CHAPTER – III

CYBER CRIME: A GLOBAL PERSPECTIVE

Cyber crime is a global issue. During the last half century, technologies have been developed that would enable people all over the world to get to know another while sitting in their rooms. The internet is a prime medium for such communication.¹

The World Wide Web in the internet has transformed global communications. An exciting new service, it provides the user with seemingly limitless access to news, products and services. The web is an entirely new medium for entertainment, communication and self-expression.²

Online services are becoming new targets for cyber criminals in the global cyber trends. Cyber criminals continue to refine their means of deceit as well as victims. In general, the global threats affecting users today are: new and sophisticated forms of attacks, attacks targeting new technologies, such as Voice over Internet Protocol (VOIP), peer-to-peer services, attacks targeting online social network, online services and particularly online banking services.³

The types and numbers of extent of crimes have been increasing over the years. As a result, United Nations has taken note of increasing trend of cyber crimes came up with several suggestions to prevent the cyber crimes. One such initiative is that guidelines released to prevent the types of cyber crimes.

Cyber Space ~ Cyber Crime

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The “offence” is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.4

Traditional Crime ~ Cyber Crime

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual property. Cyber crime in the context of national security may involve hacktivism, traditional espionage, or information warfare and related activities.

Cyber crimes have been reported across the world. Cyber crime is not amongst the most important revenue sectors for global organized crime. Because of this, the potential risks associated with malware have risen dramatically. Unlike in traditional crimes, the Information Technology infrastructure is not only used to commit the crime, but very often is itself the target of the crime. Pornography, threatening email, assuming someone’s identity, sexual harassment, defamation, spam and phishing are some examples where computers are used to commit

4 Criminal Investigation Department Review, Tamil Nadu – January 2008, Cyber Crime Scenario in India, article submitted by Dr.B. Muthukumaran, Chief Consultant, Gemini Communication Limited p.17.
crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

There are two sides to cyber crime. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that, the number of cyber crimes committed should be related to the number of victimizations experienced. Of course, there will not be a one-to-one correspondence since one crime may inflict multiple victimizations. Multiple crimes may be responsible for a single victimization. Some crimes may not result in any victimization, or at least in any measurable or identifiable victimization.5

---

**Comparison between Conventional Crime and Cyber Crime**6

<table>
<thead>
<tr>
<th>Conventional Crime</th>
<th>Cyber Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burglary</td>
<td>Hacking</td>
</tr>
<tr>
<td>Deceptive callers</td>
<td>Phishing</td>
</tr>
<tr>
<td>Extortion</td>
<td>Internet Extortion</td>
</tr>
<tr>
<td>Fraud</td>
<td>Internet Fraud</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Online Identity Theft</td>
</tr>
<tr>
<td>Child Abuse</td>
<td>Online Child Exploitation</td>
</tr>
</tbody>
</table>

---

**Cyber Crime Variants**

There are a good number of cyber crime variants. A few varieties are discussed for the purpose of understanding. The major cyber crimes reported, in India, are denial of services, defacement of websites, spam, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. ‘Net surfing’ by youngsters lures them into dangerous domain. The need for a conscious effort to checkmate the undesirable fallout of youngsters accessing and using the Internet is of concern.

---


Identification

In cyber crime, computer is an integral part of the criminal act. Computers are either victim of the crime or the tool used in the crime or the witness in a committed crime. Corrupting the operating system, stealing data/information, disrupting functioning of computer are examples where computers are victims. Credit card frauds, transaction of illegal goods via Internet, software piracy fall under the category or crimes where computer is the tool. While money laundering, drug trafficking, transaction of records, bullet board systems, etc., fall under the third and final slot of computers acting as witness to crime.

Classifications

Cyber crime is broadly classified into four basic categories – data related crimes, software crimes, Internet crimes and physical crimes. (i) Data related crimes involve fraudulent input of data in the hierarchy of levels – encoding, examining, checking, storing, converting and transporting data to be entered into the computer. (ii) Software crime is the use of viruses or other such damaging software such as Trojan Horse and Logic Bombs. Trojan Horse is a spy programme that will stalk spy and corrupt files in computer forcing them to send signatures on the progress of system processing to a designated path of device or telecom line. Logic Bombs are designed to carry out certain unwarranted commands on encountering pre-designated data or logic in a system. (iii) Internet crimes encompass those in which people are cheated by false, luring promises of

---

jobs, winning lotteries, etc. (iv) While physical crime includes theft, breakage, etc.  

