**CYBER TERRORISM**

*A*

***Project Report***

*submitted*

*in partial fulfilment*

*for the award of the Degree of*

***Masters of Computer Applications***

***in Department of MCA***



**SESSION (2015-2016)**

**Submitted To:**

Mr. Saurabh Maheshwari

(Head, MCA)

**Submitted by**:

Ankita Jain

MCA (VI Sem )

College ID-

**Department of Masters of Computer Applications**

**Govt. Mahila Engineering College, Ajmer**

**Rajasthan Technical University, Kota**

**Candidate’s Declaration**

I hereby declare that the work, which is being presented in the project, entitled **“Cyber Terrorism”** in partial fulfillment for the award of Degree of **“Masters of Computer Applications”** in Department of **Masters of Computer Applications**, Govt. Mahila Engineering College, Ajmer, from Rajasthan Technical University, Kota is a record of my own investigations and experiments carried for this training and project.

I have not submitted the matter presented in this report anywhere else for the award of any other degree.

**Ankita Jain**

MCA

College ID: -

Govt. Mahila Engineering College, Ajmer

**ACKNOWLEDGEMENT**

I feel profound happiness in forwarding this project report as an image of sincere efforts. All who generously helped by sharing their valuable experience and devoting their precious time with me, without whom this seminar report would never been accomplished.

First and foremost I extend my thanks and gratitude to **Mr. Saurabh Maheshwari (Asst. Professor & Head Dept. of MCA), Govt. Mahila Engineering College, Ajmer** my project coordinator whose guidance, teaching and certain suggestion provide me the timely valuable input which enhanced my knowledge and thus helped in development of this seminar report.

**Yours Sincerely**

**ANKITA JAIN**

**TABLE OF CONTENTS**

**CHAPTER NO. TITLE PAGE NO.**

CANDIDATE’S DECLARATION

CERTIFICATE

ACKNOWLEDGEMENT

ABSTRACT

1) **INTRODUCTION 1-3**

1.1 History and Instances2

1.2 Definition of Cyber Terrorism 2

1.3 Computers the weapon of the Cyber Terrorism3

1.4 Objective of Cyber Terrorism 3

1.5 Difference between real world physical 3

Terrorism and cyber terrorism

2) **FORMS OF CYBER TERRORISM**

2.1 Bank Threatening 4

2.2 Personal Information Gain 4

2.3 Gaining Publicity 4

2.4 Data Diddling 4

3)  **STRATIGIES OF CYBER TERRORISM 5-6**

3.1 Unauthorised access and Hacking 5

3.2 Virus Writing 5

3.3 Electronic Snooping 5

3.4 Old Fashioned Human Spying 6

4) **TYPES OF CYBER TERRORISM**

4.1 Information Theft 7

4.2 Electronic Cash 7

4.3 Credit Card No. theft 7

4.4 Hacking 7

5) **CYBER ATTACKS 8-9**

5.1 Physical Access Attack 8

5.1.1 Wire Tapping 8

5.1.2 Vandalism 8

5.2 Penetration Attack 8

5.2.1 Scanning 8

5.2.2 Denial of services 8

5.2.3 Malware 9

5.2.4 Viruses 9

5.2.5 Worms 9

5.3 Dialog Attack

5.3.1 Eaves Dropping 9

5.3.2 Message Alteration Attack 9

6) **CASE STUDY 10-11**

**7) CYBER LAW IN INDIA 12-13**

7.1 Why Cyber Law in India? 12

7.2 What is the importance of Cyber Law? 13

7.3 Cyber Law awareness program 13

8) **COMPARATIVE STUDY OF INDIAN IT ACTS 14-15**

**AND FOREIGN IT ACTS**

9) **WAYS TO PREVENT CYBER TERRORISM 16-18**

9.1 Be aware of mail attachments 16

9.2 Engage Anti-Virus software 16

9.3 Establish Rules 16

9.4 Explain appropriate behavior 16

9.5 Live by example 16

9.6 Monitor 16

9.7 Filter 17

9.8 Look for warning signs 17

9.9 Communicate 17

9.10 Talk to school personnel 17

9.11 Remain vigilant 17

9.12 Contact the police 17

9.13 Develop the strong password 17

9.14 Keep the software update 17

9.15 Maintain the accurate browser settings 17

9.16 Compile strong firewalls 17

10) **CONCLUSION 19**

**REFERENCES 20**

**ABSTRACT**

Cyber terrorism is a new terrorist tactic that makes use of information systems or digital technology, especially the Internet, as either an instrument or a target. As the Internet becomes more a way of life with us, it is becoming easier for its users to become targets of the cyber terrorists. The number of areas in which cyber terrorists could strike is frightening, to say the least.

