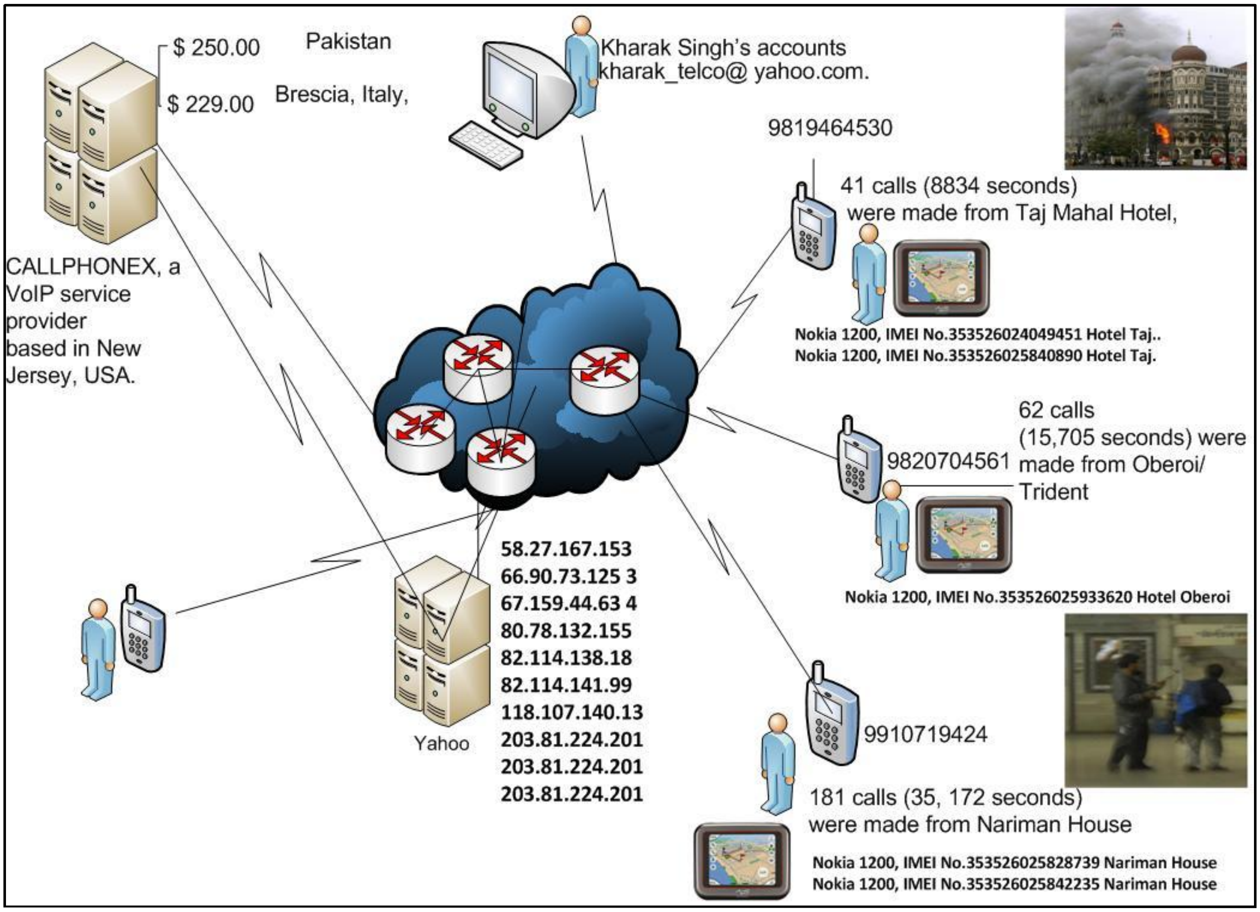

$ 250.00
Pakistan
$ 229.00
Brescia, Italy,
CALLPHONEX, a VoIP service provider based in New Jersey, USA.
Kharak Singh's accounts
kharak_telco@ yahoo.com.
9819464530
41 calls (8834 seconds) were made from Taj Mahal Hotel,
Nokia 1200, IMEI No.353526024049451 Hotel Taj..
Nokia 1200, IMEI No.353526025840890 Hotel Taj.
9820704561
62 calls (15,705 seconds) were made from Oberoi/ Trident
Nokia 1200, IMEI No.353526025933620 Hotel Oberoi
58.27.167.153
66.90.73.125 3
67.159.44.63 4
80.78.132.155
82.114.138.18
82.114.141.99
118.107.140.13
203.81.224.201
203.81.224.201
203.81.224.201
Yahoo
9910719424
181 calls (35, 172 seconds) were made from Nariman House
Nokia 1200, IMEI No.353526025828739 Nariman House
Nokia 1200, IMEI No.353526025842235 Nariman House

Figure 3, the network behind a terrorist attack.

