CHAPTER 2

EVOLUTION AND CLASSIFICATION OF CYBER CRIMES AND CYBER TERRORISM

2.1 Introduction

In the cyber era of 21st century the second industrial revolution, as it is often called, the Internet and the network computers have posed the biggest ever challenge to the legal systems all over the world\(^1\). The new revolution brings new crimes. Cyber space\(^2\) is a unique medium for cyber criminals for three reasons. First, and most importantly, the use of computers and other equipment is a cheaper means to perpetrate crime. Second, cyber crime adds additional parties to the traditional perpetrator-victim scenario of crime. Thirdly, the criminals can hide their identity easily and the law enforcement agencies may never reached to them.

The advancement of the information technology sector has become life-line for the world’s economy. This new invention of the last century give fuel to the development, and new e-highway is also positively gets the place in the routine of people through various forms and contribute to the various socio-economic parameters such as employment, standard of living and diversity among others. There is no hesitation to say that information technology (IT) helps in the makeover of India’s image at the global level player in providing world-class technology solutions and business services. The government has been a key driver for increased adoption of information technology based products and solutions in the country.

In order to elevate and to promote Indian IT industry, the Government of India had set up a National Task Force on IT and Software Development to

---

\(^2\) The word ‘cyberspace’ was coined by the science fiction author William Gibson, when he sought a name to describe his vision of a global computer network, linking all people, machines and sources of information in the world, through which one could move or ‘navigate’ as through a virtual space.
examine the feasibility of strengthening the industry. Venture capital has been the main source of finance for software industry around the world. In line with the international practices, norms for the operations of venture capital funds have also been liberalized to boost the industry. It has embarked on various IT-enabled initiatives including in Public Services (Government to citizen services, citizen identification, and public distribution systems), Healthcare (telemedicine, remote consultation, and mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial Service (mobile banking/payment gateways), etc.

Human beings, by their very nature, have a tendency to find the destructive side of most innovations and advancements. Current technological developments present us with opportunities to enrich our lives by using simple, quick and high-quality devices. At the same time, these technological developments also hold the potential to be used as weapons in the hands of terrorists.

In particular, much cyber crime is carried out through the use of Internet Service Providers (ISPs), such as America Online. Third parties can develop ways to make criminal activity more expensive and may be able to do so in ways that the government cannot accomplish directly. Third, and more generally, a host of thorny problems arises because most activities that occur in cyber space are invisible to third parties and sometimes even to second parties.

So, the cyber space gives criminals a safer and gray space to accomplish their motives without being at the targeted place. It is necessary to understand the

---


5 Neal Kumar Katyal, “Criminal Law in Cyberspace”, University of Pennsylvania Law Review, April 1 2001. Available on http://lrd.yahooapis.com/_ylc=X3oDMTVvNDIxYm5mBF9TAzIwMjxNTI3MDIEYXZwQWQTDTHlazRUTFYzNEdRVjYWVDFRYVHeC5xMDYuMHVj a2pJb3dIyQzJFV3NGejbWZiX2xkQjRPX1YweDZPdVNOME9zVjg2ad012BGNgLSVudANi b3NyBHlJcnZpY2U2UDQ9TUVZbG5sDDQfJsGUEc3JjczHZpZWkZT3J5YVnZUF1M3N5ckZQMmNWZHJFZ1MwRG1lO0tVx6c0FETXR2/SIG=12pn9n86i/**http%3A//www.articlearchives.com/crime-law/criminal-offenses-cybercrime/1834657-1.html. Retrieved on 11 December 2011.
historical development of computer, internet and cyber crimes. The following
discussion provides historical development of computer, internet, World Wide
Web and cyber crimes.

2.2 Historical Background of Computer and Internet

“The origins of the internet lie in the military domain.”\textsuperscript{6} The information
society of today is nothing but the culmination of the electronic development and
the invention of communication system way back towards the end of the 19\textsuperscript{th}
century. After passing through prolonged inventory phases stretching over about a
century, in the year 1876, the telephone was patented by Grahm Bell. This can be
termed as the sapling sowed by him for the fast moving telephonic global
communication system of today about more than a century thereafter. Not only the
voice communication of yesteryears but also data transmission (through devices
like fax machines and computers) comprise the communication world of today.
The history of the communicational progress and the internet can be divided into
various phases.

i. Phase I - Jungle Telegraph to Mobile Phone

“……to write far” is the English explanation of the Greek expression of
“telegraph”. In it, the human society saw the first substitute to direct dialogue. The
earliest forms of telegraphy the mankind saw was smoke, fire, drum signals often
termed as “Jungle Telegraph”. These were the very first methods to say something
from a distance. As early as 1500s, the contemporary thinkers had first started
deliberating on the use of light and electric impulses as the means of
communication. The first crude system was made without electricity; it was a

\textsuperscript{6} S. Furnell, “Cybercrime: Vandalizing the Information Society”, p. 103 Great Britain: Pearson
Education Limited 2002. Cited in Suleyman Ozeren, “Global Response to Cyberterrorism and
Cybercrime: A Matrix for International Cooperation and Vulnerability Assessment”, Dissertation
submitted for the Degree of Doctor of Philosophy, University of North Texas, August 2005.
system of semaphores\textsuperscript{7} or tall poles in which the messages were conveyed physically using flags or lights\textsuperscript{8} but the sound was not easily audible.

William Sturgeon invented the electromagnet in 1825 which led to an evolution in electronic communication. The earlier non-electronic telegraph invented by Claude Chappe in 1794 was gradually overtaken by the new experiments in the field like the invention by Harrison Dyer who successfully experimented with transmission of electronic sparks through chemically treated paper tape to burn dots and dashes. Three telegraph system based on electromagnet were developed by Joseph Henry in 1830, by William Cooke and Charles Wheatstone in 1837 and by Samuel Finley Breese Morse who improved Henry’s invention. Within a few decades thereafter, the first trans-Atlantic cable was laid in 1858 but the successful link was achieved in 1866.

Before the invention of electromagnetic telephones, mechanical acoustic devices existed for transmitting speech and music over a distance greater than that of normal direct speech. The earliest mechanical telephones were based on sound transmission through pipes or other physical media\textsuperscript{9}. The highly similar acoustic tin can telephone, or lover’s phone, has been known for centuries. The modern telephone is the result of work of many people\textsuperscript{10}. Graham Bell’s attempt to improve the telegraph resulted in telephone. Until 1877, telegraph remained the only means of long distance communication but the position was changed and the telephone emerged as the rival technology in the field of communication. It was the historic day 10\textsuperscript{th} March, 1876 when Bell invented telephone. The quicker but less reliable media, the telephones were just born.

\textsuperscript{7} Claude Chappe in 1790, developed as system of wooden shutters on a tower which could show 63 different signals. Obviously, it was liked by the military which helped them to send signals in remote areas. Napoleon used Chappe telegraph in his invasion of Italy.

\textsuperscript{8} Samuel Finley Breese Morse, “The Invention of the Telegraph”, papers at the Library of Congress.


The computers can not strictly be called the contemporaries of telephone, yet it was the concomitant research and development going on in the field of calculations and computing that complemented to the new inventions in the field of communication. The birth of computers and computer law are inexorably intertwined and fixing of their origin is difficult. Blaise Pascal who built the first digital but non electronic computer in 1642 taught to the world the ABC of computer building. Charles Babbage considered as the “father of computers” is credited with inventing the first medicinal computer that eventually led to more complex designs. He began in 1822 with what he called the difference engine, made to compute values of polynomical functions. Herman Hollerith developed a mechanical tabulator based on punched cards to rapidly tabulate statistics from millions of pieces of data. Machines built by him were used in the 1890 census and was adopted by the International Business Machines Corporation (IBM) in the decades of the 20th century. Many great scientists can be credited for sowing the sapling of brisk and accurate calculations; however, it was Alan Turning, an Englishman who published On Computable Numbers which adapts the notion of algorithms to the computation of functions. This led to the first colossus computer being built in 1941 and Mark II in 1944.

In 1946, in the University of Pennsylvania, first general purpose electronic computer was built by the two engineers. It was called Electronic Numerical Integrator & Computer (ENIAC). The weight was above thirty short tons11. Invention of transistors in 1947 led to the production of faster and more reliable electronic computers. In 1958, Control Data Corporation introduced the first fully transistorized computer designed by Seymour Cray. Miniaturization continued through the 1960s and in 1965, the first successful commercial mini-computer was launched called PDP-8. Computers at this stage meant mainframe computers. By

---

late 1960s, big businesses started relying on computers and the first PC was introduced in 1975\textsuperscript{12}.

Much before the world was introduced to the internet, its main plank—the computers were already active. It took 101 years to move from a static telephone to a mobile phone and less than further twenty years to reach anyone globally through a cell phone\textsuperscript{13}.

\textbf{ii. Phase II - From ARPANET to the Semantic Web}

With the launch of first artificial earth satellite by the USSR in 1957 the internet age had started. Next was the USA who forms the Advanced Research Projects Agency (ARPA) within the Department of Defence (DoD) for the purpose to enable US military in science and technology. The year 1962 is historically very important because of RAND Paul Baran, of the RAND Corporation (a government agency), was commissioned by the U.S. Air Force. Its main objective was to do a research for the control and command over its missiles and bombers, after a nuclear attack. This was to be a military research network that could survive a nuclear strike, decentralized so that if any locations (cities) in the U.S. were attacked, the military could still have control of nuclear arms for a counter-attack\textsuperscript{14}. Baran’s finished document described several ways to accomplish this. His final proposal was a packet switched network.

In 1968 ARPA was awarded the ARPANET contract to BBN and it selected Honeywell minicomputer as base for building the switch. Thereafter in 1969 a physical network was constructed and linked it with four nodes: University of California at Los Angeles, SRI (in Stanford), University of California at Santa

\textsuperscript{12} Computers came to non-specialists part of the society when in 1977; two American students, Jobs and Woznaik founded the Apple Computer and introduced the Apple 11 PC. In 1978, the 5.25 inches floppy disk became the standard medium for software. In 1981, the IBM entered the PC market, with its PC based on the Intel 8088 chip. In 1981 itself, only Microsoft created MS-DoS on a floppy. Change was catching up speed this time and 2M PCs were in use globally and today it can be around 500M or more. Windows came up on the scene in 1990. While the 3.5 inch disk drive was introduced in 1984; the IBM launched its PS/2 machines.

Barbara, and University of Utah. Ray Tomlinson of BBN created the first e-mail program in 1972 and the Advanced Research Projects Agency (ARPA) was renamed The Defence Advanced Research Projects Agency (or DARPA) ARPANET was currently using the Network Control Protocol or NCP to transfer data. This allowed communications between hosts running on the same network. Development began on the protocol later to be called TCP/IP, it was developed in 1973 by a group headed by Vinton Cerf from Stanford and Bob Kahn from DARPA. This new protocol was to allow diverse computer networks to interconnect and communicate with each other.

Vint Cerf and Bob Kahn use first time ‘Internet’ in the paper on Transmission Control Protocol in 1973. In 1976 Dr. Robert M. Metcalfe develops Ethernet which gives data transfer a new speed. This was a crucial component to the development of LANs. The practical use of packet satellite project started. A new SATNET, Atlantic Packet Satellite Network, was born and it linked the US with Europe. Amazingly, it used INTELSAT satellites that were owned by a consortium of countries and not exclusively the United States government. UUCP (Unix-to-Unix CoPy) developed at AT&T Bell Labs and distributed with UNIX one year later. The Department of Defence began to experiment with the TCP/IP protocol and soon decided to require it for use on ARPANET.

Steve Bellovin and Tom Truscott and Jim Ellis created the USENET (the decentralized news group network) in 1979 which was based on UUCP. The Creation of BITNET, by IBM, “Because Its Time Network”, introduced the “store and forward” network. It was used for email and list servers. In 1981 National Science Foundation was created CSNET 56 Kbps network for institutions without access to ARPANET. Vinton Cerf proposed a plan for an inter-network connection between CSNET and the ARPANET. Internet Activities Board (IAB)

---

15 Ibid.
16 Ibid.
17 A graduate student at University of North Carolina and Tom Truscott and Jim Ellis were the programmer in it.
was created in 1983. On January 1st, every machine connected to ARPANET had to use TCP/IP and it became the core Internet Protocol and replaced NCP entirely.