The difference between the conventional approaches of terrorism and new methods is primarily that it is possible to affect a large multitude of people with minimum resources on the terrorist's side, with no danger to him at all. We also glimpse into the reasons that caused terrorists to look towards the Web, and why the Internet is such an attractive alternative to them.

The growth of Information Technology has led to the development of this dangerous web of terror, for cyber terrorists could wreak maximum havoc within a small time span. Various situations that can be viewed as acts of cyber terrorism have also been covered. Banks are the most likely places to receive threats, but it cannot be said that any establishment is beyond attack. Tips by which we can protect ourselves from cyber terrorism have also been covered which can reduce problems created by the cyber terrorist.

We, as the Information Technology people of tomorrow need to study and understand the weaknesses of existing systems, and figure out ways of ensuring the world's safety from cyber terrorists. A number of issues here are ethical, in the sense that computing technology is now available to the whole world, but if this gift is used wrongly, the consequences could be disastrous. It is important that we understand and mitigate cyber terrorism for the benefit of society, try to curtail its growth, so that we can heal the present, and live the future.

**CHAPTER 1**

**INTRODUCTION**

The world is a very large place, but it is getting smaller, thanks to the advent of computers and Information Technology. However, the progress that we've made in these fields also has a dark side, in that a new terrorist tactic, commonly called Cyber terrorism has developed. The old, conventional methods of assassination and hostage taking are slowly fading, as terrorists head towards the Internet to pull their stunts. The cause for this kind of a transition stems from the fact that the terrorist has long since realized that removing one official from office only causes another official to take his place; which is not the end-result the terrorist wished to achieve. This causes the terrorist to take to the net, thus affecting a wider section than could otherwise have been targeted. From disabling a country's economy to shutting off power in large areas, it's all possible, with less risk to the terrorists.

Cyber terrorism is any act of terrorism that uses information systems or digital technology (computers or computer networks) as either an instrument or a target. Cyber terrorism can either be "international", "domestic" or "political", according to the nature of the act, but it is always an act involving a combination of the terrorist and the computer.

**Why IT is so attractive to the terrorist?**

Terrorist groups have been using computer technology to secure many of their goals. They have been exploiting existing modern technology to accomplish the same goals that they have been working towards in the past. However, the key differences between their old tactics and their newer methods lie in the ease with which their operations can be performed, as well as increased anonymity. It is extremely difficult to detect such clandestine operations, and needless to say, even more difficult to counter such acts. Terrorist groups take advantage of computer technology to create support structures that serve to strengthen their tactical and strategic plans and goals. These are achieved by:

• Political propaganda

• Recruitment

• Financing

• Information and intelligence gathering

• Ease of operations that are cost-effective, both in terms of resources used, and ability to strike worldwide.

Specific examples of the facilitation of terrorism through the use of computer technology illustrate the appeal this technology has for terrorist groups interested in advancing their particular agendas. The use of the Internet for propaganda and disinformation purposes is an especially popular one. Many exiled political opposition groups from such states as Iran, Iraq, Mexico, Northern Ireland and Saudi Arabia have used the World Wide Web for just such purposes.

* 1. **History and Instances**

One of the most demonstrative examples, however, involves the case of the

December, 1996 takeover of the Japanese Ambassador's residence in Lima, Peru by

the Tupac Amaru Revolutionary Movement. Not only did this terrorist group use the

Internet to communicate its revolutionary message to the rest of the world through a

European website, it even offered a video clip of its members preparing for their

Mission.

As a whole, cyber terrorism wasn’t really popular until the end of the millennium. At this particular moment, the big hysteria around the [Millennium bug](http://en.wikipedia.org/wiki/Year_2000_problem) started to kindle peoples’ imagination. There were many apocalyptic scenarios which apparently did not transpire. Nevertheless, the fear of what might happen, either intentionally or by accident, if computers or technology were to go wrong, remained. Then the 9/11 terrorist attacks happened, leading inevitably to a new wave of anxiety with relation to all possible terrorist threats.

