CYBER TERRORISM
IN THE CONTEXT OF GLOBALIZATION

Paper presented at:

II World Congress on Informatics and Law
Madrid,
Spain
September 2002

Paper presented by:

Rohas Nagpal
President,
Asian School of Cyber Laws
rn@asianlaws.org

ABSTRACT

Computer crime has hit mankind with unbelievable severity. In the past, hackers have taken down national defense systems, taken control of a huge dam, shut down large segments of America's power grid, silenced the command and control system of the US Pacific Command in Honolulu, disrupted troop deployments during the Gulf War etc.

Technology savvy terrorists and organized crime syndicates are using 512-bit encryption and digital steganography to secure their communication channels.

In light of this disturbing scenario, it is prudent to distinguish between cyber crime, a domestic issue that may have international ramifications and cyber terrorism, an international issue that may have domestic ramifications.

While a cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both, cyber terrorism merits a more detailed definition.

The author has proposed the following definition of the term "cyber terrorism":

> **Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.**

This paper first examines the tools and methodologies of cyber terrorism such as viruses, worms, Trojans, denial of service attacks and cryptography. The paper then discusses the proactive and reactive legislative measures undertaken by various countries to counter cyber crime in general and cyber terrorism in particular.

Finally, the paper discusses some of the major incidents of cyber terrorism that have ravaged the real and virtual worlds in the recent past.

1. DEFINING CYBER TERRORISM

Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm.

However, all these pale in the face of the most dreaded threat – that of cyber terrorism. In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA. He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people.

Two cyber terrorist groups—the Unix Security Guards and the World Fantabulous Defacers—made 111 digital attacks on Indian educational and business sites recently. A pro-Islamic cyber-alliance now operates across the Internet against U.S., Israeli, and Indian targets.

In light of this disturbing scenario, it is prudent to distinguish between cyber crime, a domestic issue that may have international ramifications and cyber terrorism, an international issue that may have domestic ramifications.

While a cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both, cyber terrorism merits a more detailed definition.

The author has proposed the following definition of the term "cyber terrorism":

> **Cyber terrorism is the premeditated use[1] of disruptive activities[2], or the threat[3] thereof, in cyber space[4], with the intention[5] to further social, ideological, religious, political or similar objectives, or to intimidate[6] any person[7] in furtherance of such objectives.**

The underlying premise in this definition is that cyber crime and cyber terrorism differ only on the basis of the motive and intention of the perpetrator.

[1] Premeditated use implies use preceded by careful planning, thought and / or deliberation.

[2] Disruptive activities are those that prevent the normal continuance of something.

[3] The threat need not necessarily be directed towards the target of the act of cyber terrorism, but may be directed towards any person in whom the target has an interest.

[4] The term cyber space used here extends to the entire virtual world, i.e. the Internet, stand alone computers, every bit of information stored in storage media - removable, non removable, physical and virtual.

[5] The term intention implies the reason or purpose for which an act is committed, sought to be committed or threatened to be committed.

[6] To intimidate means to put a person in fear and thereby compel him to do or not to do something that he does not desire to do.

[7] The term person used here includes a human being, a corporate entity, a State, or a collection thereof.

2. TOOLS OF TERROR

Cyber terrorists use various tools and methods to unleash their terrorism. Some of the major tools and methodologies are discussed below:

2.1. Hacking

“Hacking” is a generic term for all forms of unauthorised access to a computer or a computer network.

Hacking can manifest itself in many ugly forms including “**cyber murders**”. A British hacker hacked into a Liverpool hospital in 1994 and changed the medical prescriptions for the patients. A nine-year-old patient who was "prescribed" a highly toxic mixture survived only because a nurse decided to re-check his prescription. The hacker’s motive – he wanted to know "what kind of chaos could be caused by penetrating the hospital computer"! Others have not been so lucky. An underworld don who was only injured in a shoot out was killed by an overdose of penicillin after a hacker broke into the hospital computers and altered his prescription.

Hacking is facilitated by many technologies, the major ones being packet sniffing[8], tempest attack[9], password cracking[10] and buffer overflow[11].

[8] When information is sent over computer networks, it gets converted into hex and broken into lots of packets. Each packet is identified by a header, which contains the source, destination, size of packet, total number of packets, serial number of that packet, etc. If a hacker wants to see this information, he uses Packet Sniffing technology that reconverts the data from hex to the original. This technology is like putting the equivalent of a phone tap on a computer. Sniffing can be committed when a packet leaves the source or just before it reaches the destination. For this, the hacker would need to know only the IP Address (the unique number that identifies each computer on a network). A packet sniffer can log all the files coming from a computer. It can also be programmed to give only a certain type of information – e.g. only passwords.

[9] TEMPEST (Transient Electromagnetic Pulse Emanation Standard) technology allows someone not in the vicinity to capture the electromagnetic emissions from a computer and thus view whatever is on the monitor. A properly equipped car can park near the target area and pick up everything shown on the screen. There are some fonts that remove the high-frequency emissions, and thus severely reduce the ability to view the text on the screen from a remote location. This attack can be avoided by shielding computer equipment and cabling.