Domain Name System (DNS) was created by the University of Wisconsin which allowed packets to be directed to a domain name, which would be translated by the server database into the corresponding IP number\textsuperscript{18}. This invention makes process, easier to access other servers, because now need not to remember the numbers. ARPANET was divided into two networks: MILNET and ARPANET. MILNET was to serve the needs of the military and ARPANET to support the advanced research component, Department of Defence continued to support both networks. Upgrade to CSNET was contracted to MCI. New circuits would be T1 lines, 1.5 Mbps which is twenty-five times faster than the old 56 Kbps lines. IBM would provide advanced routers and Merit would manage the network. New network was to be called NSFNET (National Science Foundation Network), and old lines were to remain called CSNET\textsuperscript{19}.

In 1985 new T1 lines began deploying by the National Science Foundation and finished by 1988. In 1986 the Internet Engineering Task Force (IETF) was created to serve as a forum for technical coordination by contractors for DARPA working on ARPANET, US Defence Data Network (DDN), and the Internet core gateway system. In 1987 the Corporation for Research and Educational Networking (CREN) was formed with the merger of BITNET and CSNET in 1987. Soon after the completion of the T1 NSFNET backbone in 1987, traffic increased so quickly that plans immediately began on upgrading the network again. Merit, IBM and MCI formed a not for profit corporation called ANS, Advanced Network & Services, which was to conduct research into high speed networking. It soon came up with the concept of the T3, a 45 Mbps line. NSF quickly adopted the new network and by the end of 1991 all of its sites were connected by this new backbone\textsuperscript{20}.

\textsuperscript{18} Supra Note 14.
\textsuperscript{19} Ibid.
\textsuperscript{20} Ibid.
After completion of the T3 lines, original 50Kbps lines of ARPANET were taken out of service and the Department of Defence disbanded the ARPANET and was replaced by the NSFNET. Tim Berners-Lee and CERN in Geneva implemented a hypertext system to provide efficient information access to the members of the international high-energy physics community. In 1991 CSNET (which consisted of 56Kbps lines) was discontinued having fulfilled its important early role in the provision of academic networking service. A key feature of CREN is that its operational costs were fully met through dues paid by its member organizations.

A new network NREN (the National Research and Education Network) was established by the NSF for high speed networking research. World-Wide Web released in 1992 by CERN. InterNIC created by NSF in 1993 to provide specific Internet services: directory and database services (by AT&T), registration services (by Network Solutions Inc.), and information services (by General Atomics/CERFnet). The WWW, called “Mosaic for X” was developed by Marc Andreessen and NCSA and the University of Illinois. There were no major changes to the physical network but the most significant was the growth of networks. The new networks were added at large scale and hundreds of thousands of new hosts were added to the INTERNET. ATM (Asynchronous Transmission Mode, 145Mbps) backbone is installed on NSFNET.

In April 30, 1995 it was announced by the National Science Foundation that direct access to the NSF backbone will be allowed. The National Science Foundation entered into a contract with the four companies for selling connections to groups, organizations, and companies. An annual fee of $50 was imposed on domains, other then .edu and .gov domains. Most Internet traffic is carried by backbones of independent ISPs, including MCI, AT&T, Sprint, UUenet, BBN planet, ANS, and more. The Internet Society, the group that controls the

---

21 Ibid.
INTERNET, researches new TCP/IP technology that will be able to have more than the approximately 123.5 million addresses currently available\textsuperscript{23}. In the transition phase the problem arises how both the old and the new addressing systems will be able to work at the same time\textsuperscript{24}. Commercial development of the World Wide Web exploded over the course of these four years. Learn about the Coarsegold Era Dataset—the millions of web sites developed by non-professionals during these years\textsuperscript{25}.

A new technology recommendation called IPv6 is suggested to replace the current IPv4 technology. IPv4 allows for fewer than 4.3 billion directly connected Internet devices, problematic because the world population (as of 2009) is well over 6.5 billion. In 1999, a wireless technology called 802.11b, more commonly referred to as Wi-Fi, is standardized. Over the years that follow, this technology begins appearing as a built-in feature of portable computers and many handheld devices\textsuperscript{26}.

Under the project of One Laptop Per Child Project, Netbooks\textsuperscript{27} were distributed among the students, sparks the network industry in 2005. Multi-touch technology replaced the traditional keyboard and mouse systems. Ciplex builds world’s first multi-touch website using silverlight ciplex unveils world’s first full multi-touch web experience ushering in the future of human-to-computer interfaces in December 2010\textsuperscript{28}. United States launched 4G Wireless Networks in December 2010 which allowed high-speed connections to devices such as cell phones, tablet computers, netbooks, and laptops. It was 2011 when technology companies started working with educators and independent developers, for

\textsuperscript{24} Supra Note 14.
\textsuperscript{27} Netbooks are small portable computers with extended battery life and built-in Wi-Fi connectivity.
\textsuperscript{28} Supra Note 25.
improving education system and to provide for immersive experiences, applying the best learning techniques with technology.\textsuperscript{29}

\section*{iii. Evolution of World Wide Web}

The World Wide Web (abbreviated as WWW or W3, commonly known as the web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks. The web was developed between March 1989 and December 1990.\textsuperscript{30}

In March 1989, Tim Berners-Lee wrote a proposal that referenced ENQUIRE, a database and software project he had built in 1980, and described a more elaborate information management system.\textsuperscript{31} It was further worked and published a more formal proposal in 1990 with help from Robert Cailliau with a possibility of a read-only web would be developed within three months and that it would take six months to achieve “the creation of new links and new material by readers, authorship becomes universal” as well as “the automatic notification of a reader when new material of interest to him/her has become available.”\textsuperscript{32,33} By 1991, people outside of CERN joined the new Web community. Very important to the growth of the Web, CERN announced in April 1993 that the World Wide Web technology would be available for anyone to use on a royalty-free basis. The first server outside Europe was set up at the Stanford Linear Accelerator Center (SLAC) in Palo Alto, California, to host the SPIRES-HEP database.

\textsuperscript{29} Ibid.
\textsuperscript{33} “Tim Berners-Lee’s original World Wide Web Browser”. “With recent phenomena like blogs and wikis, the web is beginning to develop the kind of collaborative nature that its inventor envisaged from the start.” Available on http://info.cern.ch/NextBrowser.html., Retrieved on 27 July 2013.
In 1994 Tim Berners-Lee left the European Organization for Nuclear Research (CERN) and founded the World Wide Web Consortium (W3C) October 1994. By the end of 1994, while the total number of websites was still compared to present standards, quite a number of notable websites were already active, many of which are the precursors or inspiration for today’s most popular services. The web is a collection of documents and both client and server software using Internet protocols such as TCP/IP and HTTP. Tim Berners-Lee was knighted in 2004 by Queen Elizabeth II for his contribution to the World Wide Web34.

Many web pages use HTML to reference the URLs of other resources such as images, other embedded media, scripts that affect page behavior, and Cascading Style Sheets that affect page layout. The browser will make additional HTTP requests to the web server for these other Internet media types. As it receives their content from the web server, the browser progressively renders the page onto the screen as specified by its HTML and these additional resources35.

Many domain names used for the World Wide Web begin with www because of the long-standing practice of naming Internet hosts (servers) according to the services they provide. The hostname for a web server is often www, in the same way that it may be ftp for an FTP server, and news or nntp for a USENET news server. These host names appear as Domain Name System or [domain name server] (DNS) sub domain names, as in www.example.com. The use of ‘www’ as a sub-domain name is not required by any technical or policy standard and many web sites do not use it; indeed, the first ever web server was called nxoc01.cern.ch.36 The primary function of a web server is to deliver web pages on the request to clients. This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets and scripts.

35 ibid
Early studies in 1998 and 1999 estimating the size of the web using capture/recapture methods showed that much of the web was not indexed by search engines and the web was much larger than expected\(^\text{37}\). From 2000 to 2014 the growth in percentage of internet users worldwide is 741 and total number of users are till mid of 2014 were 3,035,749,340\(^\text{38,39}\). According to a 2001 study, there was a massive number, over 550 billion, of documents on the Web, mostly in the invisible Web, or Deep Web and in 2015 it increased to 241.62 million pages\(^\text{40}\). Statistics measuring a website’s popularity is usually based either on the number of page views or on associated server ‘hits’ (file requests) that it receives\(^\text{41}\).

The web has given the criminals a new and highly sophisticated preferred pathway for spreading malware. Cyber criminals used for the ends of their motives identity theft, fraud, espionage and intelligence gathering, etc.\(^\text{42}\). Web-based vulnerabilities now outnumber traditional computer security concerns,\(^\text{43}\) and it has been found by Google that about one in ten web pages may contain malicious code\(^\text{44}\). It has also found that the majority of web-based attacks took


\(^{40}\) The size of the World Wide Web (The Internet), http://www.worldwidewebsize.com/, Retrieved 5 March 2015.

\(^{41}\) Supra Note 34.


place on legitimate websites, and most of them are hosted in the United States, China and Russia as measured by the Sophos.\(^{45}\)

### 2.3 Cyber Crime

The new millennium brings new crimes. Cyber crime is a crime which committed by the criminals in a cyber environment using Internet, computer networks, and wireless communication systems as a tool or target. Cyber crime can be regarded as “computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks.”\(^{46}\) In other words, cyber crime involves crime committed through the use of the computer.

#### 2.3.1 New Challenge - Cyber Crime

In fact, 21\(^{st}\) Century, the societies are increasingly getting transformed into Knowledge Societies and their inhabitants into Knowledge Networkers who are more informed of the events happening locally and globally. Their actions are based on the strong foundation of knowledge which is universal, objective, timely and retrieved from various sources. People are becoming more aware of their rights and opportunities\(^{47}\). However, this revolutionary change is brought by computer, internet and information technology. This has lead to new ways of functioning of government and business\(^{48}\).

Very interestingly, the question now arises—what is cyber crime? The description of the cyber crime is very problematic. The first difficulty is to provide a definition of cyber crime, as at the first point of time there is no uniform or universally accepted definition. This is not surprising, given different legal

---


traditions around the word and the fact that cyber crime is used as an umbrella term to refer, partially at least, to a very recent set of activities that have yet to be incorporated fully into national legal regimes around the word\textsuperscript{49}.

Cyber crime is invariably used with “computer crime”, “computer misuse” or “IT crime”.

**2.3.2 Meaning and Definition of Cyber Crime**

**a. Information Technology Act 2000**

With regards to exact definition of cyber crime, it has not been statutorily defined in any statute or law as yet. Even the IT Act, 2000 does not contain the definition of cyber crime. However, cyber crime may precisely be said to be those species of crime in which computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus, any activity that uses computer as an instrument, target or a means for perpetrating further crime, falls within the ambit of cyber crime.

**b. Prof. S.T. Viswanathan**

Prof. Vishwanathan has given three possible definitions of cyber crime and these are as follows:

a. Any illegal action in which a computer is the tool or object of the crime i.e., any crime, the means or purpose of which is to influence the function of a computer,

b. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

c. Computer abuse is considered as any illegal, unethical or unauthorized
behavior relating to the automatic processing and transmission of data\textsuperscript{50}.

c. **UN Congress on Prevention of Cyber Crime and Treatment of Offenders**

Cyber crime as defined internationally by the UN Congress on Prevention of Cyber Crime and Treatment of Offenders\textsuperscript{51} comprises of following two categories:

i. **Narrow Sense**: Cyber crime in a narrow sense connotes a computer crime and includes any illegal behavior directed by means of electronic operations that targets the security of the computer systems and the data processed by them.

ii. **Broader Sense**: Cyber crime in broader sense includes all computer related crimes and consists of any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Cyber crime is the most dangerous of all crimes because of magnitude of the loss, it is causing today and its potential, the ease with which it is committed; its invisibility and the disregard for geographical boundaries; the difficulty in investigation, collection of evidence and the successful prosecution of the cyber criminals and the cost of dealing with cyber crimes by law enforcement and protective technology. As rightly remarked by Dave Marcus\textsuperscript{52}:

“In a lot of ways, the criminals are doing a better job of communicating than the security industry itself; we tend to operate in our own groups, whereas these people are sharing code and algorithms and doing so on an increasingly frequent basis.”

\textsuperscript{50}S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, p. 81, Bharat Law House, New Delhi, 2\textsuperscript{nd} ed. 2001.

\textsuperscript{51}Tenth UN Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17 2000.

The term ‘cyber crime’ refers to the use of a computer to facilitate or carry out a criminal offense. A computer crime is defined by the US Department of Justice, “…...as an illegal act requiring knowledge of computer technology for its perpetration or prosecution.”

Cyber crimes are harmful acts committed from or against a computer or network differs from most terrestrial crimes. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

A computer can be electronically attacked. It can be further subdivide by distinguishing among acts that involve:

i. unauthorized access to computer files and programs,
ii. unauthorized disruption of those files and programs, and
iii. theft of an electronic identity.