Following a more recent series of events, in 2008, the [Stuxnet](http://en.wikipedia.org/wiki/Stuxnet) worm sabotaged an Iranian nuclear plant. The Iranian government cast the blame on the joint efforts of USA and Israel. The latest cyber attacks on [Saudi Aramco](http://en.wikipedia.org/wiki/Saudi_Aramco), [RasGas](http://www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgas-offline-471345.html), and [US banks](http://www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html) are considered as a strike back from the Iranian side.

* 1. **Definition of Cyber Terrorism**

Terrorism conducted in cyber space, where criminals attempt to disrupt computer or telecommunication services. Cyber terrorism: the user of the internet for terrorist purposes.“The convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computer, networks and the information stored there in when done to intimidate or coerce a government”. The cyber terrorism is bloodless war? It is first important to note that no single definition of the term “terrorism” has yet gained universal acceptance. Additionally, no single definition for the term “cyber terrorism” has been universally accepted. Also, labeling a computer attack as “cyber terrorism” is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred.

The National Infrastructure Protection Center (NIPC), now within DHS, defines cyber terrorism as “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.”

“Cyber terrorism can be defined as the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via electronic communication.” National Conference of State Legislature.

* 1. **Computers the Weapons of the Cyber terrorism**

The most likely ‘weapon’ of the cyber terrorist is the computer. Thus, one might ask, are we arguing that one should restrict access to computers, just as access to explosives is restricted? Not quite, but close. We believe that the stockpile of connected computers needs to be protected. There are many laws that define how one should protect a firearm from illegal/dangerous use. The mandatory use of trigger locks, though controversial, has been put forward to prevent danger should the gun end up in the wrong hands. Similarly, powerful explosives like C4 are not simply sold over the counter at the corner store. Explosives and guns are certainly not entirely analogous to computers. A better analogy might stem from the concept of an ‘attractive nuisance’. For example, a homeowner shares some responsibility for injury caused by a pool on his property — it is deemed an attractive nuisance, and as such, the innocent should be prevented from simply being attracted and harmed. Thus, there are many instances of laws which already discuss damage done by/to a third party from the intentional/unintentional misuse of a piece of corporate/personal property. The application of these laws or the definition of ‘misuse’ with respect to computers seems unclear. However, there is a need for clear laws and standards which require operators of large networks of Internet-connected computers .

**1.4 Objective of Cyber Terrorism**

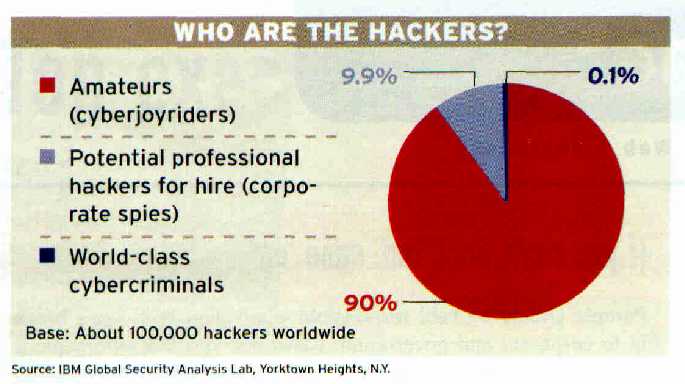
* To be able to determine which unlawful acts are actually considered cyber

Terrorism.

* The United States “susceptibility to cyber terrorism”.

**1.5 Difference between real worlds physical terrorism and cyber terrorism**

* Chances of capture, injury or death to a cyber terrorist are less Cyber terrorism is difficult to track.



**CHAPTER 2**

**FORMS OF CYBER TERRORISM**

**2.1 Bank Threatening**

As you know one of the most popular forms of Cyber terrorism is to threaten a large bank. The terrorists hack into the system and then leave an encrypted message for senior directors, which threaten the bank. What adds to the difficulty to catch the criminals is that the criminals may be in another country. A second difficulty is that most banks would rather pay the money than have the public know how vulnerable they are.