[10] A password is a type of secret authentication word or phrase used to gain access. Passwords have been used since Roman times. Internal to the computer, passwords have to be checked constantly. So, all computers try to "cache" passwords in memory so that each time a password is needed the user does not need to be asked. If someone hacks into the memory of a computer, he can sift the memory or page files for passwords.
Password crackers are utilities that try to ‘guess’ passwords. One way, the dictionary attack, involves trying out all the words contained in a predefined dictionary of words. Ready-made dictionaries of millions of commonly used passwords can be freely downloaded from the Internet. Another form of password cracking attack is ‘brute force’ attack. In this attack, all possible combinations of letters, numbers and symbols are tried out one by one till the password is found out.

[11] Also known as buffer overrun, input overflow and unchecked buffer overflow, this is probably the simplest way of hacking a computer. It involves input of excessive data into a computer. 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.

2.2. Trojans

In the 12th century BC, Greece declared war on the city of Troy because the prince of Troy abducted the queen of Sparta with a wish to make her his wife. The Greeks besieged Troy for 10 years but met with no success as Troy was very well fortified.

In their last effort, the Greeks pretended to be retreating, leaving behind a huge wooden horse. The people of Troy saw the horse, and, thinking it was a present from the Greeks, pulled the horse into their city, unaware that the hollow wooden horse had the best Greek soldiers inside.

Under the cover of night, the Greek soldiers snuck out, opened the gates of the city, and later, together with the rest of their 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.

Trojans are of various types, the important ones being:

i. Remote Administration Trojans[12]

ii. Password Trojans[13]

iii. Privileges-Elevating Trojans[14]

iv. Key loggers[15]

v. Destructive Trojans[16]

[12] They let a hacker access the victim's hard disk, and also perform many functions on his computer (copy files, shut down his computer, open and close his CD-ROM tray etc.).

[13] Password Trojans search the victim’s computer for passwords and then send them to the attacker or the author of the Trojan. There are Trojans for every kind of password. These Trojans usually send the information back to the attacker via email.

[14] These Trojans are usually used to fool system administrators (the system administrator is considered to be the king of the network as he has the maximum privileges on the network). They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system.

[15] These Trojans log all of the victim’s keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually don't take much disk space and can masquerade as important utilities, thus making them very hard to detect.

[16] These Trojans can destroy the victim’s entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually destroying every file they encounter.

2.3. Computer Viruses

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it.

Viruses are very dangerous; they are spreading faster than they are being stopped, and even the least harmful of viruses could be fatal. For example, a virus that stops a hospital life-support computer could be fatal.

Over the years thousands of viruses have ravaged the information of computer users, the most (in)famous ones being Melissa[17], ExploreZip[18], Chernobyl[19], I Love You virus[20], Pakistani Brain[21], Stoned-Marijuana[22], Cascade[23] and Michelangelo[24].

[17] This virus, when it was first noticed on 26th March 1999 was the fastest spreading virus the world over. The virus by itself was quite harmless. It merely inserted some text into a document at a specified time of the day. What caused the maximum harm was that the virus would send itself to all the email addresses in the victim's address book. This generated enormous volume of traffic making servers all over the world crash.

[18] In its activities it was similar to Melissa, but there was one major difference. ExploreZip, first discovered in June 1999, was not a virus but a Trojan. This means that it was incapable of replicating itself. Thus, the Melissa virus had more far reaching presence. Also, ExploreZip was more active. It not only hijacked Microsoft Outlook but also selected certain files and made their file size zero – reduced their data to nothing. Those files were then of no use to the user and they could not be recovered.

[19] The Chernobyl, or PE CIH, virus activates every year on the 26th of April – on the anniversary of the Chernobyl, Ukraine, nuclear power plant tragedy. The virus wipes out the first megabyte of data from the hard disk of a personal computer thus making the rest of the files of no use. Also, it also deletes the data on the computer's Basic Input-Output System (BIOS) chip so that the computer cannot function till a new chip is fitted or the data on the old one is restored. Fortunately only those BIOSes, which can be changed or updated, face a threat from this virus.

[20] In May 2000, this deadly virus beat the Melissa virus hollow – it became the world's most prevalent virus. It struck one in every five personal computers in the world. Losses incurred due to this virus were pegged at US $ 10 billion. The virus used the addresses in the victim's Microsoft Outlook and e-mailed itself to those addresses. The email, which was sent out, had "ILOVEYOU" in its subject line. The attached file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". People wary of opening email attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".
This virus has a destructive effect. Whereas Melissa merely inserts some text into the affected documents at a particular instant during the day, this virus first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing copies of itself.

[21] This is the first virus known to have spread all over the world.