**The Global Cyber Crime Scenario**

Cyber crime acts show a broad distribution across financial-driven acts, computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems.  

Perceptions of relative risk and threat vary between Governments and businesses.  

Individual cyber crime victimization is significantly higher than for ‘conventional’ crime forms. Victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorised access to an email account, vary between 1 and 17 per cent of the online population.  

Individual cyber crime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen the prevention efforts in these countries. Private sector enterprises in Europe report victimization rates of between 2 and 16 per cent for acts such as data breach due to intrusion or phishing. Internet content targeted for removal by governments includes child pornography and hate speech, but also defamation and government criticism, raising human rights law concerns in some cases. Some estimates place the total global proportion of internet traffic estimated to infringe copyright at almost 24 per cent.

---

Social Networking

Social Networking has been the fashion of the day both by youngsters and senior people around the world. While social networks bring lot of healthy developments, it also poses severe threats to a person personally and officially when it is done without security measures.11

Social Networking Scam

Social and business networking websites like Facebook, MySpace, Bebo, LinkedIn and Friendster allow us to create our own profile and share conversations, photos, videos, links and personal information with friends and other online users. Unfortunately scammers also use legitimate and trusted online networking services to create profiles using fake names. They then use these profiles to personally target victims with scams. There are two goals in most social networking scams; to spread quickly and to make money. With those billions of clicks per day, Like buttons help achieve that prompt and widespread propagation, particularly as Facebook users get wise to traditional social media scams.

Emergence of Global E-Commerce

The industrial revolution was perhaps the biggest change that businesses ever faced. In the beginning, we did everything manually, recording them on paper. Organisation maintained a clearly defined and often impenetrable boundary that separated them from the rest of the universe. In order to speed up the work, we computerized it. Then, we set up networks to share information pertaining to work. In our simple model of the business universe, the network first appeared

---

within the organisation. Interactions of the network with the outside world were almost zero. For any data to get added to or get out of the system, manual intervention was required.\textsuperscript{12}

\textbf{Statistical Data of USA on Cyber Crime}

The Internet Fraud Complaint Center of USA began operation on 8\textsuperscript{th} May 2000. In the year 2003, it was renamed as Internet Crime Complaint Center (IC3) under Federal Bureau of Investigation to better reflect the broad character of such criminal matters having a cyber (Internet) nexus. IC3 has received complaint across a wide variety of cyber crime matters, including online fraud (in its many forms), intellectual property rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters.

The following charts show the number of complaints received on cyber crimes and dollars lost under these crimes.\textsuperscript{13}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{chart.png}
\caption{Number of complaints from 2000 to 2009.}
\end{figure}

\textsuperscript{12} S.K.Bansal: \textit{Cyber Millennium Challenges and Opportunities}, A.P.H.Publishing Corporation, New Delhi, 2001, p.157

\textsuperscript{13} www.ic3.gov - Annual Reports browsed on 24\textsuperscript{th} June 2011.
Mr. Baroness Neville-Jone, Security Minister of United Kingdom said cyber crime costs the UK economy 27 billion a year. They are made up of 21 billion of costs to businesses, 2.2 billion to government and 3.1 billion to citizens.\textsuperscript{14}

It is estimated in Ireland that the cost of cyber crime to the Irish economy is over 600 million a year.\textsuperscript{15}

Cyber crimes are costing Singapore an estimated $1.25 billion as crooks get smarter in activities ranging from market manipulation to cyber espionage.\textsuperscript{16}

The top 10 countries by count given by individual complainants for the year 2009 which was numbered by bank are as follows:\textsuperscript{17}

- USA – 92.02%
- Canada – 1.77%
- UK – 0.96%
- Australia – 0.59%
- India – 0.42%

\textsuperscript{14} www.bbc.com released on 17\textsuperscript{th} February 2011 browsed on 17\textsuperscript{th} January 2016.
\textsuperscript{15} www.rte.ie browsed on 17\textsuperscript{th} January 2016.
\textsuperscript{16} https://readyspace.com.sg browsed on 17\textsuperscript{th} January 2016.
\textsuperscript{17} www.ic3.gov Annual Report for the year 2009 – browsed on 24\textsuperscript{th} June 2011.