**2.2 Personal Information gain**

Cyber-terrorists often commit acts of terrorism simply for personal gain. Such a group, known as the Chaos Computer Club, was discovered in 1997. They had created an Active X Control for the Internet that can trick the Quicken accounting program into removing money from a user's bank account. This could easily be used to steal money from users all over the world that have the Quicken software installed on their computer. This type of file is only one of thousands of types of viruses that can do everything from simply annoy users, to disable large networks, which can have disastrous, even life and death, results.

**2.3 Gaining Publicity**

Cyber-terrorist are many times interested in gaining publicity in any possible way. For example, information warfare techniques like Trojan horse viruses and network worms are often used to not only do damage to computing resources, but also as a way for the designer of the viruses to "show off." This is a serious ethical issue because many people are affected by these cases. For one, the viruses can consume system resources until networks become useless, costing companies’ lots of time and money. Also, depending on the type of work done on the affected computers, the damage to the beneficiaries of that work could be lethal. Even if the person never meant to harm someone with their virus, it could have unpredictable effects that could have terrible results.

**2.4 Data Diddling**

Minor attacks come in the form of "data diddling", where information in the computer is changed. This may involve changing medical or financial records or stealing of passwords. Hackers may even prevent users who should have access from gaining access to the machine. Ethical issues in this case include things like invasion of privacy and ownership conflicts. It could be even more serious if, for instance, the person who needed access to the machine was trying to save someone's life in a hospital and couldn't access the machine. The patient could die waiting for help because the computer wouldn't allow the necessary access for the doctor to save his or her life.

**CHAPTER 3**

**STRATEGIES OF CYBER TERRORISM**

**3.1 Unauthorized access & Hacking**

One of the criminal activities is unauthorized access that would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction.

**3.2 Virus writing**

A program that has capability to infect other programs and make copies of itself and spread into other programs.

.

**3.3 Electronic Snooping**

As the Internet grows by leaps and bounds, information about nearly anyone is just a few keystrokes away. While it is clearly not a crime to perform an internet search on someone’s name, ask friends and family or e-mail your acquaintances for information, it is surprisingly easy for mere curiosity to cross the line into an unethical or even illegal act. Trying to enter someone’s private e-mail account or breaking into protected updates on social networking sites like Facebook™, MySpace™ or Twitter™ can actually be criminal acts. In some states, these actions can be considered violations of privacy or fall under the purview of anti-stalking laws. Federally, these acts may be considered computer fraud, computer and information theft or cyber terrorism, violations of which can even result in felony charges.

When Does Snooping Cross the Line?

Sometimes businesses or government agencies actually use hacking-type actions for legitimate purposes. So long as these actions are strictly-controlled, for example to gather evidence of civil torts (such as dissemination of trade secrets, libel or defamation of character), criminal actions, or as part of a clearly-publicized school / workplace policy, it is legal to access private e-mails. E-mails can be particularly valuable sources of information given the fact that people are generally less-guarded with their language and more apt to share incriminating information.

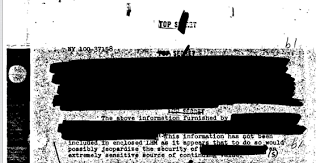
Hacking, defined as breaking through a security barrier without permission to access data, is both unethical and illegal if not used for a legitimate civil or law enforcement purpose. There are several different methods of accessing someone’s e-mail, all of which can be unethical, rude and possibly illegal. Hackers have even posted videos on the Internet describing how to do it! Some computer software programs can be utilized which will run infinite combinations in an attempt to obtain a user’s e-mail password; more common is for an individual to try and guess the password of an acquaintance. Should you be given a person’s e-mail password it is unethical, but probably not illegal, to “snoop” on them by reading it.

It is also possible to gain access to private e-mails or Web pages via interception of information routed across the public Internet. This may or may not be considered a criminal act, since the public Internet is an unsecured forum. Another method of gaining access to seemingly private e-mails or Web pages visited is to just open the pages or programs on a computer where the prior user did not log out. Again, this is inappropriate, unethical and rude, but is probably not illegal; there is no expectation of privacy in the information if it was left for public access.