[22] This virus was originally written in New Zealand and would regularly display a message, which said, "Your PC is stoned. Legalize Marijuana."

[23] This virus is also called "Falling Letters" or "1701". It initially appeared as a Trojan horse in the form of a program designed to turn off the Num-Lock light on the user's keyboard. In fact, what it did was to make the characters on the screen drop in a heap to the bottom of the screen.

[24] This virus is titled after famous Italian Renaissance artist Michelangelo Buonarroti. It gets activated every year on the artist's birthday – 6th March.

2.4. Computer Worms

The term "worm", in relation to computers, was used for the first time by science fiction author John Brunner in his book called "The Shockwave Rider".

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms – host computer worms[25] and network worms[26].

The first computer worm was developed for the assistance of air traffic controllers in 1971.

This "worm" programme would notify air traffic controllers when the controls of a plane moved from one computer to another. In fact, this worm named "creeper" would travel from one computer screen to the other on the network showing the message, "I'm creeper! Catch me if you can!" The difference was that this creeper did not reproduce itself.

The world has seen thousands of worms, the more (in)famous ones being the Internet Worm[27], the SPAN network worm[28] and the Christmas tree Worm[29].

[25] Host computer worms are entirely contained in the computer they are on and use network connections only to copy themselves to other computers. The original terminates itself after launching a copy on another host (so there is only one copy running somewhere on the network at a given moment). They are also called "rabbits".

[26] Network worms consist of multiple parts (called "segments"), each running on different machines (and possibly performing different actions), 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 "octopuses".

[27] On November the 22nd, 1988, Robert Morris, a Cornell University science graduate accidentally released his worm on a very large network in the area. This network was named Arpanet, which later became the Internet. The worm managed to infect approximately three thousand computers during eight hours of activity.
The Internet worm disabled all those machines by making copies of itself and thus clogging them. During repairs, many machines had to be completely taken off the network till all copies of the worm could be totally removed.

[28] On the 16th of October 1989, a worm named WANK infected many computers on a network. This worm, if it found that it had system privileges, would change the system announcement message to "Worms against Nuclear Killers!" The message was graphically shown as the first letters of each word and the last three letters of the last word.

[29] The Christmas tree worm was a combination of a Trojan horse and a chain letter. This mainframe worm managed to paralyze the IBM network on Christmas day 1987. The worm was written in a language called Exec. It asked the user to type the word "Christmas" on the screen. Then it drew a Christmas tree and sent itself to all the names of people stored in the user files "Names" and "Netlog" and in this way propagating itself.

2.5. Email Related Crime

Email has emerged as the world's most preferred form of communication. Like any other form of communication, email is also misused by criminals.

The ease, speed and relative anonymity of email has made it a powerful tool for criminals. Some of the major email related crimes are email spoofing[30], spreading Trojans, viruses and worms; email bombing[31], threatening emails, defamatory emails.

2.6. Denial of Service Attacks

In January 2002, Cloud Nine, a UK based Internet Service Provider (ISP), was forced to shut shop after a week-long Denial of Service attack (DoS) resulted in the complete stoppage of its service.

Denial of Service (DoS) attacks are aimed at denying authorized persons access to a computer or computer network. These attacks may be launched using a single computer or millions of computers across the world. In the latter scenario, the attack is known as a distributed denial of service (DDoS) attack.

The main reason for the vulnerability of computer systems to DoS attacks is the limited nature of computer and network resources, be it bandwidth, processing power, storage capacities or other resources.

DoS attacks pose another challenge, namely timely detection and source identification. These attacks are usually launched from 'innocent' systems[32] that have been compromised by the attackers. All the attacker needs to do to launch a DDoS attack is install a Trojan in many computers, gain control over them and then employ them in sending a lot of requests to the target computer.

DDoS attacks are a very perturbing problem for law enforcement agencies mainly because they are very difficult to trace. In addition, usually these attacks target sensitive systems or networks sometimes even those that are vital to national security. Sometimes, even when the perpetrators can be traced, international extradition laws may prove a hitch in bringing them under the authority of the law.

[30] A spoofed email is one that appears to originate from one source but actually has been sent from another source.

[31] Email bombing refers to sending a large number of emails to the victim causing his email server to crash.

[32] Numerous websites allow the "free" and simple download of Trojans. This feature is especially interesting to amateur hackers who like harassing their friends. What they are left unaware of is that these free Trojans that they download are designed so as to give the creator absolute control over the computer systems of the users of the Trojan and their intended victims. Such computers become innocent pawns in a denial of service attack.

Some of the common modes of DoS attacks are teardrop[33], SYN attack[34], UDP flooding[35], Land attacks[36], Bandwidth Consumption[37], Consumption of Other Resources[38] and Ping of Death[39].