An example of the first category is a break-in to Ministry of Defence (India) computers. An example of the second category is the ILoveYou Worm. The third category, identity theft, occurs when a person’s or entity’s identity is wrongfully appropriated.

The above crimes involve situations in which a computer is the subject of an attack. A rather different type of computer crime occurs when a computer is

53 Supra Note 5.
56 Supra Note 5.
used to facilitate or carry out a traditional offense. Complicated insurance fraud, large check-kiting operations, and other sophisticated forms of white collar crimes rely on computers to run the criminal operation. In these cases, computers make it easier to carry out a crime in realspace. In these circumstances, computers are tools that expedite traditional offenses. Donald Brackman rightly commenting on the Annual Cyber crime Report said,

“.......the criminals are taking full advantage of anonymity; they are developing sophisticated means of defrauding unsuspecting consumers. Internet crime is evolving in ways we couldn’t have imagined just five years ago.”

As news reports suggest, cyber crime is becoming an increasingly common form of criminal activity. The numbers are staggering. Yet many believe that cyber crime is still in its infancy, and that criminals have not yet

---

58 Donn B. Parker, Fighting Computer Crime - A New Framework for Protecting Information, Robert Ipsen, USA, 1998. Because of the broad nature of crimes in cyberspace and the ease of committing them, there is no one “type” of cybercriminal. Their profiles span the gamut of society. Mark D. Rasch, “Criminal Law and the Internet”, in “The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues” pp. 141-142; Joseph F. Ruh, Jr. ed., 1996. (“Computer criminals are not of a discrete type. They range from the computer world equivalent of a juvenile delinquent, the hacker or cyberpunk, to the sophisticated white-collar embezzler attacking financial institution computers, and include cyberterrorists, extortionists, spies, petty thieves and joy riders.”).
59 Of course, sometimes an act will overlap categories. A boy who breaks into a record label’s stored computer recordings to listen to an unreleased song by his favorite band, and who then decides to use Napster to distribute the song to his friends, both commits unauthorized access and carries out a traditional offense. The only important definitional principle at stake is to avoid unnecessarily forcing expansion of the last category, traditional offenses. In today’s society, virtually everything has some nexus to a computer. Using WordPerfect to type a threat to the President is rather different than using a computer program to place thousands of copies of copyrighted material on the internet. Mark D. Rasch, Criminal Law and the Internet, in The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues 141, 144. In the latter, the computer is achieving something that would be quite difficult to do without computers—namely, rampant distribution of the illegal material. It is this use of hardware and software that this Article addresses.
60 NW3C Director, 13-03-2010-FBI release 2009 Annual Reports on Cybercrime.
reached their potential. This is likely to change. As more targets in realspace are hardened against criminal acts, more geographic substitution from realspace to cyber space will occur. Damage to computer related property is more straightforward. The crime has been committed when a person damages a computer, computer systems, computer data, computer programs, or other computer-related property. As early as ten years ago, reports began to describe computer crime as the “weapon of choice” among white-collar criminals. Thus, the queer nature of the latest crimes and the technical potentiality of the cyber criminal is the biggest challenge faced by the information society today.

Nevertheless, law enforcement has not responded adequately to the threat. As one industry analyst puts it, “law enforcement online ranges from haphazard to nearly nonexistent.”

Although the computer world may exist only in intangible form, it affects and in some cases controls our physical environment and lives to a very significant extent. The shift of crime to intangibles has staggering impact on the society, both socially and economically. Never before in the history of mankind has science been so cruel to the legal world.

2.4 Characteristics of Cyber Crimes

Cyber crimes can go unnoticed, undetected and unreported due to its...
anonymity. There are several mechanisms that facilitate anonymity encryption being the most common methods. Encryption has become an essential part of doing business on the internet for companies and consumers alike. And the rising use of encryption technology has long been a concern of the FBI which has said the technology could be devastating to criminal investigations. Within a millisecond, the cyber criminals can hack/attack several computers in different parts of the world. Cyber crimes are the scene less crimes. The scene of the crime in traditional scene is an essential requirement for the detection process. However, cyber crimes cannot be bound down to a particular scene. A hacker in America can hack a computer in China or Delhi through software and deliver payments out of, say, a bank in Japan to the account of a person in Australia.

A traditional policeman will find it difficult to understand where the scene of crime lies and can even question whether there is a scene of crime at all. Cyber crimes are borderless. It can transcend state and national boundaries, in no time. The operational canvass in a computer crime is vast and the criminal respects no national borders. Sitting comfortably in far off countries, the entire economy of another nation could be destroyed. Old concepts of jurisdiction in crime investigation have become irrelevant, as the whole world could be the crime scene in a network crime.

Though the traditional crimes may inflict heavy damage to the victim, he is not totally devastated by it. In the case of bank robberies, for example, the quantum of losses is constrained by the weight and volume of currency that can be carried away by the burglars. The amount burled does not close down the bank operations permanently. The chances of robbery taking place again in the same bank are remote since it is possible to take suitable precautionary measures and revamp the security of the bank. The loss of goodwill is also not very huge. On the contrary, in case of computer crimes, its impact is very severing and it is not a one-time blow but may be a long-term one. It could cripple the operations of the

---

victim and in most of the cases maim them permanently. More than the financial loss, it is the loss of customers that would deliver the knockout punch, especially in case of companies whose main businesses are dependent on the internet, i.e., on e-commerce. The customers would lose faith on the seller and all the investments made to gain that trust lost through the actions of few clicks.

2.5 Cyber Criminal

The emerging information and communication technology inevitably has an immense impact on the life of the people in modern time. The real advantages and benefits of global connectivity explore by the cyber criminals to carry on their criminal activities in cyber space. Computer crimes are committed mainly for money but that is not the sole reason. In fact range of motives in such crimes depends on the type of the cyber crimes. These may be committed to personal vendetta; blackmailing; ego; mental aberrations; mischief; sexual gratification; stealing vital information; damaging, destroying or changing vital computerized control systems at various installations. The website of the Cyber Crime Cell, Mumbai states greed, power, publicity, revenge, adventure, desire to access forbidden information, destructive mindset, wants to sell new security services are generally the motives of the cyber criminals71.

Cyber criminals can be classified into various groups and categories. The cyber criminals are hi-tech knowledgeable and expert persons who easily invade the rights of computer users by penetrating to their computer system or computer networks. Cyber criminals usually indulge in techno-vandalism causing damage to files and programs of the computer user without having monetary benefits, but for the adventure or the creating panic in the public. They may constitute various hi-tech groups or organizations as per requirements or objectives of their criminal activities.

Some of the young or new users of computers having the excitement to

explore the web, get into the criminal activity just for the sake of fun and may not be aware that it is illegal, wrong or involve any harm. However, there is also a set of criminals who love to cause damage intentionally but not for the sake of any monetary gain. Some criminals may find it to break into other’s computers. There is also a serious set of cyber criminals which may be organized and professionals who can launch serious attacks on large scale especially on banks and other financial institutions. Therefore categories of these cyber criminals vary with their experiences with computers, their technical skills, age and their motives above all. Besides the techno-criminals, the other category of cyber criminals may be as follows:

2.5.1 Professional Hackers and Crackers

As earlier discussed hacking stands for intruding into a computer system or network illegally, without the permission of the authorized person. Hackers write or use ready-made computer programs to attack the target computer. They are equipped with all in and outs of computers and programming and thus are quite capable to launch complicated intrusions. Professional hackers hack for personal financial gains. Thus they launch cyber attacks like transferring money from various bank accounts to their own account or stealing of the credit card information. Sometimes such attacks of stealing information are followed by cyber extortion wherein they extortion from big companies, threatening them to leak out the information in case of non-payment.

Hacking becomes highly paid white collar crime. Use of computer in business makes big business entities vulnerable. Vast use of computers for e-business and industrial management for storing data and information in electronic form has led these enterprises to employ some to filch the credible, reliable and

---

73 “Cyber Crimes”, Supra Note 71.
74 ‘Hacker’ is a person who is good at programming or operating systems and maliciously meddles with the computer software to extract sensitive information by poking around. Hackers who meddle with the computer system maliciously or for criminal purposes are technically called as ‘Crackers’.
valuable information for commercial gain. The temptation of hiring the professional hackers in business or industrial intelligence also flows from the fact that no physical presence is required to access to critical data. They are also employed to penetrate the systems of the employer as a measure to make it safe by detecting the loopholes.

Hackers are mostly organized together to accomplish certain objective. Hacktivists work with a particular motive which may be to avenge their political bias, fundamentalism or an act done for some big business organization for causing damage to its rival competitors. Thus, the motive may be social, political, communal or commercial activism etc. Pakistani hacktivists mainly target the Indian Government sites with political motives also are known to be world’s most notorious hackers.\(^\text{75}\)

It is also believed that hackers who wanted to distinguish themselves from the crackers carved out this word themselves. Further it is supposed that while the hackers have a great deal of understanding of computer systems to develop their own hacking software; the crackers tend to be unskilled and inexperienced comparatively. They are not very sophisticated experts and launch their cracking attacks just by downloading free hacking software from hackers’ web sites. Even though the crackers cannot compete with hackers technically, but they are considered quite dangerous due to their reckless and irresponsible use of sophisticated software for illegal purposes. Lastly, it must be clarified that from the perspective of Indian laws, there is no such difference between the terms cracking and hacking.

### 2.5.2 Spies

Cyber Espionage has become very common since there have been a heavy computerization of industries, companies or organizations. Lot of reliance is placed on computer systems and networks for the purpose of electronically storing

---

and using information on industrial project, plans, researches and experiments. Such spies are hired by the industries quite often these days. Money is the natural motive behind such activities as the competitor who hires such spies is ready to pay quite handsomely for gathering information which value millions of dollars to them. Such espionage is not only limited to economic competitors. Even many governments, organized criminals, guerrillas and terrorists have been using online spies for collecting military and other intelligence related information.

2.5.3 Organized Hacktivists

The hackers which are organized for the purpose of getting certain objectives fulfilled by force of their hacking exploits are known as organized activists\(^{76}\). Reasons behind their organization could be many. They would have joined hands for fulfilling their political bias or even fundamentalism. Often they are quite well funded\(^{77}\). Usually they endeavour to commit cyber crimes like hijacking and defacement of websites or even in redirecting traffic to some spoofed website. Generally they target their attacks on government websites, along with financial institutions, international and multinational organizations\(^{78}\).

A stunning example of work of political hacktivists came to light in the recent past when around two hundred well known Indian websites were attacked by a Pakistani hacker group know as Pakistani Cyber Warriors (PCW)\(^{79}\). These attacks are part of cyber war that started in May 1998 between the political hacktivists of both the countries after India conducted some nuclear tests. After the Indian government announced the nuclear tests officially, the Pakistani hacker group, posted anti-nuclear messages on the website of the Bhabha Atomic Research Centre, by intruding into it illegally. After the 26/11 Mumbai attacks, a new cyber war is started between the organized hacktivists of both the countries.

Many of the Indian and Pakistan government websites were attacked and defaced in the unhealthy atmosphere that prevailed between both the countries after the Mumbai Terror attacks in November 2008. The website of the Oil and Gas Regularity Authority of Pakistan was hacked by the Indian Group Guards of Hindustan who posted their group’s logo and the Indian national emblem on the website. The hackers in Pakistan responded by hacking the websites of Oil and Natural Gas Corporation of India (ONGC), the Centre for Transportation Research and Management, Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, and the Kendriya Vidyalaya Sangathan. This attack is said to be launched by the Pakistani group known as Pakistan Cyber Army. Thus, hacker groups from both the countries tried to get the upper hand. In this process this situation worsened when Eastern Railways website was defaced by another Pakistani hacker group known as Mianwalian of Whackerz. This was not the end as the website of the State Bank of India also got hacked. In these cyber wars Pakistani hacktivists seems to have an edge over Indians as they are said to be quite well organized in groups.

On the other hand Indian hackers involved in this cyber war are supposedly working alone. Indeed the figures corroborate this fact as number of four Indian websites being hacked in 1999 was reached to 72 in year 2000. On the other hand, the rise in statics of Pakistani hacked website is quite low, as in 1000 just seven times Pakistani websites were hacked and in the year 2000 the figure could hardly reach up to 18.