Using hacking techniques to break into the e-mail or private social networking page of another person (for example an ex-boyfriend or boyfriend, former spouse, adult child or new beau) is just wrong. These actions may seem innocent to you – you may be just trying to gather information or trying to play an innocent prank by resetting a friend’s password. No matter your intent, you may be in violation of state or federal law. It is important to remember that ignorance of the law is no defense — you can still be held liable regardless of whether or not you thought your actions were criminal.

**3.4 Old-fashioned human spying**

While the news debates the NSA's PRISM program, a massive collection of data points of electronic communication, the more human side of spying is being pushed to the background. Yet if you are fearful of privacy invasion, there is nothing more chilling than a reading of FBI files with accounts of informants and statements about "Communist leanings" and "pro-Russian" attitudes. You can get a taste for this in the [FBI Vault](http://vault.fbi.gov/), a public file of de-classified documents, most of which are revealed upon the death of the target. The A-Z list (which appears to be a selection, as other names can be found with searches) is full of famous names, from Al Capone to Al Gore, from George Burns to Marilyn Monroe, and from Helen Keller to Leon Trotsky. (The list is only marginally alphabetical, by first name, which is almost as shocking as the contents of the files.)This is old-fashioned stuff for the most part. Type-written letters, lots of scribbled initials, and whole chunks of documents blacked out with what must be a special FBI-invented marker.

[](http://1.bp.blogspot.com/-R8Un8C0H3_E/UcHiSTMJiGI/AAAAAAAABKM/At4oAt2IBpY/s1600/topSecret.png)

On a more modern note, who could resist adding their favorite FOIA file to face book? Sending malicious codes through email E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

**CHAPTER 4**

**TYPE OF CYBER TERRORISM**

**4.1 Information theft**

Minor attacks come in the form of “data diddling”, where information in the computer is changed This may involve changing medical or financial records or stealing of passwords. Hackers may even prevent users who should have access from gaining access to the machine.

**4.2 Electronic cash**

People now use ATM cards, credit cards and check cards for a large percentage of their punching new types of crime will emerge as accessing these is quite easier.

**4.3 Credit card Number theft**

People are using credit cards for more and more of their purchases as time go on. Credit cards are especially easy to use fraudulently because they require no extra identification number to use.

**4.4 Hacking**

Hacking basically knows programmable systems and now they work, some agencies hire hackers to show them the down falls in their security system so they can improve if against hackers that want information or access into the computer for other reasons. Hacking is a form of art for some people.



**CHAPTER 5**

**CYBER ATTACKS**

**5.1 Physical access attacks**

**5.1.1Wire tapping**

Wiretapping is a particular form of electronic surveillance that gmonitor telegraphic communication .the introduction of such surveillance raised fundamental issues concerning personal privacy.

**5.1.2 Vandalism**

Vandalism is any addition, removal, or change of content in a deliberate attempt to compromise the integrity of Wikipedia. Examples of typical vandalism are adding irrelevant obscenities and crude humor to a page, illegitimately blanking pages, and inserting obvious nonsense into a page.

**5.2 Penetration attack**

A penetration test, occasionally pen test, is a method of evaluating [computer](http://en.wikipedia.org/wiki/Computer_security) and [network security](http://en.wikipedia.org/wiki/Network_security) by simulating an attack on a [computer system](http://en.wikipedia.org/wiki/Computer_system) or [network](http://en.wikipedia.org/wiki/Computer_network) from external and internal threats.

**5.2.1 Scanning**

Once in possession of special restricted information, or a few critical phone numbers, an attacker performs additional surveillance by scanning an Organization’s computer software and network configuration to find possible entry points. This process goes slowly, sometimes lasting months, as the attacker looks for several vulnerable openings into a system.

**5.2.2 Denial of services**

In [computing](http://en.wikipedia.org/wiki/Computing), a denial-of-service attack (DOS attack) or distributed denial-of-service attack (DDOS attack) is an attempt to make a machine or network resource unavailable to its intended [users](http://en.wikipedia.org/wiki/User_%28computing%29).