[33] The Teardrop attack exploits the vulnerability present in the reassembling of data packets. Data sent using the TCP/IP protocol is broken into packets at the origin and rejoined at the destination. Presuming that 3000 bytes of data are being sent from X to Y, the transaction could look something like this:

Packet number 1 contains bytes number 0001 through 1000
Packet number 2 contains bytes number 1001 through 2000
Packet number 3 contains bytes number 2001 through 3000

In case of a teardrop attack, the transaction could be something like this:

Packet number 1 contains bytes number 0001 through 1000
Packet number 2 contains bytes number 0801 through 2000
Packet number 3 contains bytes number 1501 through 3000

This kind of repetition of bytes within data packets can cause the recipient system to crash / hang / reboot.

[34] When two computers, say X and Y establish a TCP/IP connection, the initial transaction, known as a three-way handshake, is something like this. (Note: SYN means Synchronization packet while ACK means Acknowledgement packet).

X sends a SYN packet to Y. Y replies with a SYN ACK packet. X then replies with an ACK packet.

Only upon completion of these steps is the TCP/IP connection established.

In a SYN attack, numerous SYN packets, all having bad source IP addresses (e.g. non-existent IP address), are sent to the target machine. The target machine responds to each SYN packet with a SYN ACK packet and waits for the ACK packet. Since the source IP address in all these is bad, the ACK packet never comes. Meanwhile the requests get added to the queue resulting in blockage of resources. A sufficiently large number of such SYN packets can crash / hang / reboot the system.

[35] In this attack, the intruder uses forged UDP packets (UDP or User Datagram Protocol is a protocol for the Internet) to connect the ‘echo’ service on one machine to the ‘chargen’ service on another machine. Chargen (character generator) is a server that “babbles”. When you connect to it, it produces characters in an endless stream. Echo simply echoes back any data that is sent to it. These protocols are normally used for testing purposes. The result is that the two services consume all available network bandwidth between them. The network connectivity for the network may be affected.

[36] A Land attack differs from a SYN attack in that instead of a bad source IP address, the IP address of the target system is used as the source IP address, thus creating an infinite loop.

[37] All the bandwidth available to a network can be consumed if someone generates numerous data packets and directs them to the target network.

[38] Apart from network bandwidth, there are other resources available that, if harmed, may make it difficult and sometimes impossible for the system to operate.

[39] Ping of Death can occur when one machine sends another a very large data packet – the size exceeding 65536 bytes. When the receiving machine receives the packet it is in the form of small data packets. The receiving computer then tries to reassemble the packet. When reassembled, the final packet proves to be excessively large and causes a buffer overflow. This method (although no longer as much in use) can cause anything from system hangs, crashes, or reboots in the victim machine.

2.7. Cryptography

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, steganography[40] etc. by terrorists and members of organized crime cartels.

Notable examples are those of Osama bin Laden[41], Ramsey Yousef[42], Leary[43], the Cali cartel[44], the Dutch underworld[45] and the Italian mafia.

Strong encryption is the criminal's best friend and the policeman's worst enemy. If a criminal were to use 512-bit symmetric encryption, how long would it take to decrypt the information using brute force techniques?

Suppose that every atom in the known universe (there are estimated to be 2^{300} of them) becomes a computer capable of checking 2^{300} keys per second, then it would take 2^{162} millennia to search 1% of the key space of a 512-bit key. The universe is believed to have come into existence less than 2^{24} years ago.

Some of the (in) famous cases of criminals using encryption technologies are:

1. Aum Shinri Kyo (Supreme Truth) Case[46]

[40] Steganography, literally meaning covered writing, involves the hiding of data in another object. It can be used to hide text messages within image and audio files.

[41] The alleged mastermind behind the September 11 attack on the World Trade Center in the USA is believed to use steganography and 512-bit encryption to keep his communication channels secure.

[42] He was behind the bombing the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995

[43] He was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.

[44] This cartel is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

[45] Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops serve as an unmarked police / intelligence vehicles database.

[46] On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more. Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever. It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life! The records of the cult had been stored in encrypted form (using RSA asymmetric algorithm) on computers. The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related plans of the cult to cause mass deaths in Japan and USA.

2. Bolivian terrorists case[47]

3. James Dalton Bell case[48]

4. Kevin Poulson case[49]

[47] In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel. A raid on one of the hideouts of the terrorists yielded information encrypted using symmetric encryption. A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

[48] James Bell had launched a vendetta against the Internal Revenue Service (IRS) of the USA. His activities included intimidating IRS officials, rewarding those who killed selected government employees and contaminating an area outside IRS premises in many states of the USA with Mercaptan (a stink gas). After his arrest, the investigators were able to decrypt PGP encrypted messages that he had received only because he divulged the passphrase to his private key.

[49] Kevin Poulson was a skilled hacker who rigged radio contests and burglarized telephone-switching offices and hacked into the telephone network in order to determine whose phone was being tapped and to install his own phone tapping devices. Poulson had encrypted files documenting everything from the phone tapping he had discovered to the dossiers he had compiled about his enemies. The files had been encrypted several times using the Data Encryption Standard. A US Department of Energy supercomputer took several months to find the key. The result yielded nearly ten thousand pages of evidence.