2.5.4 Teenagers - Cyber Delinquent

The stereotypical cyber criminal is running botnets, stealing bank accounts, hacking into major companies to steal trade secrets, and performing other nefarious high-profile crimes that capture the fancy of major news organizations, but the problem is really far more insidious than most people

---

A considerable number of cyber criminals are amateur hackers are teenagers who do not know that what they are doing is an act prohibited by law or is a crime. The reason for this kind of delinquent behavior among children and adolescents are mainly due to curiosity of knowing and craze for grasping new things. Hacking of computers or websites for them is merely an adventurous and courageous task. Mostly children resort to this type of delinquent behaviour pattern because of curiosity to know and explore out things. Also there are some children who try to prove themselves to be outstanding among their classmates or group of friends. Further, even the psychological reasons may be there. Take for example the case of a 16 year old schoolboy who was teased by his classmates for the ugly birthmarks that he was having on his face. This affected his mind so much that he created a website on internet named www.amazing-gents.8m.net on which he uploaded vulgar contents about his classmates. Mostly the vulgar references were related to those classmates of him who use to torment him in relation to his birthmarks. He also fabricated and pasted the obscene pictures of his classmates and teachers on the Internet. This is not just one incident of this kind. Many similar cases of delinquent behaviour have been in news in the recent times. It was in 2002 when a School Principal in Delhi got an email full of threats after he caught some students for a blast in school’s lobby. Thereafter in 2005, again a Delhi student was caught making a website with obscene content on teachers. In 2006, a student was accused of cyber defamation when he circulated some defaming content about the school in an email. Such behaviour of children should not be ignored in fact, as it could get serious in the times to come. If not deterred they could turn themselves into serious cyber criminals.

81 The stereotypical cybercriminal is running botnets, stealing bank accounts, hacking into major companies to steal trade secrets, and performing other nefarious high-profile crimes that capture the fancy of major news organizations, but the problem is really far more insidious than most people realize.
82 Supra Note 76.
83 Supra Note 77, p. 15.
outside India, teenagers are more tech-savvy and thus computer security experts have already started taking them as a big threat.

Teenagers in the foreign countries spent lot more time on computers and they readily exchange phishing kits and cracking tips, crack itself, key-generators, virus codes and other malicious software, in the Internet forums, online chat-rooms and communities. According to Chris Boyd who is director of malware research at Face Time Security, many of the malicious programs are developed by teenagers for the purpose of exploiting the members of social networking sites. However they believe that most of them have inferior hacking skills as compared to the professional cyber criminals. Some even damage their own computers with viruses they write while preparing for launching such cyber attacks. Moreover, very often they can be easily caught as they have quite strong tendency to boast about their skills. Especially to get famous they post videos about their attacks on websites like YouTube. Secondly, they usually sign in with the similar alias which was used by them for hacking a website, cracking software, or running a phishing attack. Therefore, due to these flaws they can be quite easily tracked down by the investigators. Thus, thrill seeking, self-esteem and a desire to be recognized are the main motives what apparently motivate the budding online criminals rather than money itself.

2.5.5 Computer Pirates

Computer piracy is a distinct kind of cyber crime which is perpetuated by many people online who distribute illegal and unauthorized pirated copies of software. Computer pirates are those cyber criminals who violate copyrights of various companies when they copy music, movies, pictures, books and software available on the Internet.

87 Supra Note 84.
There are many P2P (peer-to-peer) file sharing software programs in the market with the help of which they can easily copy and exchange software, movies, music downloads, books etc. on the internet. However, most of this material is copyright protected which implies that one is prohibited from using such stuff as he or she has not purchased it. However, this criminal offence occurs every day on computer systems around the world including the internet. It is quite a serious problem to tackle because almost every internet user has a temptation to get the stuff for free. People online have get so much accustomed to get everything for free they find it awkward to pay for any product. Even disturbing is the fact that most of the users indulged in using pirated products online are not even aware that it is illegal. Crackers cracking the software for individual use are not that big threat. However it is a challenge to tackle those commercial groups who have been selling the pirated software through their websites. As it includes a large chunk of people, it must be considered as a distinct category of cyber criminals.

2.5.6 Malicious Insiders

Charles D’Hericault said, “Lord, defend me from my friends; I can account for my enemies”. This is because sometimes insiders who work for you may prove much more harmful than the outsiders. Most of such insiders are by and large quite reliable and trusted employees who have work associated with computer systems of the company or at least they can easily access those. Some of these might have been punished earlier, but primarily they are first time offenders. Generally such people have good edge in computer technology and with the thorough knowledge of company’s computer security, they take due care to hide their cyber crimes. They could manipulate stored data, destroy company’s confidential records or they could even threat their seniors by sending emails. Hence they operate in various ways.

2.5.7 Greedy Employees

This category includes that set of employees whose major motive is to get
illegal financial gains for themselves or their associates either by some concealed cyber frauds or by extorting from their employer directly or indirectly. Such employees prefer adopt illegal means to increment their salary with large sums of money\textsuperscript{89}. Especially the temporary employees often succumb to the goddess of the quick buck\textsuperscript{90}.

2.5.8 Disgruntled Employees

This category of employees includes those persons who have either been spared by their employers or are reprimanded for their unpleasant behaviour. In consequences, they try to take revenge from their employer and started extensive use of hacking of computer system of their employers to cause them loss or damage in their office or account. With the extensive use of computers and automation processes in cyber age, it is easier for the disgruntled employees to do more harm to their employers by hacking the computer which can bring the entire system down and thus paralyze the employer’s business related activities.

Indeed, this set of employees are those who are either dissatisfied with their employer or who have been sacked by their employer. They usually hack the computer of their employer or post defamatory material about him or her on the web for the sake of avenging. The spitefulness of the displeased employees could sometimes cross limits. Until now, such employees used to adopt methods like going on strike to show protests. However, in cyber world they have changed their strategies. Due to the excessive dependence of companies on computers disgruntled employees think that they could do more harm to their employers by committing computer related crimes\textsuperscript{91}. In 2002, in United States, 3 million dollars of damage was caused by way of a logic bomb to the company’s computer network by a disgruntled computer systems administrator working for JBS Paine.

---

\textsuperscript{89} Supra Note 78, p. 18.  
In a recent case in India, a female ex-employee was found to be accused of sending obscene and threatening emails to superior colleague. She worked for the complainant’s organization for a year. But as she believed that she was ill-treated in the company, for the purposes of avenging she started sending obscene and threatening emails to the complainant posing as a male. A crime was registered against her under section 67 (Publishing of information which is obscene in electronic form) of the Information Technology Act, 2000, read with section 507 (Criminal Intimidation by an anonymous communication) of the Indian Penal Code, 1860 and she was finally traced by the Police.  

2.5.9 **Dejected Lovers**

Dejected Lovers include those disturbed persons in love whose proposals have been turned down by their beloved. This category may also include those ex-lovers who failed to satisfy their desires with their former lover or who feel that they have been betrayed. They resort to harassing behaviour towards victim because they feel that the other person should suffer as much as they have suffered. Often they resort to crime of cyber stalking to disturb their beloved. Besides they may also try to hack their email id’s to know if the person is going around with someone else. They often hack their profiles on social networking sites to defame them. Usually such criminals are not experts and may get caught easily if reported. Recently, a 24 year old computer professional was arrested who started harassing his former lover after she rejected his offer for marriage. For getting her back he hacked her e-mail account and her colleagues’ and started sending pornographic pictures. Police tracked him to his Gurgaon based company.

---


After the arrest he admitted to his crime\textsuperscript{94}. This is not just the one case. There are thousands of similar cases all over the world where such incidents have been happening regularly.

2.5.10 **Sex Maniacs**

Internet is full of online sex maniacs who perform variety of illegal activities like pornography, child pornography, production, possession, distribution or transmission of sexual material, and inducing minors for sex over internet etc. Although some offenders have adopted illegal activities like pornography as their industrial business, sex maniacs do it primarily to satisfy their lust. In fact, these offenders are responsible for corrupting minds of others and further making them sex maniacs too. In Georgia, a forty-year-old car dealer was charged of raping a thirteen-year-old girl whom he fetched as a friend in online chatting sessions\textsuperscript{95}. In other words cyber space provides a safe place to the sex maniacs, where they can follow their targets and can chat and asked to come at a pre-planned place.

A research has been conducted by National Center for Missing & Exploited Children (NCMEC) which gives an outline that how these sex maniacs has been using internet, for the purpose of seducing and exploiting them and how the investigational agencies have responded to such behavior\textsuperscript{96}. Such adults who are sexually attracted to children are known as Pedophiles. Computers and Internet enable pedophiles to locate and interact with other pedophiles more readily than ever before. Chatting in online chat-rooms through instant messengers have been their primary hunting ground to meet, lure and develop sexual relationships with their victims.


2.5.11 Other Cyber Criminals

Beside the main categories of cyber criminals mentioned as above, there are following persons having tendency to indulge in computer crimes to fulfill their variety of individual motives. These are: Competitors in various fields (both indigenous and foreign); Hostile (even friendly) foreign Powers; Cyber Terrorists; Detectives; Mischief mongers; Cheaters or even Psychic persons.

2.6 Cyber Attack

Most Internet users have seen it at some point, if not often. Many have faced more serious threats and in some cases, had their entire lives changed by this problem. Although it sounds like an idea out of an old science fiction book, the issue of cyber-crime is a growing phenomenon that even now threatens the most powerful governments across the world. Cyber-attack could cause present individuals with several important questions. On an individual level, what can be done to prevent a cyber-attack? How can one protect himself, his family, or his business? However, at the national level, the stakes are raised. Some believed that a state-sponsored cyber-attack is an act of war.

Cyber attacks began decades ago. Rudimentary viruses were distributed by random individuals hoping to annoy the technologically inept, middle-aged computer greenhorn, while also using their computer knowledge in a less productive, albeit more fun, way. Cyber-attacks have now become more malicious and much more of a threat. Credit card information, personal records, and sensitive business documents began to be at risk. By 2010, one in every ten American consumers had been a victim of identity theft. Over $50 billion was stolen from individuals and businesses in 2009, and in spite of a rapid expansion of new businesses producing protective software, cyber-attacks have only grown in number. In fact, LifeLock (identity security) CEO Todd Davis offered a

---

challenge to any anonymous hacker to steal his identity. It was successfully accepted 13 times.\footnote{99}{Ibid.}

Cyber attacks just not constraint to the individuals or small businesses but in recent years world has seen some of the largest, most protected corporations around the world attacked. In recent there are more than 8,000 cyber attacks on the Commonwealth Games’ ticketing and scoring systems in India.\footnote{100}{Shivsankar Menon told at the Prem Bhatia Memorial Lecture, New Delhi, “Over 8,000 Cyber Attacks on CWG Ticketing System”, The Hindu, 12 August 2011, Available on http://www.thehindu.com/sci-tech/over-8000-cyber-attacks-on-cwg-ticketing-system-shivshankar-menon/article2350657.ece., Retrieved on 11 March 2015.} Dozens of national governments, including India, have been electronically attacked, allowing the intruder access to sensitive military information, defence secrets, or even embarrassing diplomatic events. Some of these instances have been linked to foreign governments, while others have been carried out by independent people from groups such as Wiki Leaks.

There are significant evidences that several nations are beginning to use this technology against other nations. In the past, websites of the Indian Army, the Prime Minister’s Office, even NIC’s own website had been attacked by hackers. North Korea and Iran, despite sparse evidence that they have advanced capabilities, have openly boasted of their superior ‘cyber-warriors’. Russia, too, has warned of their potential in the cyber-realm, famously using it against Estonia’s government following Estonia’s decision to disassemble a Soviet-era statue in Tallinn. Most notably, China has a massive cyber-force as part of the People’s Liberation Army.\footnote{101}{Supra Note 98.}
Top Nations affected by Cyber Crime, Cyber Crime: Top 20 Countries, Europol, 2010\textsuperscript{102}.

2.7 Causes of Cyber Crime

The following are the main causes of cyber crimes:

2.7.1 Capacity to Store Data in Comparatively Small Space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier\textsuperscript{103}.


\textsuperscript{103} Supra Note 55.
2.7.2 **Complex**

Computers work on very complex operating systems and these operating systems in turn are composed of millions of codes and human mind is fallible and it is possible that there might be a lapse at any stage so the cyber criminals take advantage of these lacunas and penetrate into the computer system.

2.7.3 **Easy to Access**

A mad can have a computer and penetrate others computers having basic knowledge of it. The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system\(^{104}\).

2.7.4 **Loss of Evidence**

In cyber era it is easy to destroy the evidences, especially in case of cyber crime. Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation. The traditionally trained police staff is useless in care of cyber crime cases.