- Puerto Rico – 0.20%
- Germany – 0.17%
- Mexico – 0.16%
- South Africa – 0.15%
- Philippines – 0.15%.

Much of this crime is transnational, organized and highly secretive, with major criminal groups operating in over 30 countries spread across 6 continents (no cyber crime has been detected yet to origin from Antarctica).\(^\text{18}\)

**INTERPOL**

The role of International Criminal Police Organization (Interpol) is to enable police around the world to work together to make the world a safer place. Its high-tech infrastructure of technical and operational support helps to meet the growing challenges of fighting crime in the 21\textsuperscript{st} century.

Interpol’s cyber crime programme is built around training and operations and works to keep up with emerging threats. It aims to:

1. Promote the exchange of information among member countries through regional working parties and conferences;
2. Deliver training courses to build and maintain professional standards;
3. Coordinate and assist in international operations;
4. Establish a global list of contact officers available around the clock for cyber crime investigations (the list contained 131 contacts at the end of 2011).

\(^{18}\) www.blackhat.com browsed on 17\textsuperscript{th} January 2016.
5. Assist member countries in the event of cyber-attacks or cyber crime investigations through investigative and database services;

6. Develop strategic partnership with other international organizations and private sector bodies;

7. Identity emerging threats and share this intelligence with member countries;

8. Provide a secure web portion for accessing operational information and documents.\(^9\)

**Supporting Police Worldwide**

Interpol works to ensure that police around the world have access to the tools and services necessary to do their jobs effectively. It also provides targeted training, expert investigative support, relevant data and secure communications channels.\(^{20}\) This combined framework helps police on the ground to understand crime trends, analyse information, conduct operations and, ultimately, arrest as many criminals as possible. In the year 1990, X.400 communication system was launched, enabling to send electronic messages to each other and to the General Secretariat directly. In 1992, an automated search facility for remote searches of Interpol databases introduced. In 1998, Interpol Criminal Information System (ICIS) database was created. In 2002, I-24/7 web-based communication system was launched, significantly improving NCB’s access to Interpol’s databases and services. Canada is the first country to connect to the system. Database of stolen and lost travel documents was launched. In 2005, first Interpol-United Nations Special Notices were issued for individuals subject to UN sanctions against Al Qaeda and the Taliban. Technology known as Mobile Interpol Network

\(^{19}\)www.interpol.int browsed on 29th May 2014.

Database/Fixed Interpol Network Database (MIND/FIND) allows frontline officers to connect directly to Interpol’s systems.

**A Global Presence**

Interpol has global membership of 190 countries. Each country maintains a National Central Bureau (NCB), staffed by national law enforcement officers. It forms the link with Interpol’s global network, enabling member countries to work together on cross-border investigations. The NCBs are increasingly involved in shaping the Organization’s direction.²¹

Interpol collects, stores, analyses and shares information on cyber crime with all its member countries through I-24/7 its global police communications system.

Interpol’s High-Tech Crime Unit facilitates operational co-operation among member countries through global and regional IT crime expert group meetings and training workshops, as well as co-operation among law enforcement, industry and academia. It also assists member countries in the event of cyber-attacks or cyber crime investigations through investigative and database services.

The first cyber crime police station in Asia was formed in Singapore.²²

**Legal Position around the Globe**

Problem of cyber crime induced many states to reconsider their own legislation. Nowadays more than 100 countries (including 60% Interpol members) have no laws regulating fighting cyber crimes. The problem in regulating cyber crime is that there are no uniform laws. Some countries, such as the UK, have cyber crime laws like the Computer Misuse Act (1990) that are well implemented.

---
²¹ [www.interpol.int](http://www.interpol.int) browsed on 29th May 2014.
²² Sun TV News: 7th December 2012 at 7.45 AM.
Other territories have laws that have yet to be fully implemented, while some countries are yet to make provisions for cyber crimes within their judicial system at all.\(^{23}\)

**Global anti-Malware Market**

Malware is software designed to infiltrate or damage a computer system without the owner’s informed consent.\(^{24}\) The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or programme code.