3. LEGAL ISSUES

3.1. Unauthorised Access

The new law concept of unauthorised access is sometimes compared to the traditional law concept of trespass. However, in most countries, this traditional law concept cannot be stretched to protect information stored in computers.

To fill in this lacuna, several countries have enacted legislations pertaining to unauthorised access of computers. These include Australia[50], Canada[51], Denmark[52], Finland[53], France[54], Germany[55], Greece[56], India[57], Luxembourg[58], the Netherlands[59], Norway[60], Spain[61], Sweden[62], Switzerland[63], the United Kingdom[64] and the United States[65].

Some countries e.g. Belgium, Japan[66] and Austria[67] do not have special criminal law provisions against unauthorised access.

[50] Part VI A of Crimes Act, 1914

[51] Article 342.1 Criminal Code (the slightly wider concept of "interception" is used as against "access")

[52] Section 263 (2) and (3) Penal Code

[53] Chapter 38 Section 8 of the Penal Code (as amended 1990)

[54] Article 462-2 Criminal Code, amended in 1988

[55] Section 202a Penal Code

[56] Article 370 C (2) Criminal Code, as amended in 1988

[57] Section 43 (a) of the Information Technology Act, 2000

[58] Article 509-1 Penal Code, as amended in 1993

[59] Article 138a (1), (2) Criminal Code, amended 1992

[60] Section 145 Penal Code, amended 1987

[61] Article 256 Criminal Code 1995

[62] Section 21 Data Protection Act

[63] Article 143bis Criminal Code

[64] Sections 1, 2 Computer Misuse Act 1990

[65] The Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984, 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as various state laws.

[66] In Japan, unauthorised access is, also after the criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g. as obstruction of business (Article 234-2 Penal Code) or theft of electricity (Article 245, 235 Penal Code).

The laws relating to unauthorised access reflect divergent approaches ranging from provisions that criminalize "mere" access to computer systems[68], to those punishing access only in cases where the accessed data is protected by security measures[69], stored in a protected system[70], where the perpetrator has harmful intentions[71], where information is obtained, modified or damaged[72] or where a minimum damage is caused[73].

Some countries[74] combine several of these approaches with a basic unauthorised access offence and the creation of qualified forms of access carrying more severe sanctions.

Some laws, like those of Singapore[75], Canada[76] and USA[77] criminalize preparatory acts such as "password swapping".

3.2. Computer Espionage

The fact that legal provisions developed for tangible property cannot be easily applied to intangible property is made apparent by an analysis of the applicability of traditional trade secret protection law to electronic records.

Theft of corporeal information (e.g. books, papers etc, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic record are copied quickly, inconspicuously and often via telecommunication facilities. Here the “original” information, so to say, remains in the “possession” of the “owner”.

[67] In Austria, unauthorised access is punishable under special circumstances under the aspects of data protection (Section 49 Data Protection Act) and alteration of data (Section 126a Criminal Code) or at least attempt thereof

[68] Australia, Denmark, England, Greece and the majority of states of the USA

[69] Germany, the Netherlands, Norway

[70] India, Singapore, USA

[71] Canada, France, Israel, New Zealand, Scotland

[72] India and some states of the USA

[73] Spain

[74] E.g., Finland, the Netherlands, India, the United Kingdom

[75] Section 8 of the Computer Misuse Act

[76] Section 342.1 of the Criminal Code

[77] As per USA Title 18 Section 1030 (a) (6) of the United States Code "whoever ... knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorisation". Californian Law penalises one who "knowingly and without permission provides or assists in providing a means of accessing a computer"; see Californian Penal Code Section 502 (c) (6).

The laws of countries like Austria[78], Belgium[79], Germany[80], Greece and Italy[81], do not apply the traditional provisions on theft and embezzlement to the unauthorised "appropriation" of electronic information, as they require that tangible property be taken away with the intention of permanently depriving the victim of it.

In Japan[82], the definition of the intention of unlawful appropriation has been widened, and includes the intent to use property only temporarily; nevertheless, Japanese law still requires the taking of tangible property and cannot be applied if data are accessed via telecommunication facilities e.g. the Internet.

In India[83], the definition of theft mandates that “movable” property be taken out of the possession of a person without his consent. Although this would apply to theft of electronic information stored in tangible media (e.g. hard disks, CD ROMs etc), it would not apply to data accessed via telecommunication facilities.

This problem in applying the general property law to cover electronic data is solved by special provisions of trade secrets law. Legal provisions of Austria[84], Germany[85], Finland[86],

France[87], Italy[88] and Spain[89] protect trade secrets by prohibiting certain acts of obtaining information, either by provisions of the penal code or by penal or civil provisions of acts against unfair competition.[90]

[78] Section 127 Criminal Code

[79] Section 461 Penal Code

[80] Sections 242, 246 Penal Code

[81] Sections 624, 646 Penal Code

[82] Article 235, 252, 253 Penal Code.