2.7.5 **Motivation**

Intellectual challenge of mastering complex system was the motivation in the past for criminals, but presently criminals are driven by greed, lust, power, revenge, adventure. The desire to inflict loss or damage or revenge is the present

---

motivation for criminals\textsuperscript{105}.

i. Financial Motivation

Money is a major motivator for many cyber criminals; particularly danger of prosecution is less. The perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing, identity theft and fraudulent money request attacks.

ii. Ideological Motivation

The denial of contribution by the companies to the hactivist’s groups also invites the cyber attacks. They anonymous coordinated a series of bot attacks on the companies’ servers, rendering them unreachable to Internet users. These kinds of attacks are conducted for perceived ethical, ideological or moral reasons, damaging or disabling computer equipment and networks to express grievances against individuals, corporations, organizations or even national governments.

2.7.6 Negligence

Negligence is very closely connected with destruction. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

2.7.7 Opportunities

Growth of computing abilities in banking, stock exchange, air traffic control, telephones, electric power, health welfare institution and education, has though brought down the cost leading to revolutionary changes in commerce, communications, entertainment and education, and is providing more criminal

\textsuperscript{105} Supra Note 55. Jivika Govil and Jivesh Govil.
opportunities owing to few vulnerabilities that exist in information technology\textsuperscript{106}.

\subsection*{2.7.8 Poor Response from Law Enforcing Agencies}

Many developing countries lack appropriate law to tackle the cyber crime attackers. Due to this the criminal are far from reach and easily get rid of punishments.

\section*{2.8 Classification of Cyber Crimes}

The complex nature of cyber crimes is understood by various thinkers in varied manner. While all of them recognize the role of computer in the commission of cyber crimes, their categorization differs. Ian Walden gives three categories of cyber crimes as regarding the role of computers. He says,

The computer may constitute the instrument of the crime, such as in murder and fraud; the object of the crime such as the theft of the processor chips; or the subject of the crime such as hacking and distributing viruses\textsuperscript{107}.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{classification.png}
\caption{Classification by Ian Walden}
\end{figure}

Walden refers to some of the offences of English criminal law where there is an involvement of computers. The first category of such crimes is traditional crimes that are committed by using the computer, like fraud, and which are

\textsuperscript{106} Ibid.
referred as computer related crimes. The second category concerns content related crimes which involves intellectual property and pornography. The third category is offences that have been established specifically to address activities that attack the integrity of computer and communication systems referred to as computer integrity offences. These are the typical high-tech crimes. Another thinker, D. S. Wall in 1998 recognized three categories of computer related crimes. In the first category, he identifies that computer networks have become a communication vehicle that facilitate “existing harmful activities”, or in the other words, it facilitates “traditional criminal activities”, “every crime have the migrated or have been re-engineered to function online.”

As Wall says, the internet has allowed for the creation of a new environment within which novel forms of misbehaviour are engineered. The examples of the third category are unlawful appropriation of intellectual property

108 Some other writers have categorized cybercrimes on more or less the same lines. Cybercrimes can be divided into three general categories:
Firstly, crimes where computer is the target. For instance, when a private or official computer system is attacked by intruding into it through Internet either manually or by other means, like use of software. This activity, generally called hacking, may involve erasing of data programme, defilement of website, stealing of data, identity theft and denial of service attack or terrorist activity threatening the critical infrastructure.
Secondly, crimes where computer is a tool of the crime. This is done when computer is used to commit traditional crime in high tech way. Fraud, embezzlement, forgery, blackmailing, sedition, promoting enmity between different classes and defamation may be committed in digital environment. Other crimes committed on the internet include creation and distribution of obscene and pornographic material on the internet, theft of intellectual digital property, stalking, gambling, and money laundering. Besides these, there are numerous other undesirable activities involving the internet.
Thirdly, there is a category of crimes where computer is incidental. It relates to situation where a computer is needed for the criminal activity but is used but in some way connected to the crime. Examples include, personal and financial records of a person involved in economic and financial crimes, notes maintenance by a drug trafficker or person belonging to a terrorist groups, etc. Information on computer is often locked with a password. Here, use of computer by a criminal is incidental. Information contained in the computer is of high evidentiary value in any prosecution for the crime.

M. Zakaria Siddiqui, “Cyber Crimes : The Indian Response” paper presented at the 26th All India Criminology Conference held during 26, 27 and 28 December 2002, University of Madras, Chennai.


110 A typical example might be the use of the internet by pedophiles, which have used the anonymity that is granted to every Internet user to ‘groom’ children in unregulated chat rooms, and to maintain and build networks where illegal images and even victims are exchanged.
such as images, softwares, music and video products. Within this category, even cases of “virtual violence” are also included where the online community members are harassed and verbally attacked by other internet users. Even cases of “virtual rape” have been reported\(^{111}\). Such types of crimes are posing the greatest challenge to the legal systems. However in 2001, D.S. Wall\(^ {112}\) has added four more categories which are helpful in understanding the deviant cyber activity: cyber trespass, cyber-obscenity, cyber-theft and cyber violence, etc.

---

**Figure-2.3: Classification by D.S. Wall**

![Classification by D.S. Wall](image)

Due to the ever-increasing amounts of jargon, a brief description of some of the major forms of cyber crime may help facilitate the theoretical discussion.

---


2.8.1 Unauthorized Access to Computer Programs and Files

Unauthorized access is the main tool used by cyber criminals. Unauthorized access occurs whenever an actor achieves entry into a target’s files or programs without permission. The actor may be a person or another computer, and the access may be achieved electronically (through passwords and other mechanisms) or physically (by, for example, breaking into a file cabinet and stealing a personal identification number (PIN). Electronic access is by far the more common threat, and it is perpetrated by those who steal passwords, use computers to generate random passwords until entry is accomplished, or use ‘trap doors’ to enter a secure area\(^\text{113}\). A trap door is a fast way into a computer program that allows program developers to bypass security protocols built into the program. Programmers and software manufacturers place trap doors in programs so that they can quickly modify the underlying code. But these doors also permit anyone with a modest level of computer sophistication to break into a computer and run it in any way he or she sees fit. For example, a ubiquitous computer platform in the late 1980s-UNIX-contained a trap door that allowed anyone to break into mainframe computer systems and run them from a remote location. East German agents penetrated the University of California at Berkeley’s computers in one such attack\(^\text{114}\). The crime of unauthorized access is one of simply invading another’s workspace.

There are several different targets for unauthorized access; broadly speaking, they may be categorized as the government, individuals, or commercial entities. The government has vast information on its computers, ranging from nuclear secrets to Defence planning contingencies and from human intelligence to law enforcement information about criminal organizations. Unauthorized access

\(^\text{113}\) Passwords are commonly stolen through the use of “sniffer” programs. These programs monitor a user’s keystrokes, and transmit the information back to the host computer that initiated the sniffer program. The electronic thief then has a full transcript of the passwords necessary to achieve entry into a system. In 1994 as many as 100,000 sites were affected by sniffer attacks. David Icove, et. al., Computer Crime: A Crime Fighter’s Handbook, p. 51, O’Reilly Media, Sebastopol, USA, 1995.

to such material can pose severe security risks. By contrast, unauthorized access to an individual’s personal files presents a different set of harms. These harms are generally harms to privacy, as personal files contain private and intimate thoughts. In any event, the computer thief gains access to that information without permission. Commercial access, by contrast, may place at risk a company’s proprietary information and trade secrets. There also may be individual privacy interests at stake (such as personnel files), but the interests here will largely be financial ones. Additional targets may include hospitals and research institutions with important data.\textsuperscript{115}

If a criminal uses the fruits of an unauthorized access, the results may be devastating. Military secrets could be turned over to terrorist rogue states; people’s most private thoughts could be placed on the internet for all to see; a company’s most cherished secrets—the formula for Coca-cola and the like—could be given to rival firms;\textsuperscript{116} and assets may be shaved off for profit. Although these are four separate types of activity, each shares the common nucleus of unauthorized access combined with distribution of the information to others. Following are the common techniques used for unauthorized access.

\subsection*{2.8.2 Buffer Overflow}

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.\textsuperscript{117} In buffer overflow attacks, the extra data may contain codes designed to trigger

---

\textsuperscript{115} Laura DiDio, “A Menace to Society”, \textit{Network World}, pp. 71&84, 6 February 1989, (describing how a computer virus attacked a large hospital and destroyed more than forty percent of its patient records); Christopher Elliott, “Experts To Classify Computer Viruses”, \textit{Sunday Telegraph}, p. 2, London, 10 March 1991, (noting that an Italian university lost one year of AIDS research data due to a computer virus).

\textsuperscript{116} Alternatively, the perpetrators of the theft could blackmail the victim for return of the information. In January 2000, “a group of intruders based in the United Kingdom broke into the computer systems of at least 12 multinational companies and stole confidential files. The group issued ransom demands of up to 10 million [British pounds] in exchange for the return of the files.” Supra Note 61. (Statement of Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University) 2000 WL 11068413.

specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user’s file, change data, or disclose confidential information\(^{118}\). As the excess data “overflows” into other areas of the computer’s memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer\(^{119}\).

### 2.8.3 Packet Sniffing

Packet sniffing is the act of capturing packets of data flowing across a computer network. The software or device used to do this is called a packet sniffer. Packet sniffing is to computer networks what wire tapping is to a telephone network\(^{120}\). Packet sniffing has legitimate uses to monitor network performance or troubleshoot problems with network communications. A packet sniffing is difficult to detect, but it can be done. But the difficulty of the solution means that in practice, it is rarely done\(^{121}\).

### 2.8.4 Port Scanner

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it\(^{122}\). With this advantage of port scan it can be used by hackers to determine which ports are open or in use on a system or network. By using various tools a hacker can send data to TCP or UDP ports one at a time. Based on the response received the port scan utility can determine if that port is in

---


\(^{119}\) Jivika Govil and Jivesh Govil.


use. Using this information the hacker can then focus their attack on the ports that are open and try to exploit any weaknesses to gain access.\footnote{Jivika Govil and Jivesh Govil.}

2.8.5 Password Cracking

All systems cache passwords in memory during login session. Therefore, if a hacker can gain access to all memory on the system, he can likely sift the memory for passwords. Likewise, hackers can frequently sift page files for passwords. To crack a password means to decrypt a password, or to bypass a protection scheme. Another form of password cracking attack is all possible combinations of letters, numbers and symbols are tried out one by one, till the password is found out.\footnote{Dr. Fred Cohen in his doctoral thesis on electrical engineering presented to the University of Southern California in 1986 defined ‘computer virus’ as a program that can infect to other programs by modifying them to include replicate version of itself.}

2.8.6 Unauthorized Disruption

Unauthorized disruption is the heart of what most people consider cyber crime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. By now, the lingo is familiar - viruses, worms, logic bombs, Trojan horses, and denial-of-service attacks.\footnote{Supra Note 5, p. 6.}

2.8.7 Virus

Virus or Vital Information Resource Under Siege is basically a program written for destructive purpose. The term ‘computer virus’ was used for the first time by Dr. Fred Cohen in his thesis published in 1986 wherein he referred to viruses that propagate by attaching themselves directly to the computer programs. These viruses are widespread today as a real danger to most computers and, therefore, the computer users are expected to have basic knowledge of the

\footnote{“Net Security”, Available on http://netsecurity.about.com/cs/generalsecurity/def_portscan.htm.}
working of the viruses in order to save their computer against viral infections.\textsuperscript{127}

A virus may temporarily intercept the computer service to display a message on the screen, or it may bring down the infected computer system. Thus, it may be disruptive or destructive. Most viruses need some kind of activation mechanism to set them off. They may remain dormant and undetected for long periods of time.\textsuperscript{128} It often lurks in the computer memory, waiting to infect the next program that is activated or next disk that is accessed.\textsuperscript{129}

A computer virus is a software program that can copy itself. The construction of viruses, worms, logic bombs and Trojan horses, all of which can attack, damage or disarm a computer system or network can be done by anyone having basic knowledge of programming.\textsuperscript{131} A virus is a program that modifies other computer programs. The modifications ensure that the infected program replicates the virus.\textsuperscript{132} In other words, the original program (the analogue to a healthy cell) is changed by the virus so that the virus can multiply. Once infected, the program secretly requests the computer’s operating system to add a copy of the virus code to the target program.\textsuperscript{133} Once that computer is connected to another computer, either through the internet, direct computer connection, or even through a common floppy disk, the virus may spread beyond the original host computer. A virus is not inherently harmful—its harmfulness will depend on the additional codes placed into the virus besides the code for self-replication. Some viruses, however, have caused enormous damage.\textsuperscript{134} A computer virus acts in a

\textsuperscript{130} Winn Schwartau, Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder Mouth Press, New York. See also Jonathan Matusitz & Gerald-Mark Breen, Cyberterrorism: A Description from Multiple Perspectives, University of Central Florida at Seminole State College, Partnership Center, 100 Weldon Bldv., Sanford.
\textsuperscript{131} Supra Note 49.
\textsuperscript{132} Supra Note 5. (Neal Katyal) p. 1014.
\textsuperscript{133} Peter J. Denning, Computers under Attack, in the Chapter of Computer Viruses, pp. 286-87, 1990.
\textsuperscript{134} A recent example is the Melissa virus, which became famous in March 1999. Melissa infected its first victim when a reader of the pornographic alt.sex newsgroup caught it. Jim Conley,
way that resembles a biological virus: it proliferates by putting itself into living cells. Not all viruses that target our computer systems are harmful; some are in fact innocuous. Sadly, though, we rarely see those. Viruses have been classified into (1). File infectors, (2). Boot-sector viruses, (3). Macro viruses (4). Parasitic viruses, (5). Hostile applets and (6). File system viruses as per their working methods and effects.