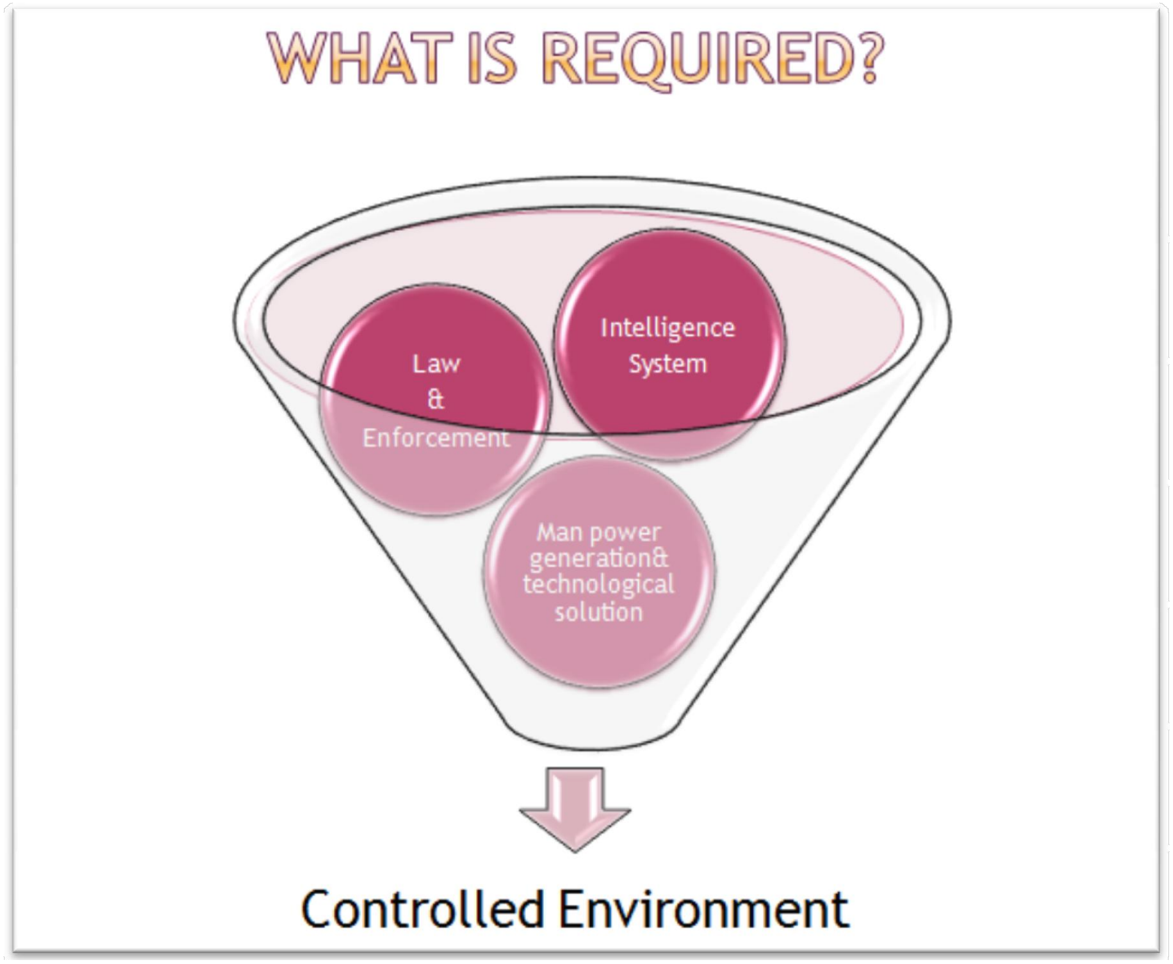
Proposed Solution:

The above mentioned challenges of cyber crime put before us the need to look for the solution that should address the complexity of cyber crime. The proposed solution works from three perspective i.e., technological need, intelligence system and law enforcement agencies.

1. **Technological Means:** Every nation is required to develop their indigenous product that should be used for the purposes of the nation's cyber security protection. The standards to check the tool and technology should also be developed and duly reviewed.

2. **Intelligence System:** In the world of cyber space, by intelligence system we mean that a dedicated team should be constitute through the legislation means and are responsible to protect, monitor and response in case of emergency for the country. This kind of team is known as computer emergency response team and should act as a backbone to the nations cyber security need. The other important aspect is the man power generation and therefore it is imperative for every nation to consider cyber security training and education as integral part of nation's wealth.

3. Law enforcement agency: Judiciary and legal system of the nation will play the pivotal role to strengthen the nation's cyber space environment. The nation will require a comprehensive legislation dedicated to address the various aspect of cyber security, cyber crime, cyber terrorism, e-evidence, etc. additionally, the investigative agencies requires specialize training and understanding to tackle cyber crimes.



Conclusion:

India is now become super power in Information technology and software industry. In past countries relied upon the power of conventional military forces, in information technology edge, future of a country is depend on the trained and well equipped cyber warfare unit.

Reference:

1. *www.security-gurus.de/papers/cyberwarfare.pdf*
2. http://www.cert-in.org.in/knowledgebase/annualreport/annualreport08.pdf
3. www.**cert**-in.org.in/
4. http://www.cert-in.org.in/roles.htm
5. http://isea.gov.in/isea/isea/currentstatus.jsp
6. http://isea.gov.in/isea/organization/rcdetails.jsp
7. http://isea.gov.in/isea/organization/pidetails.jsp
8. http://isea.gov.in/isea/organization/impagencys.jsp
9. http://www.ccc-rac.in/cybercrime.htm
10. http://www.slideworld.com/slideshows.aspx/CYBER-SKIRMISHES-ppt-2743472
11. http://www.mynews.in/News/India_Should_Develop_Cyber_War_Capabilities___N35343.html