[83] Section 378, Indian Penal Code

[84] Sections 11, 12, 19 of the Act Against Unfair Competition and Sections 122-124 Criminal Code

[85] Sections 17, 18, 20 of the Act Against Unfair Competition

[86] Chapter 30 Sections 4-6 of the Penal Code (as amended 1990)

[87] Section 418 Criminal Code

[88] Section 623 Penal Code

[89] Articles 278, 279, 280 Criminal Code 1995.

[90] See, for Austria, Sections 11, 12, 19 of the Act Against Unfair Competition and Sections 122-124 Criminal Code; for Germany, Sections 17, 18, 20 of the Act Against Unfair Competition; for Finland, chapter 30 Sections 4-6 of the Penal Code (as amended 1990); for France, Section 418 Criminal Code; for Italy. Section 623 Penal Code; for Spain, Articles 278, 279, 280 Criminal Code 1995.

Canada, Denmark[91], Germany[92], the Netherlands[93], Sweden[94], the United Kingdom and the United States[95] have strengthened penal and civil trade secret protection laws in recent years.

3.3. Computer Sabotage

Traditional legal provisions for damage to property, vandalism and mischief were developed to protect tangible objects and hence their application to electronic information poses several challenges.

In the criminal codes of Belgium[96] and Canada[97], the mere erasure of information without damaging the physical medium did not fall under the provisions of damage to property, since electronic impulses are not considered to be "corporeal property" and interference with the use of the physical medium is not thought of as "destruction".

However, the law in countries like Austria[98], Denmark[99], Germany[100], Italy[101], Japan[102], Netherlands[103], Norway[104], Spain[105], and Sweden[106], considers the deliberate damage or destruction of information on tapes or discs as damage to property or vandalism.

This approach is based on the premise that the perpetrator either damages or interferes with the function of the physical tape or disc upon which the information is stored.

[91] The qualifications in Section 263 and 264 Penal Code, amended in 1985.

[92] Section 17 of the Act Against Unfair Competition, amended in 1986

[93] Article 138a (2) of the Dutch Criminal Code

[94] Section 21 Data Protection Act, chapter 10 Section 5 Criminal Code, Protection of Trade Secrets Act 1990

[95] The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839)

[96] Sections 528, 559 Penal Code

[97] Sections 428, 430 Criminal Code

[98] Section 125 Penal Code

[99] Section 291 Penal Code

[100] Section 303 Penal Code

[101] Sections 420, 635 Penal Code

[102] Articles 258-261 Penal Code and in addition Articles 233, 234 concerning obstruction of business

[103] Section 350 Criminal Code

[104] Section 291 Penal Code

[105] Articles 547 et seq. of the old Criminal Code

[106] Chapter 12 Section 1 Criminal Code

However problems occur in cases in which data is not recorded on corporeal carriers but is merely transmitted.

In order to clarify the situation, legislation has been enacted in Austria[107], Canada[108], Denmark[109], Germany[110], Finland[111], France[112], India[113], Japan[114], the Netherlands[115], Spain[116], Sweden[117], Switzerland[118], the United Kingdom[119] and the United States[120].

In these countries the statutes use different legislative techniques. Finland has amended the traditional statutes on mischief, vandalism or damage to tangible property.

Japanese law covers all kinds of documents and not only computer-stored data. Austria, Germany, France, India, Japan, the Netherlands, New Zealand, Spain, the United Kingdom specifically protect the integrity of computer-stored data. Some legal systems also include specific qualifications for computer sabotage leading to the obstruction of business or of national security.

Independent statutes, which protect the integrity of computer-stored data, have the advantage that they can include the destruction or erasure of computerised data and their alteration or manipulation (a form of attack which is typical for information but not for tangible property), as well as the interference with the lawful use or access of data.

Such comprehensive statutes can be found in Austria, Canada, Germany, India, Singapore, Luxembourg and France.

[107] Section 126a Penal Code

[108] Section 430(1.1) Criminal Code

[109] Section 193 Penal Code, amended in 1985

[110] Sections 303a and 303b Penal Code

[111] Chapter 35 Sections 1-3, amended 1990, chapter 34 Section 1 para. 2 Penal Code, amended 1995

[112] Articles 462-3 and 462-4 Criminal Code

[113] Section 66 of the Information Technology Act, 2000

[114] Articles 234-2, 258, 259 Penal Code

[115] Articles 350a, 350b Criminal Code

[116] Article 264.2 Criminal Code 1995

[117] Section 21 Data Protection Act

[118] Article 144bis Criminal Code

[119] Section 3 Computer Misuse Act 1990

[120] Section 18 U.S.C. § 1030 (a) (5), as well as various state laws.