**Figure-2.4: Kinds of Virus**

---

“Germ Warfare”, Ziff Davis Smart Bus. for New Econ., pp. 62, 65, 1 June 2000. Within days of this initial contact, Melissa infected more than one hundred Fortune 1000 companies. The virus operated by e-mailing a list of eighty pornographic web sites to fifty e-mail addresses in the electronic address book of the infected system. The fifty recipients received e-mails with the subject line “Important Message From...” and the virus automatically filled in the initial user’s name-so that it appeared that the recipient was receiving a message from his or her friend, rather than from the Melissa culprit. Rose Simmons, “Computer Users Fell Hard for the Love Bug”, p. 23, Asbury Park Press, 12 May 2000. The e-mail systems of the fifty recipient computers then were infected, and each passed the virus to fifty additional addresses. Id. When this process was repeated over and over, the number of affected computers increased dramatically. As a result, the virus caused many millions of dollars in damage to computers worldwide; in the United States alone, the virus affected 1.2 million computers in one-fifth of the country’s largest businesses; David Smith pleaded guilty last December to state and federal charges associated with his creation of the Melissa virus. John Snell, “Think You’ve Computer Viruses? Hold onto Your Mouse”, Star Tribune (Minneapolis), 3 April 2000, at 2E (“For all the trouble Smith now finds himself in, there is no shortage of virus writers waiting to follow the trail he blazed.”).

2.8.8 Worms

Historically, the term ‘worm’ was used for the first time by John Brunner in his book on science fiction entitled ‘The Shockwave Rider’. In his book Brunner described a totalitarian form of government, which kept control over their citizens by the use of a powerful computer network. A worm is a type of virus that slowly moves around from computer to computer and, then, slows things down. A worm tends to eat through and at resources and does not attach itself to other programs. Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. The infamous ILOVEYOU bug shared elements of both viruses and worms. It resembled a virus because it bred on a host computer’s hard drive, but was a worm because it reproduced without any additional human input over a network. More than one million computers in North America alone received a copy of the bug, and it spread nine times faster than the Melissa virus. Most companies, including AT&T Corp., Ford Motor Co., and Merrill Lynch & Co., shut down their e-mail systems to prevent a spread of the attack, resulting in lost time and productivity. Government agencies were also affected, including the Pentagon, the CIA, NASA, the Swiss Government, Danish

136 Supra Note 130.
137 Supra Note 135.
138 The ILOVEYOU bug was spread primarily through e-mail, but was also transmitted through internet chat and company intranet systems. Here is how most users were infected. First, a user would open an e-mail, entitled “ILOVEYOU,” and its attachment, entitled “LOVE-LETTER-FOR-YOU.TXT.vbs.” Then the bug installed itself in the computer’s system. Once the machine was restarted, the bug spread by mailing itself to everyone in the user’s e-mail address book, using the popular Microsoft Outlook Express. The bug then overwrote certain files with extensions such as jpg, jpeg, mp3, and .mp2, deleting them and leaving infected copies of the files in the computer. The bug also used the Internet Explorer home page to download a program that stole passwords and mailed them to e-mail addresses in the Philippines. Finally, the bug changed the default home page to one of the four Web pages hosted by skyinet.net, a Philippine Internet Service Provider. The perpetrators were discovered because one of them, Onel A. de Guzman, had proposed a thesis to a professor exploring the ability to steal computer passwords. The proposal was rejected because of its immorality. This helped link Philippine investigators to de Guzman and another primary suspect, Michael Buen. The duo posted the password-stealing program on the Web using an internet service provider in Manila. That service provider, as well as another provider that Guzman and Buen subsequently hacked into, had caller-identification technology, which allowed technicians to pinpoint the phone number quickly. Foolish mistakes by the suspects led investigators to an apartment owned by de Guzman’s sister. A search of the apartment produced little evidence since the original computers and disks had been removed. “Any Idiot Can Make a Virus”, Straits Times (Singapore), July 12 2000; John Schwartz, “No Love for Computer Bugs”, Washington Post, July 5 2000.
Parliament, and the British House of Commons. Investigators traced the I Love You bug to several computer students in the Philippines, but the case was ultimately dropped because the Philippines had no applicable law against viruses or hacking\textsuperscript{139}. In addition to replication, a worm may be designed to do any number of things such as delete files on a host system or send documents via e-mail.

Worms are of following three types:

i. **Host Computer Worms**

They are contained in the computer they run on and use network connections only to copy themselves to other computers. They are also called as ‘rabbits’ which infect other machines via multiplication. It is so named because of the speed at which it clogs the system with copies of itself, thus reducing system’s performance, before crashing\textsuperscript{140}.

ii. **Network Worms**

These consist of multiple parts called as ‘segments’, each running on different machines and using the network for several communication purposes. Network worms that have one main segment which coordinates the work of the other segments are sometimes called as ‘octopuses’.

iii. **Internet Worm**

The Internet worm of 1988 was world’s famous worm which was developed by Robert J. Morris of the Cornell University on November 22, 1988. It infected nearly 3,000 computers during 8 hours of its activity. It disabled all

\textsuperscript{139} Philippines Drops Charges in “I Love You” Virus Case. Available on http://www.penki.lt/IT-News/Philippines-drops-charges-in-ILOVEYOU-virus-case.im?id= 18752&f=c., Retrieved on 13 March 2015. Another example of a worm was the “Joke” e-mail sent to about 13,000 people in June 2000. This e-mail said it was a joke and when opened, said, “this is funny” or “funny.” When the actual attachment, titled “Life-Stages-.txt.shs” was opened, the worm spread much like the I Love You bug. Another famous example is the Robert Morris case, in which a Corell student launched a worm that ultimately caused major computer havoc. Ted Eisenberg et. al., “The Cornell Commission: On Morris and the Worm”, *Communications of the ACM*, Volume 32 Issue 6., June 1989 Pages 706-709, in *Computers Under Attack*. pp. 253&254, Available on http://dl.acm.org/citation.cfm?id=63526.63530, Retrieved on 12 March 2015.

computers by making copies of itself and thus clogged them. Another famous worm having devastating effect was Christmas Worm, 1987 which managed to paralyze IBM network on the Christmas day in 1987. It asked the users to type ‘Christmas’ on the screen. Then it drew a Christmas tree and sent itself to all the names of people stored in the user file and in this way propagated itself.\textsuperscript{141}

### 2.8.9 Logic Bombs

A logic bomb may be defined as a program, which is designed for operation at some later date or upon the occurrence of specified conditions. It tells a computer to execute a set of instructions at a certain time under certain specified conditions.\textsuperscript{142} Those commands could be benign (a nice message from the programmer each year on her birthday) or damaging (telling the hard disk to erase itself on May Day). A logic bomb can lie undetected in software or hardware, ready to be detonated when a series of events unfolds. Infecting software code with a logic bomb is a powerful way to magnify a crime; so that its effects are far greater than they would be were the crime committed in realspace. The bomb resides in each version of the software, and millions of copies might be sold, all ready to detonate at a certain time. With a logic bomb, instead of just assaulting one computer, an attacker can reach thousands or even millions at once.\textsuperscript{143}

The use of trap door is similar to a logic bomb. It is a secret way back into a system instead of to the software. One can build in circuitry to a chip that performs specific functions.\textsuperscript{144}


\textsuperscript{143} Supra Note 5.

2.8.10 Trojan

The term ‘Trojan’ has its origin from the classical myth of the ‘Trojan Horse’. In the 12th Century B.C., Greece declared a war on the city of Troy. The dispute arose when the Prince of Troy abducted the Queen of Sparta and declared that he wanted to marry her. This naturally angered the Greeks and they besieged Troy for ten years but met with no success as Troy was very well fortified. In the last resort, the Greek Army pretended to be retreating and left behind a huge wooden horse. The people of Troy saw the horse and thinking that it was some kind of present from the Greeks, pulled the horse into their city unaware of the fact that the hollow wooden horse had some of the best Greek soldiers sitting inside it. Under the cover of night, the soldiers snuck out, opened the gates of the city, and later, together with the rest of the Army, killed the entire Army of Troy. Similar to the wooden horse, a Trojan horse program pretends to do one thing while actually doing something completely different 145.

In software field, Trojan means an unauthorized program, which passively gains control over another’s system by representing itself as an authorized program. The most common form of installing a Trojan is through e-mail 146. A Trojan horse is not a virus; yet, a virus might include a Trojan horse 147. A Trojan horse is a software application where users are misled into installing a program that is replete with infected documents. This program is to be downloaded, for instance, through clever e-mails. To make the trick even more realistic, such e-mails sometimes appear to come from friends or colleagues. In other words, a Trojan horse is masqueraded as another legitimate program 148. The goal of the cyberterrorist is to damage the victim’s computer or files 149.

145 Ranbir Singh and G. Singh, Cyberspace and Law - Issues and Challenges, p. 97, NALSAR University Press.
146 Supra Note 41, p. 288.
147 Supra Note 130.
148 Supra Note 135.
Trojans are mainly of following six types:

i. **Remote Administration Trojan (RAT)**
These are the most common Trojans. They let a hacker access the victim’s hard disk and also performs many functions on his computer like shut-down his computer, open and close his CD-ROM drive etc. Modern RATs are very simple to use. They come packaged with two files namely, the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gains full control over his computer.

ii. **Password Trojan**
Password Trojans search the victim’s computer for password and then send them to the attacker or the author of the Trojans. Whether it is an Internet password or an email password, there is a Trojan for every password. These Trojans usually send the information back to the attacker via e-mail.

iii. **Privileges Elevating Trojan**
These Trojans are used to befool the system administrators. They can either be bound into a common system utility or pretend to be something harmless and quite useful and appealing. Once the administrator runs it, the Trojans will give the attacker more privileges on the system.

iv. **Key-loggers**
This type of Trojans is very simple. They log all the victim’s keystrokes on the keyboard including the password and then either save them on a file or e-mail them to the attacker. Key loggers usually do not take much disk space and can masquerade as important utilities, thus making them very difficult to detect.\(^{150}\)

v. **Destructive Trojans**
These Trojans can destroy the victim’s entire hard drive or just scramble important files. Some might seem like joke program, while they are actually ripping every file they encounter to pieces.

---

\(^{150}\) Supra Note 145, p. 99.
vi. Joke Programs

Generally joke-programs are not harmful. They can either pretend to be formulating your hard drive sending all your passwords to some hacker, self-destructing your computer, turning in all information about illegal and pirated software that you might have on your computer. In reality, the programs do not cause any damage. For e.g. Back Orifice (BO), Net Bus 2 Pro, Deep Throat V2 etc.

2.8.11 Distributed Denial of Service (DDOS)

Distributed Denial of Service (DDOS) attack is a technique that overwhelms the web sites and stops them from communicating with other computers. In this attack, hackers and crackers prevent or deny access to a computer or web server for legitimate users. The computer criminals through tools send numerous requests to a targeted internet server (usually the web, file transfer protocol, or mail server). This floods the server’s resources rendering the system unusable. DOS attacks “flood servers with so many incoming messages that the server can do nothing else but try and deal with the flood.”

To carry out a DDOS attack, an individual obtains unauthorized access to a computer system and places software code on it that renders that system a ‘Master’. The individual also breaks into other networks to place code that turns those systems into agents (known as ‘zombies’ or ‘slaves’). Each Master can control multiple agents. In both cases, the network owners become third-party victims, for they are unaware that dangerous tools have been placed on their systems. The Masters are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents. After receiving this information, the agents make repeated requests to connect with the attack’s ultimate target, typically using a fictitious or ‘spoofed’ IP address, so that the recipient of the request cannot learn

---

152 Supra Note 135; Supra Note 130, Jonathan Matusitz & Gerald-Mark Breen, p. 58.
its true source\textsuperscript{153}. Acting in unison, the agents generate a high volume of traffic from several sources. As a result, it loses all or most of its ability to serve legitimate customers—thus the term Distributed Denial of Service\textsuperscript{154}.