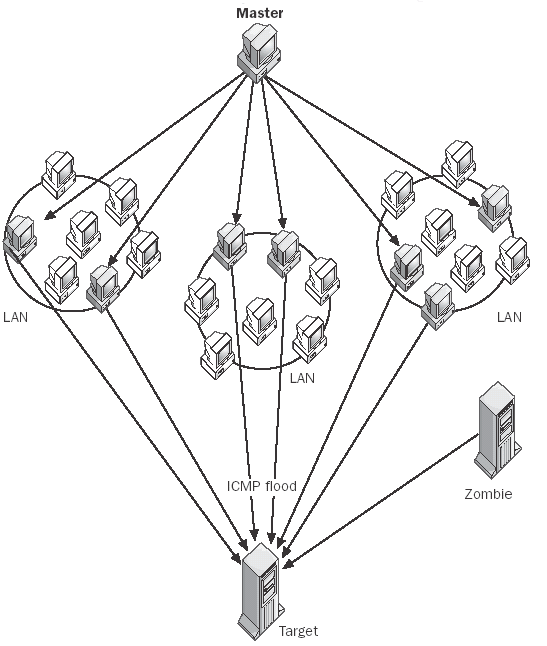


Figure :- 7.2.2 .Distributed denial-of-service attack

Denial-of-service attacks are considered violations of the [Internet Architecture Board](http://en.wikipedia.org/wiki/Internet_Architecture_Board)'s [Internet proper use policy](http://en.wikipedia.org/wiki/Internet_ethics), and also violate the [acceptable use policies](http://en.wikipedia.org/wiki/Acceptable_use_policy) of virtually all [Internet service providers](http://en.wikipedia.org/wiki/Internet_service_provider). They also commonly constitute violations of the laws of individual nations.

**5.2.3 Malware**

Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of [code](http://en.wikipedia.org/wiki/Source_code), [scripts](http://en.wikipedia.org/wiki/Script_%28computing%29), active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes [computer viruses](http://en.wikipedia.org/wiki/Computer_virus), [ransom ware](http://en.wikipedia.org/wiki/Ransomware_%28malware%29), [worms](http://en.wikipedia.org/wiki/Computer_worm), [Trojan horses](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), [root kits](http://en.wikipedia.org/wiki/Rootkit), [key loggers](http://en.wikipedia.org/wiki/Keystroke_logging), [dialers](http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialer), [spyware](http://en.wikipedia.org/wiki/Spyware), [adware](http://en.wikipedia.org/wiki/Adware), malicious [BHOs](http://en.wikipedia.org/wiki/Browser_Helper_Object), [rogue security software](http://en.wikipedia.org/wiki/Rogue_security_software) and other malicious programs; the majority of active malware threats are usually worms or Trojans rather than viruses

**5.2.4 Viruses**

A computer virus is a type of [malware](http://en.wikipedia.org/wiki/Malware) that, when executed, [replicates](http://en.wikipedia.org/wiki/Self-replicating_program) by inserting copies of itself (possibly modified) into other [computer programs](http://en.wikipedia.org/wiki/Computer_programs), data [files](http://en.wikipedia.org/wiki/File_%28computing%29), or the [boot sector](http://en.wikipedia.org/wiki/Boot_sector) of the [hard drive](http://en.wikipedia.org/wiki/Hard_drive); when this replication succeeds, the affected areas are then said to be "infected.

**5.2.5 Worms**

A computer worm is a standalone [malware](http://en.wikipedia.org/wiki/Malware) [computer program](http://en.wikipedia.org/wiki/Computer_program) that replicates itself in order to spread to other computers. Often, it uses a [computer network](http://en.wikipedia.org/wiki/Computer_network) to spread itself, relying on security failures on the target computer to access it. Unlike a [computer virus](http://en.wikipedia.org/wiki/Computer_virus), it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming [bandwidth](http://en.wikipedia.org/wiki/Bandwidth_%28computing%29), whereas viruses almost always corrupt or modify files on a targeted computer.

**5.3. Dialog attacks**

**5.3.1 Eavesdropping**

Eavesdropping is the act of secretly listening to the private conversation of others without their consent, as defined by [Black's Law Dictionary](http://en.wikipedia.org/wiki/Black%27s_Law_Dictionary). This is commonly thought to be [unethical](http://en.wikipedia.org/wiki/Unethical) and there is an old [adage](http://en.wikipedia.org/wiki/Adage) that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

**5.3.2 Message alteration attack**

Alteration of message involves some change to the original message. For instance ,suppose user A send an electronic message transfer $1000 to D’s account to bank B. User C might capture this and change it to transfer $10000 to C’s account .note that the beneficiary and the amount have been changed-instead, only one of these could have also caused alteration of the message.