The Indian law specifically addresses computer viruses and imposes civil[121] and criminal liabilities[122] for introducing a computer virus[123] or computer contaminant[124] into a computer.

Six US states have laws specifically addressing the virus problem.[125] In most of these states, the law provides for criminal liability for the introduction or insertion of a "computer virus", a "destructive program" or a "computer contaminant". Minnesota and Nebraska have gone a step further by criminalising the act of "distribution without authorisation and with intent to damage or destroy any computer system or software or data".

Italy[126] and the Netherlands[127] have taken a similar approach. Switzerland has an even broader provision and not only the "production of a malicious program" but also giving instructions to create such programs is a crime[128].

3.4. Denial of Service

The laws of some countries, including Australia[129], Canada[130], Germany[131], India[132] and Singapore[133] contain specific clauses relating to denial of service attacks. In other countries, denial of service would come under clauses relating to damage to computers or to data.

[121] Section 43 (c) of the Information Technology Act, 2000 provides for damages up to Rs 1 crore.

[122] Section 66 of the Information Technology Act, 2000 applies if the virus causes any damage.

[123] A "computer virus" has been defined as any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

[124] "Computer contaminant" has been defined as any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network.

[125] The six US states are California, Illinois, Maine, Minnesota, Nebraska, and Texas.

[126] The new Italian law (Section 614 of the Criminal Code, introduced in December 1993) criminalises the introduction, communication or passing on of a data processing program which was the purpose or the effect of damaging a data processing or telecommunication system or its data or programs or of interrupting or altering its operation.

[127] The new Dutch provision covers "any person who intentionally or unlawfully makes available or distributes any data which is meant to do damage by replicating itself in an automated system, however, shall not be an offence to carry out the act ... with the object of limiting damage resulting from such data."

[128] "Anyone, who creates, imports, distributes, promotes, offers, makes available, circulates in any way, or gives instructions to create programs, that he/she knows or has to presume to be used for, (unauthorised deleting, modifying or rendering useless of electronically or similarity stored or transmitted data), will be punished".

[129] Section 76C Crimes Act 1914

[130] Section 430(1.1) Criminal Code

[131] Section 303b Criminal Code

3.5. Offensive Information

The dissemination of racist statements, hate speech, and violence related information via the Internet has raised numerous legal questions. The major issues that need to be examined are in respect of the liability of the author of the material and the additional liability of the network service provider.

A great diversity and variety of provisions can be found when examining provisions on incitement to violence (Canada[134], Germany[135], Switzerland[136]), hatred (Canada[137], Ireland[138], Spain[139]) or racism (Spain[140], Portugal[141], Sweden[142], Switzerland[143]; UK[144]).

Many countries, e.g. Austria[145], Denmark[146], Finland[147], Germany[148], India[149] and Switzerland[150], apply their criminal laws to illegal Internet content, e.g. pornography and hate speech, stored on foreign server.

[132] Section 43(f) Information Technology Act, 2000

[133] Section 7, Computer Misuse Act

[134] Section 318 Criminal Code

[135] Section 111 Criminal Code

[136] Article 135 Criminal Code

[137] Section 319 Criminal Code

[138] Section 2 of the Prohibition of Incitement of Hatred Act 1989

[139] Article 510 Criminal Code

[140] Article 607.2 Criminal Code

[141] Articles 239, 240 Criminal Code

[142] Chapter 16 Section 8 Criminal Code

[143] Article 261 bis Criminal Code

[144] Section 19 Public Order Act 1986

[145] Sections 62, 67 (2) Austrian Criminal Code

[146] Section 9 Danish Criminal Code

[147] Section 10 Finnish Penal Code

[148] Sections 3, 9 German Criminal Code

[149] Section 1(2) and 75 Information Technology Act, 2000

[150] Sections 3 (1), 7 (1) Swiss Criminal Code

In such cases, not only is the place of commission taken into account, but also the place of potential results.

3.6. Cryptography

While some countries impose no control on the use of cryptography[151], others regulate the import and export of cryptography through a licensing regime[152]. In some countries, there are no import controls, but export is controlled[153]. In other countries, import and export of cryptography is restricted[154]. Some countries have laws that empower the Government to order compulsory decryption of information under special circumstances[155].

At the international level the erstwhile COCOM[156] (dissolved in March 1994) and the Wassenaar Arrangement[157] have played an important role in the control of cryptography.

3.7. Laws Specific to Cyber Terrorism

In this context, this paper examines the provisions of the law of the USA, UK and India.

3.7.1 United States of America

Section 814 of The Patriot Act[158] is titled "Deterrence And Prevention Of Cyberterrorism". This section amends section 1030(a)(5) of title 18, United States Code.