New analysis of Frost & Sullivan, World Anti-Malware Products Markets found that the world market for antivirus solutions reached $4,685 million in 2006, up to 17.1\% from $4 million in the previous year and expects this market to grow at a 10.9\% Compound Annual Growth Rate (CAGR) from 2006 to 2013, reaching $9,689.7 million by 2013.\(^{25}\)

**International Cyber Crime**

A significant problem that arises when working with cyber crime is that most crimes transit data through a multitude of international borders before reaching the final, intended target. Such circuitousness has a deleterious effect on investigating cyber crimes as well as the application of laws.\(^{26}\)

**The Changing Nature of Cyber Crime**

In the past, cyber crime has been committed by individuals and groups of individuals. However, that we are now seeing an emerging trend with traditional


\(^{25}\) www.frost.com

\(^{26}\) http://sysnet.ucsd.edu e-article on *Cyber criminal activity* submitted by Hemavathy Alaganandam, Pravin Mittal, Avichal Singh and Chris Fleizach
organized crime syndicates the presence of criminal minded technology professionals working together and pooling their resources and expertise.\(^{27}\)

The approach has been very effective for the criminals involved. In 2007 and 2008, the cost of cyber crime worldwide was estimated at approximately US $8 billion. As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth upto USD 1 trillion.

**Information Technology as Terrorist Weapon**

Terrorist groups engaging in cyber terrorism are noted for threats to commerce, public safety and national security. These threats can take any number of forms, but are generally parlayed into computer versus computer confrontations. While the current discussion focuses on the use of “high tech” applications in terrorist operations, “low tech” operations against a victim’s “high tech” infrastructure should not be ignored. Terrorist groups use their own computer technology to threaten or attack a victim’s computer resources. This can take the form of threats or attacks against national infrastructures that have become heavily reliant and interconnected to computer networks. Activity of this sort is tangible in nature and thus, generates most of the interest we have in cyber terrorism today. Cyber terrorist threats can include:\(^{28}\)

- rapid communication of threats to a wide or specific audience
- threats to public utilities and transportation
- threats to commercial institutions and transnational corporations
- threats to IGOs and NGOs
- threats to individuals

\(^{27}\) www.interpol.int browsed on 29th May 2014.

● threats to political groups or other ethnic, religious or nationalist entities (all of these can include other terrorist groups) identified as “the enemy”
● threats to security forces
● threats to nation states.

COUNTRIES AT STAKE

● LOW RISK: UK, Canada, France, Switzerland
● AVERAGE RISK: Brazil, Israel, Palestinian National Authority, Zimbabwe, Middle East Countries (USA, Saudi Arabia)
● HIGH RISK: China, India, Pakistan, North Korea, South Korea, Iran, Tatarstan, Kyrgyzstan, Ingushetia, Myanmar, Russia (Estonia, Georgia).

Important Cyber Crimes Reported Globally

Year 2000

In February 2000, hackers launched one of the biggest distributed denial-of-service attacks to date against eBay, Yahoo, Amazon, and others causing major business disruption to the owners of these websites. Whilst this was seen by most as an act of vandalism, there were a number of different views as to why these specific companies were targeted. One anarchist point of view is that they were attacked, because the Internet has become the new tool for exploiting mankind and that the emergence of e-commerce is killing the hopes that had for the Internet.29

---

In May 2000, a new virus called “I Love You”, also affected thousands of corporate websites, and many companies had to shut down their e-mail systems in an effort to stop its spread. A leading vendor of Anti-Virus software, Symantec, states that in terms of spreadability, the “I Love You” virus outranked anything seen so far. Unlike Melissa, this virus has the ability to destroy data, in particular pictures and music files. In the same year 2000, Activists in Pakistan and the Middle East defaced web sites belonging to the Indian and Israeli governments to protest oppression in Kashmir and Palestine. In October 2000, hacker break into Microsoft’s corporate network and accessed source code for the latest versions of Windows and Office. This attack went unnoticed for several weeks before Microsoft discovered it.\textsuperscript{30}