2.8.12 Theft of Identity

Identity theft occurs when one’s identity is wrongfully appropriated by another. Some forms of identity theft via computer are familiar. Such types of identity theft via computer, such as cross-site scripting, IP spoofing, and pages jacking, do not have clear realspace analogues. Cross-site scripting occurs when code is placed into a web site to force it to send out information against the will of its owners. With IP spoofing, a perpetrator, using software, impersonates a computer trusted by the victim. As a result, the attacker computer—believed by the victim computer to be a different, friendly computer—achieves entry into sensitive areas or even control of the victim computer by operating privileged protocols\textsuperscript{155}. Page jacking occurs when a link, logo, or other internet address is reprogrammed to bring a customer not to the intended site, but to some other one. For example, if I click on the “Buy.com” logo on the CNN web site, and it brings me not to Buy.com, but rather to an internet gambling web site, the page has been jacked.

2.8.13 Child Pornography

The internet was new and relatively unexplored territory until a few years ago. At first, it was primarily as an educational tool. The electronic revolution has made pornography more accessible, bringing decadent and hard-to-get images into the home. The expansion of computer databases on the internet has provided the greatest access till date to sexually explicit images accessed by both adults and children. Whereas a piece of child pornography once might have only reached a

\textsuperscript{153} Supra Note 5.

\textsuperscript{154} Michael Vatis, Cyber Attacks: Protecting America’s Security against Digital Threats.” ESDP Discussion Paper ESDP-2002-04, John F. Kennedy School of Government, Harvard University, June 2002. (commenting that “while attack tools for DDOS attacks have become more sophisticated, they have also become easier to use”). See Ibid. Neal Katyal also.

\textsuperscript{155} Cross, Cyberthreats, (describing how “cross-site scripting” can fool web browsers into running malicious code even on trustworthy sites).
few thousand people who bought a magazine, with the internet it can reach millions very quickly\textsuperscript{156}.

Pornography has been defined in the Oxford dictionary as “The explicit description or exhibition of sexual subjects or activity in literature, painting, film, etc. in a manner intended to stimulate erotic rather than esthetic feelings; literature etc. containing this”\textsuperscript{157}. Research has established that online pornography plays an accessory role in negative social issues such as child abuse, violence against women, rape, relationship and family breakdown, youth crime, promiscuity and sexually transmitted disease. The child pornographer in realspace is constrained by all kinds of production costs (film, printing, distribution), but these constraints do not pose the same difficulty to the pornographer in cyber space. Ease of distribution is a standard feature of cyber crime\textsuperscript{158}.

Child pornography also underscores the international aspect of cyber space, which permits transactions to occur when the buyer and seller are thousands of miles apart. Childpornographers may seek haven in countries that have no laws against child pornography or no laws against the extraterritorial distribution of such material. Through computers, the way in which child pornography is produced may be altered as well. Obviating the need to find live children, producers may use their computers to draw such images from scratch or may digitally alter photographs of clothed children so that they appear nude.

2.8.14 Copyright

Cyber space has transformed intellectual property theft. This is not the world of fiction. You would have to buy a legitimate copy, buy expensive recording equipment to copy the album to tape or audiocassette, and also reproduce the album cover and other accompanying material. The whole process would be enormously difficult. Analog degradation, high copying costs, and the


\textsuperscript{158} Supra Note 5, p. 1028.
risk that your co-conspirators will be flipped are hallmarks of the offline distribution scheme. But not in the computer age. Even copies of copies are now almost perfect. Copying costs are nil, one can simply download the album once at the computer and post the material once on the internet. Within minutes, this album could be distributed across the planet. The owner of the album would not need to bother with wholesalers, retailers, and the like; this would be self-made, with no one to extract extra costs or finger the owner down the road. The identity of the owner cannot be traced ever even by the law enforcement agencies.\textsuperscript{159}

\textbf{2.8.15 Zombie}

Sometimes called ‘bot’ or ‘robot’ a zombie is a system that has been taken over using Remote Control Software. In many cases, a zombie is used to send spam or to attack remote servers with an overwhelming amount of traffic. It also enables the cyber terrorist to have easy access to the intruded computer, to launch attacks from that computer, to delve into password-protected chat rooms, and get into the storage for the invader’s files.\textsuperscript{160} A zombie, however, is more likely to be discovered and cleaned out if stored in professionally run Web sites.\textsuperscript{161}

\textbf{2.8.16 Vampire}

A worm or a virus of which the sole purpose is to run so profusely that the infected computer cannot do anything else. To be more precise, after the vampire starts running, it begins to replicate itself, to such an extent that the victim’s server is so active running hundreds of copies of the vampire that it can do nothing else.\textsuperscript{162} As one can imagine, vampires pose a threat to Internet software and, when activated, they constitute a chance for the cyber terrorists to strike.

\textsuperscript{159} Information, once unleashed on the internet, has the characteristics of a public good in that it is tremendously non excludable and non rivalrous. But as America has recognized since its founding, intellectual property rights must be preserved in order to provide incentives to create new works.

\textsuperscript{160} Supra Note 135.

\textsuperscript{161} Supra Note 135.

\textsuperscript{162} Ibid.; Supra Note 130, Jonathan Matusitz & Gerald-Mark Breen, p. 58.
2.8.17 **Machines and Microbes**

Machines and microbes are tiny machines, like a small insect, that ‘eat’ electronic circuits, oil, plastics, etc. if unleashed on a computer centre, the result would be total shut down.

2.8.18 **Electronic Jamming, HERF Guns, and EM bombs**

These are the all forms electronic signal jamming. One can jam communications, stopping computer information flow; shoot radio signals at an electronic target to shut it down with High Energy Radio Frequency (HERF) gun; or send out a high powered electromagnetic pulse, an EMP bomb.

2.8.19 **Hitch-Hiking**

This is a group of people, a subsection of hackers, which merely sit on the net and wait. They wait for any information and interesting code to go by and then hitch a ride with it, they follow and delete it, or they simply copy and steal it.

2.8.20 **Cyberstalking**

Stalking is a legal term that has different definition in different states. What these legal terms generally boil down to is that stalking is a deliberate course of action that causes another person to be afraid. In general terms, cyberstalking occurs when someone is threatened or harassed online. Stalking is nothing new, but cyberstalking has some new features e.g. which is easier to commit against crimes against their victims. In recent years, stalkers have found internet, a new medium, which is easier to commit crimes against their victims. The perceived anonymity of the internet makes it safe vehicle through which stalkers can terrorize, harass and threaten the victims or even individuals whom he have never met before offline. An anonymous stalker is harder to catch. Because the perpetrator does not see the harm his actions inflict, the victim’s reaction

---

163 Supra Note 151, p. 155.
cannot cause a change of heart\textsuperscript{164}. Though stalking is not a violent crime, yet it may escalate to serious form of crime because the lack of an in-person confrontation also makes intent harder to presume or ascertain.

Cyberstalkers targets their victims through chat rooms, message boards, discussion forums and e-mails. Cyberstalking takes many forms such as: threatening or obscene e-mail; spamming (in which a stalker sends a victim a multitude of junk e-mail); live chat harassment called flaming; leaving improper messages on message boards or in guest books; sending electronic viruses; sending unsolicited e-mail; and electronic identity theft. Women form a major part of victims of cyberstalking, who are stalked by men or children who are stalked by adult predators. The cyberstalking victim is usually inexperienced online. Cyberstalking, which is simply an extension of the physical form of stalking, is where the electronic mediums such as the internet is used to pursue, harass or contact another in an unsolicited fashion.

To the extent that the online world shapes tastes that eventually culminate in realspace behavior, the law and internet institutions may need to act. Even if there is no causality between cyberstalking and realspace stalking, the two acts may still be heavily correlated. That is, those who cyberstalk may also be likely to engage in realspace stalking. If evidence in cyber space is easier to gather (for example, the permanent record left by a posting may be easier for law enforcement to obtain than the footsteps heard by a victim in the dark one night), the law might criminalize cyberstalking for two reasons, regardless of whether cyberstalking is itself harmful\textsuperscript{165}. First, cyberstalking investigations could provide evidence that would constitute probable cause to search an apartment for evidence of realspace stalking. Second, cyberstalking investigations could allow police to alert a cyberstalker that he or she is under suspicion and should curb his or her

\textsuperscript{164} Supra Note 5, p. 1035.
\textsuperscript{165} Ibid. p. 1036.
behavior, particularly in realspace\textsuperscript{166}.

2.8.21 Defacing Web Sites

Defacing Web sites allows attackers to change the appearance of the Web site and to add whatever the message they want to leave. Even though Web site defacement does not result in any financial losses or information breach regarding the specific governmental or private Web site, it can create a great deal of embarrassment for the Web site owner\textsuperscript{167}.

Several high profile organizations, including the Central Intelligence Agency (CIA), the US Department of Justice, the United Kingdom Labor Party, and the New York Times have suffered from such attacks\textsuperscript{168}. The hacker group, ‘Power Through Resistance’, hacked the CIA Web site on September 1996. The group deposited links on the site to various Web sites. To cover embarrassment, the CIA had to announce that ‘No security breach of private files’ occurred\textsuperscript{169}. Another example involves an Israeli teenager named Ehud Tenebaum, who was arrested by Israeli National Police for ‘illegally accessing computers belonging to the Israeli and United States governments’\textsuperscript{170}.

Defacing government web sites, particularly those such as the CIA and Federal Bureau of Investigation (FBI) Web sites could lead people to assume that all of the secret intelligence and other related information have been accessed by attackers, and in the case of cyber terrorism, by terrorists. The impact of such perception could be a very powerful force multiplier especially if it is initiated just before or following a conventional terrorist attack.

\textsuperscript{166} The two points here, about the use of sweeping criminal laws to maximize government search power and to create warning effects, are of general applicability and contradict the standard notion in criminal law that punishment should be calibrated to the harmfulness of an act.

\textsuperscript{167} Supra Note 6, p. 9.

\textsuperscript{168} Ibid. p. 104.


Just few months back in January, 2014 Indian hackers defaced the homepages of more than 100 Pakistani websites, apparently in retaliation for the defacement of more than 2,000 Indian websites by Pakistani hackers on Republic Day. The cyber security experts expected that ‘Indian Cyber Rakshak’ continue to hack the Pakistan’s websites. On Republic Day, Pakistani hackers defaced 2,118 Indian websites, including those of the Central Bank of India and the website of model-turned-actress Poonam Pandey. The Global Cyber Security Response Team (GCSRT) said that this was the retaliatory act of India hackers. Cyber security experts in Bangalore said most of the Indian websites had been defaced by Pakistani hackers going with the handle ‘StrikerRude’, ‘KashmirCyberArmy’, ‘PakCyber Expert’, “Hunter Gujar” and the Operation was named as ‘#OP26jan’\textsuperscript{171}.

\textbf{Figure-2.5: Defacement of Pakistani Websites by Indian Hackers, The Hindu, January 29, 2014.}

\textbf{INDO-PAK CYBER WAR:} The ongoing cyber war between India and Pakistan is the latest in the series of such online battles between the two neighbouring countries. GCSRT sources said the dispute between the two countries over

Kashmir had spilled into cyber space with each country’s hackers repeatedly targeting the other country’s computing database\textsuperscript{172}.

Another example involving Web site defacement was between attackers from India and Pakistan. During bloody fighting between Indian and Pakistani soldiers in Kashmir in 1999, both countries’ computer experts also fought in the cyber world. Pakistan’s experts hacked the Indian Army Web site www.atmyinkashmir.org and left anti-Indian statements about the Kashmir issue. The Indian Government, in turn, cut off all network access to the Web site of the prominent Pakistani newspaper, Dawn\textsuperscript{173}.

\textbf{2.8.22 Cyber Terrorism}

As with the development and innovation, the human tendency also get a new version and they try to find the destructive side of almost all innovations and advancements. Here the same happened in the case of computer and internet technology which enrich our lives by using simple, quick and high-quality devices on one side and the other side these technological developments also enhance the potential of cyberterrorists to create panic in the cyber world. As the world has become more and more reliant on technology and networked systems, not only have legitimate entities benefited from this trend, but also illegal groups, such as terrorists, organized crime groups, and other criminal entities have been using cyber space for their own benefits\textsuperscript{174}.

\textbf{2.9 New Threat - Cyber Terrorism}

Get ready….terrorists are preparing……cyber space based attacks....\textsuperscript{175}.