[151] Argentina, Singapore, Egypt

[152] Burma (Myanmar), Belgium, China, Hungary, India, Israel, Kazakhstan, Moldova, Pakistan, Poland, Russia, South Korea, Vietnam

[153] Australia, Estonia, Finland, Germany, Greece, Ireland, Italy, Japan, Romania, Switzerland, United Kingdom, United States of America

[154] Belarus, Canada, Czech republic, Denmark, France, Latvia, The Netherlands and New Zealand

[155] Italy, India, Spain

[156] The Coordinating Committee for Multilateral Export Controls (COCOM) was an international organization for the mutual control of the export of strategic products and technical data from member countries to proscribed destinations. The main goal of the COCOM regulations was to prevent cryptography from being exported to "dangerous" countries - usually, the countries thought to maintain friendly ties with terrorist organizations (such as Libya, Iraq, Iran, and North Korea). Exporting to other countries was usually allowed, although States often required a license to be granted.

[157] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is signed by Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, UK, USA, Bulgaria and Ukraine. It controls the export of weapons and dual-use goods (i.e. goods that can be used both for a military and for a civil purpose) like cryptography. The initial provisions were largely the same as old COCOM regulations. The Wassenaar provisions are not directly applicable: each member state has to implement them within national legislation for them to have effect.

The amended section punishes any person who causes unauthorised damage to a protected computer[159] by either:

(i) knowingly causing the transmission of a program, information, code, or command, or
(ii) intentionally and unauthorisedly accessing a protected computer

This section applies only in cases where the conduct of the accused caused[160]—

(i) loss[161] to one or more persons[162] during any 1-year period[163] aggregating at least \$5,000 in value, or
(ii) the actual or potential modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, or
(iii) physical injury to any person, or
(iv) a threat to public health or safety, or
(v) damage[164] affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Section 816 of The Patriot Act is titled “Development and Support of Cyber security Forensic Capabilities”. This section empowers the Attorney General to establish adequate regional computer forensic laboratories and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability to:

(1) provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyber terrorism),

[158] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[159] The term "protected computer" means a computer – (a) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (b) which is used in interstate or foreign commerce or communication;

[160] Or, in the case of an attempted offence, would, if completed, have caused

[161] ‘Loss’ means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service

[162] ‘Person’ means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

[163] For purposes of an investigation, prosecution, or other proceeding brought by the United States only, it includes loss resulting from a related course of conduct affecting 1 or more other protected computers).

[164] ‘Damage’ means any impairment to the integrity or availability of data, a program, a system, or information.

(2) provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer related crime (including cyber terrorism),

(3) assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime,

(4) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multi jurisdictional task forces, and

(5) carry out such other activities as the Attorney General considers appropriate.

3.7.2 United Kingdom

As per The Terrorism Act, 2000[165], the term "terrorism" includes the use or threat of action that is

i. designed seriously to interfere with or seriously to disrupt an electronic system
ii. designed to influence the government or to intimidate the public or a section of the public, and
iii. made for the purpose of advancing a political, religious or ideological cause.

3.7.3 India

Although the term “cyber terrorism” is absent from the terminology of the Indian law, section 69 of the Information Technology Act is a strong legislative measure to counter the use of encryption by terrorists.

This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource[166].

Any person who fails to assist the Government agency in decrypting the information[167] sought to be intercepted is liable for imprisonment up to 7 years.

[165] Section 1 and 2

[166] The reasons for such an order must be recorded in writing. The order can be made on the following grounds: (1) in the interest of the sovereignty or integrity of India (2) in the interest of the security of the State (3) in the interest of friendly relations with foreign States (4) for preserving public order (5) for preventing incitement to the commission of any cognizable offence.

[167] The information referred to in this section would include email messages, password protected files, steganographic images, encrypted information etc.

4. MAJOR CYBER TERRORISM INCIDENTS

Iraqi hackers disrupted troop deployments during the Gulf War.

In 1994, a 16-year-old English boy took down some 100 U.S. defense systems.

In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electrohippies, another group of hacktivists, conducted web sit-ins against the WTO when they met in Seattle in late 1999.

In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA. He was in a position to release flood waters that would have inundated Mesa and Tempe, endangering at least 1 million people.

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the web site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings".

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications". Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

During the Kosovo conflict in 1999, NATO computers were blasted with email bombs and hit with denial of service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

In 2000, the Asian School of Cyber Laws was repeatedly attacked by Distributed Denial of Service attacks by “hactivists” propagating the “right to pornography”. The Asian School of Cyber Laws has spearheaded an international campaign against pornography on the Internet.

In 2001, in the back drop of the downturn in US-China relationships, the Chinese hackers released the Code Red virus into the wild. This virus infected millions of computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

In 2001, hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, dubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures.

In the first six months of 2002 the hacker group GFORCE-Pakistan has conducted more than 150 reported cyber attacks against Indian targets to further its ideas on the Kashmir issue.

In 2002, numerous prominent Indian web sites were defaced. Messages relating to the Kashmir issue were pasted on the home pages of these web sites. The Pakistani Hackerz Club, led by “Doctor Neukar” is believed to be behind this attack.