**Australian Hacker Responsible for Attacking SCADA Nodes of a Sewage Management System on 23-4-2000**

Vitek Boden, snubbed by the rejection of his job application, attacked the SCADA system of a Queensland Waste management company. Driving around with a laptop fitted with a radio transmitter, he commandeered SCADA systems at various waste treatment centers, and managed to release millions of liters of sewage into parks, rivers and even the grounds of a Hyatt Regency hotel. He was finally caught, when he was pulled over by police on his last mission. Examination of his laptop revealed software which could control SCADA systems, and its use was linked to the time of actual attacks. Boden was convicted in October 2001 and sentenced to two years in prison.\textsuperscript{31}

\textsuperscript{31} *Ibid.*
Russian “Carders” (Credit Card Thieves) in May 2001

Credit card thieves in Russia were using similar names to open multiple Paypal accounts, and then using these accounts to buy high-value computer goods from eBay auctions.

Paypal’s team investigating this issue used sniffer tools to capture the network traffic and analyzed it to determine the originating IP address. Using this and other information gathered in investigation, PayPal froze all fraudulent accounts opened by the perpetrators, who, by this time, had managed to purchase goods worth more than $1,00,000. Following this PayPal actually started receiving phone calls from the perpetrators demanding that the funds in their accounts be released to them. Being in Russia, the brazen perpetrators considered themselves out of reach.

The FBI got involved in the investigation and lured them into custody by offering them security jobs while posing as a high-technology company. Paypal’s investigative team then used EnCase, a forensic investigation toolkit, to gather evidence from their computers which was finally used to convict them.32

Attack on World Trade Center and Pentagon

Following the tragedies of September 11, 2001 attacks on the World Trade Center and the Pentagon, the realm of security received considerable attention, and there was increased awareness among wider groups of contemporary society. Shortly thereafter, the U.S. Patriot Act was enacted. This legislation brought about wide sweeping changes to a host of existing laws resulting in the enhancement of domestic security against terrorism and additional powers of surveillance,

32 http://sysneet.ucsd.edu e-Article on Cyber Criminal Activity submitted by Hemavathy Alaganandan, Pravin Mittal, Avichal Singh and Chris Fleizch.
investigation, and international money laundering. It also emphasized the need for information sharing in order to protect the critical infrastructures of telecommunications, energy, financial services, water and transportation.

It is not just terrorists that use technology to enact political agendas. It has been estimated that over 30 nations have developed the capacity to actively participate in cyberwarfare, including the USA, United Kingdom, China, Russia, France, Israel, India, Brazil and Iran.

Cyber intruders continue to steal proprietary technical and commercial information. They have shown an ability to establish “back doors” into systems they have penetrated for later use in data retrieval and coordinated cyber attacks on bigger systems. The capacity to engage in such acts is relatively inexpensive and readily available to large numbers of individuals and groups. In the public domain, there are many proofs of these capabilities.  

First Prosecution in USA on Cracking Operation

The first successful prosecution on cracking operation in the USA was in 2005. A 20 year old American, Jeanson James Ancheta pleaded guilty in a Los Angeles court to charges of conspiring to violate anti-spam and computer misuse laws and fraud. He admitted hijacking about half a million computer systems and using them to send out spam. Ancheta also admitted to selling access to his botnet to firms which fed pop-up ads to the infected computers. Among the machines infected were US Military computers in California and in Virginia.

---

Some Hollywood Movies on Cyber Crime

The Net 2.0

This is 2006 English movie concerns a computer system analyst who finds herself in a web of identity theft, robbery and murder when she lands in Turkey for a new job whose bank accounts were siphoned online and faced many problems. Finally all were detected by Interpol.

Die Hard

This is the movie released in the year 2007 in which the hero McClane is a divorced and estranged from his daughter. Cyber terrorists hack into computers at the Federal Bureau of Investigation of USA, who had sent hero to bring in computer hacker Mathew. The villain tells McClane that the terrorists are actually in the middle of a ‘first sale’ – a crippling cyber-warfare attack on the national infrastructure: Power, public utilities, traffic and other computer-controlled systems. The hero foils the criminals and saves the hostages.