\textsuperscript{172} Ibid.
\textsuperscript{174} Supra Note 6, Suleyman Ozeren. p. 26.
Cyber terrorism is the use of electronic networks, and computer technology, as a weapon\textsuperscript{176}. Attacks through the Internet need to have a terrorist component in order to be labeled “cyber terrorism”. For the historical purpose, the word ‘cyber terrorism’ was born in the late 1980s when Collin, a senior research fellow at the Institute for Security and Intelligence (ISI) in California,\textsuperscript{177} coined this hot techno-phrase by combining two linguistic elements: cyber space and terrorism.

Today, almost two decades later, cyber terrorism remains difficult to define because this term does not have a plain, widely accepted clear definition. Part of the reason is that there is some controversy in the definition of cyber terrorism itself: the word consists of ‘cyber’- a definition for which most people would agree on - and ‘terrorism’- which, since 1793, has had over two hundred definitions\textsuperscript{178}. ‘Cyber’ is anything related to computers, computerized items (both real and imagined), and/or automated systems (both in terms of hardware and software). On the other hand, one man’s terrorist is another man’s freedom fighter. No wonder why even top scholars in the field of communication and information technology cannot agree on one single definition of cyber terrorism. An e-mail bomb can be an act of pure hacking for some, while it can be an act of cyber terrorism for others.

The word ‘cyber terrorism’ has been described in different ways and from different angles\textsuperscript{179}. Cyber terrorism was defined as hacking or malicious software attacks against target systems, but the meaning of the cyber terrorism is now expanded to criminal actions such as prostitution or child pornography through the Internet. The more alarming cases are that Internet users are addicted to cyber space and follow terrorists unconditionally and thoughtlessly.

\textsuperscript{176} Supra Note 135.
Over a decade ago, in 1998, Ehud Tenenbaum, an eighteen year old Israeli hacker known as the ‘Analyzer’, penetrated the computer systems of the Pentagon, NASA, the Massachusetts Institute of Technology, the Naval Undersea Warfare Center and other highly protected computer systems in the U.S. A U.S. Defence Department official called it “the most organized and systematic attack the Pentagon has seen to date”180. Tenenbaum’s hacking operation was even given a code name, the ‘Solar Sunrise’, by the F.B.I. In 2001, a sixteen year old from Canada, called ‘Mafia Boy’ also managed to pass the information security systems of some of the most sensitive computer infrastructures in the U.S.

Conceptually, cyber terrorism consists of using computer technology to engage in terrorist activity181. Terrorist groups have been using the Internet for various purposes, such as communicating, propagandizing, recruiting and collecting intelligence182. The network of computer-mediated communication is ideal for terrorists as communicators: it is decentralized, it is more difficult to subject it to control or restriction and it allows access to anyone who wishes to use it183. However, the cyber-world can also be used in a different way, not only as an indirect tool for executing an attack, but also as a direct weapon.

One way to use the weapon of cyber space is through cyber attacks on websites. For instance, such attacks have taken place in the India-Pakistan dispute over Kashmir, in the context of the Israeli-Palestinian conflict and against NATO websites during the crises in Kosovo in the early 1990’s184. These attacks still do not constitute “terrorism” in the sense that they do not cause physical harm and do

---

183 Id at 25.
not intend to influence the government, as required by the definition of terrorism in the Financing Convention.

Cyber terrorism is logically sub-categorized under both terrorism and cyber crimes. These categories are either relatively new phenomenon, as with cyber crimes, or phenomena that has taken on new historical significance, as with terrorism. The results being the definitions of these categories continue to be unsettled. Regarding cyber crimes generally, there must be some violation of a criminal code that involves the use of computers or other information systems, usually accomplished through the Internet, but not necessarily. With terrorism, the United States Government offers multiple definitions, and internationally, there is even less clarity on a definition of terrorism. Terrorist groups have been using the Internet for various purposes, such as communicating, propagandaizing, recruiting and collecting intelligence. The network of computer-mediated communication is ideal for terrorists as communicators: it is decentralized, it is more difficult to subject it to control or restriction and it allows access to anyone who wishes to use it. However, the cyber-world can also be used in a different way, not only as an indirect tool for executing an attack, but also as a direct weapon.

The other way of using cyber space as a weapon is the case of cyber terrorism. Cyber terrorism is the use of computer networks in order to harm human life or to sabotage critical national infrastructure in a way that may cause harm to human life. Joel Trachtman distinguishes between different types of

185 Bruce Hoffman, *Inside Terrorism*, 2nd ed., Colum. U. Press 2006) (evaluating the historical development of terrorism and why it is so difficult to define)
187 Nicholas J. Perry, “The Numerous Federal Definitions of Terrorism: The Problem of too Many Grails”, 30 J. Legis. 249 (2004) (Examining twenty-two of the definitions for terrorism in federal lexicon and arguing for a single definition); United States v. Yousef, 327 F.3d 56, 106 (2d. Cir. 2003) (“We regretfully are no closer now than eighteen years ago to an international consensus on the definition of terrorism, or even its proscription.”).
188 Supra Note 182.
189 Id at 25.
190 This is according to Shlomo Harnoy, Founder, senior VP & Professional manager at SDEMA Group, and Yossi or, VP Information Security at SDEMA Group. The SDEMA Group is an integrated, homeland security solutions partnership specializing in risk mitigation. SDEMA also
networks that may be subjected to cyberterrorist attacks; military and civilian Defence networks; other governmental networks (police, fire); privately or publicly owned networks used to control public utilities and other systems for providing infrastructural services (electricity, water); and public networks used by individual consumers and businesses for communication, education etc…\textsuperscript{191}.

Cyber terrorism may be disrupting bank data, penetrating rail company computers, blocking computer communication at an international airport, deleting the voter register 24 hours before an election, and many more. All these systems are service providers, which mean they are linked to the Internet in one way or another and therefore are under the risk of invasion. Today, Western societies are dependent in almost every aspect of life upon computer communication. Computer systems control nearly everything required for our daily routines and our emergency plans\textsuperscript{192}.

But is cyber terrorism similar in its characteristics to other forms of terrorism mentioned earlier? Surely there must be some difference between hijacking an airplane with a gun and hijacking it by taking control over the airplane’s computer system. Establishing the legal nature of cyber terrorism is crucial in combating it through international legal instruments, which, as was demonstrated above, are central to the international community’s fight against terrorism.

As stated above, terrorism exhibits the elements of physical harm and intention to cause a sense of fear and to influence the decision making process. The cause of physical harm can be attained through disruption of computer...
systems, such as disabling traffic light systems, hospital computers, electric companies’ computer, etc. These acts bring about a sense of fear and uncertainty among the victim population, which in turn leads to pressuring the government to ‘do something’ about it. Thus, you do not need to go through the trouble of getting a gun or a knife onboard an aircraft in order to become a terrorist. You can get the same results sitting in front of a computer screen.

In addition, most of the potential infrastructure targets of cyber terrorism, like those stated above, are protected by some sort of information security and anti-virus programs. Penetrating these programs takes time and knowledge, and it happens solely if the hacker intends for it to happen. Of course not every Ehud Tenenbaum is a terrorist just because he intended to break into classified computer networks. As the above mentioned definition requires, the intention element also means there was intention to influence a government course of action.

Regardless, cyber terrorism has several unique characteristics distinguishing it from other forms of terrorism. We defined terrorism as being aimed at a certain target that has great potential damage in terms of human life. The identity of the humans itself did not matter. Cyber terrorism, on the other hand, can hurt a very specific group of people e.g., governments, big business entities and critical infrastructure of a country which is the backbone of any country in cyber age.

As stated above, cyber terrorism hurts computerized infrastructure, on which advanced societies have come to depend. Thus, different societies are vulnerable to cyber terrorism in different degrees in accordance with their level of dependence on technology and computer networks. The more dependent a state is on electronic communications and information processing networks, the more

---

vulnerable to cyber terrorism it will be\textsuperscript{194}. As Richard Clarke put it already in 1999- ‘If you are connected you are vulnerable’\textsuperscript{195}

One might say that the level of technology advancement also results in better Defence systems, which enable states to protect themselves from these kinds of attacks. Another distinctive feature of cyber terrorism is its relatively low costs and low risk. A terrorist attack in the physical world requires recruiting an executor, equipping him with weapons or explosives and making sure he will pass all security checks on his way to the designated location. Cyber terrorism on the other hand, will most likely save the terrorist these costs and obstacles. Committing a cyber-attack, assuming you know how, does not involve purchasing weapons or actually being present at the attack’s location. All a cyberterrorist needs is a good computer and hacking skills that exceed his opponent’s. In today’s world, anyone has the potential to acquire the required technical skills, as a crash-course “Hacking 101” can be easily be found on the Internet itself.

Despite all the gloomy predictions of a cyber terrorism doomsday, no single instance of real cyber terrorism has yet been recorded. This fact leads people to think that the prophecies on cyber terrorism are exaggerated\textsuperscript{196}. However, there are several arguments that need to be considered. Shlomo Harnoy and Yossi Or, both experts in the field of counter terrorism, have pointed out that a possible reason as to why there have been no cyber-attacks could simply be that terrorist organizations have not yet acquired the technological ability, which is the core factor in cyber terrorism\textsuperscript{197}. Other reasons are difficult to discern. At least in theory this is a highly effective weapon for terrorists. Assuming that the reason there has, of yet, been no cyber terrorism event is indeed the technological gap between the potential targets and potential terrorist, this calls for immediate action. Technological gaps can be closed, rapidly. Since the most critical

\textsuperscript{194} Supra Note 182, p. 148; See Joel P. Trachtman, Supra Note 191, p. 5.
\textsuperscript{196} Supra Note 182, p. 149.
\textsuperscript{197} See Brenner & Goodman, Supra Note 193, pp. 44-52.
infrastructures in Western societies are networked through computers, the potential threat of cyber terrorism is, at least in theory, alarming\textsuperscript{198}.

Governments in Western countries have been taking cyber terrorism threats very seriously for at least a decade. For instance, the U.S. authorities conducted the first experiment of its kind, designed to check the level of readiness of U.S. computer systems for the next attack. This operation was held in 2002 and was given the symbolic name “Digital Pearl Harbor”. The results were startling. The “Red Team”, which was supposed to try to hack into computer systems and disrupt their functioning, succeeded in nearly all cases\textsuperscript{199}. After this experiment the U.S. government began a campaign of improving readiness for cyber terrorism, both on the technical and legislative level\textsuperscript{200}.

One way to use the weapon of cyber space is through cyber attacks on websites. For instance, such attacks have taken place in the India-Pakistan dispute over Kashmir, in the context of the Israeli-Palestinian conflict and against NATO websites during the crises in Kosovo in the early 1990’s\textsuperscript{201}. These attacks still do not constitute “terrorism” in the sense that they do not cause physical harm and do not intend to influence the government, as required by the definition of terrorism in the Financing Convention.

The other way of using cyber space as a weapon is the case of cyber terrorism. Cyber terrorism is new form of terrorism, which exploits the system we have put in place. Cyber terrorism is the use of computer networks in order to harm human life or to sabotage critical national infrastructure in a way that may cause harm to human life\textsuperscript{202}. Joel Trachtman distinguishes between different types of networks that may be subjected to cyberterrorist attacks: military and civilian

\textsuperscript{198} Supra Note 182, p. 148; See Brenner & Goodman, Supra Note 193.
\textsuperscript{201} Supra Note 184.
\textsuperscript{202} Supra Note 190, Dorothy E. Denning; See Supra also Note 182, p. 148.
Defence networks; other governmental networks (police, fire); privately or publicly owned networks used to control public utilities and other systems for providing infrastructural services (electricity, water); and public networks used by individual consumers and businesses for communication, education etc.\(^{203}\)

Cyber terrorism may be disrupting bank data, penetrating rail company computers, blocking computer communication at an international airport, deleting the voter register 24 hours before an election, and many more. All these systems are service providers, which mean they are linked to the Internet in one way or another and therefore are under the risk of invasion. So the cyber terrorism needs to deal separately and also to understand clearly. Next chapter of my research completely dedicated to the meaning, definition and other aspects related to cyber terrorism.

2.10 Conclusion

So, cyber crime also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cyber crime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government\(^{204}\). Contracts are the vital part of the economic systems of countries where private enterprise is encouraged the e-contracts. It is the reason, which tempting the cyber criminals to access the others account and play with others money illegally.

Most cyber crime is an attack on information about individuals, corporations, or governments. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cyber crime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

\(^{203}\) Supra Note 191.

Cyber space is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cyber criminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cyber crime treaties must be ratified. The purpose of this study is to identify major factors affecting or constructing the major variables: cyber terrorism, vulnerability, comprehensive cooperation, and law and policies.