**CHAPTER 6**

**CASE STUDIES**

**6.1 The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought**

**Stuxnet** is a computer worm that was discovered in June 2010. It was designed to attack Siemens Step7 software running on a Windows operating system.[]](http://en.wikipedia.org/wiki/Stuxnet#cite_note-2) Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges by making them spin out of control while simultaneously making them appear to be running normally, by replaying the recorded system values of normal operation. It is speculated to have been created by U.S and Isareli agencies to attack Iran’s nuclear facilties.



The Stuxnet virus that ravaged Iran's Natanz nuclear facility "was far more dangerous than the cyber weapon that is now lodged in the public's imagination," cyber security expert Ralph Langer tells foreign policy. Stuxnet, a joint U.S- Isarel project, is known for reportedly destroying roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control.

But the exploit had a previous element that was more complicated and "changed global military strategy in the 21st century," according to Langer.

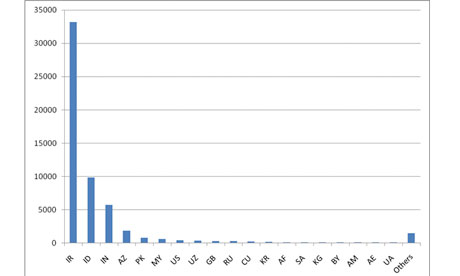
The lesser-known initial attack was designed to secretly draw "the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control" the centrifuges used to enrich uranium, Peter Sanger of The New York Times Reported  last June.

Langer adds that the worm also subtly increased the pressure on spinning centrifuges while showing the control room that everything appeared normal by replaying the plant’s protection system values while the attack occurred.

**OBJECTVIES :-**  The goal of the worm was not aimed at destroying centrifuges, but “reducing lifetime of Iran’s centrifuges and making the Iranian’s Fancy control systems appear beyond their understanding”.

**DETAILS** :- In 2010, Iran reported that as many as 1,000 of its centrifuges at the Natanz nuclear facility, used for enriching weapons-grade uranium, were destroyed by a computer virus. The virus allegedly wrecked the electric motors by accelerating them to damaging speeds and setting back the Iranian nuclear program for at least two years. Iran blamed the U.S. and Israeli intelligence agencies for the attack.  
According to the Washington-based Institute for Science and International Security, the weapon used for the attack was probably a virus called Stuxnet. But unlike other computer viruses, Stuxnet is designed to attack only networks with specific configurations.

* Stuxnet is a type of computer program called a "worm" that can be inserted into a computer or a network of computers, where it replicates itself infecting other machines. Once inside a computer, a worm can corrupt or damage files, causing malfunction of programs.  
  Stuxnet is designed to attack computers with Microsoft Windows operating systems, and it can be most easily inserted through infected removable drives - pocket-size memory banks that connect to standard USB ports.
* After the damage is done, Stuxnet is designed to self-destruct so it is very hard to trace. According to experts studying Stuxnet, it is a very complex program and only government agencies are capable of designing it.

****

**Infection Statistics**

The following graph shows the number of unique infected hosts by country. The above graph shows that 60% of computers infected by stuxnet is located in Iran.

**IRANIAN REACTION (MEASURES)**

In response to the infection, Iran had assembled a team to combat it. With more than 30,000 IP addresses affected in Iran, an official said that the infection is fast spreading in Iran and the problem has been compounded by the ability of Stuxnet to mutate. Iran has set up its own systems to clean up infections and has advised against using the Siemens SCADA antivirus since it is suspected that the antivirus is actually embedded with codes which update Stuxnet instead of eradicating it.

**CHAPTER 7**

**CYBER LAW IN INDIA**

**THE INFORMATION TECHNOLOGY ACT, 2000 AND IT ACT AMENDMENT 2008.**

The Government of India has put in place some mechanisms to counter the threat of cyber terrorism.

* Indian Computer Emergency Response Team (CERT-In): a functional organization of the department of Information Technology with the objective of securing Indian cyber space.
* National Cyber Security Assurance Framework is established by the CERT-In for protection of Critical Information.
* The Information Technology Act, 2000 and IT (Amendment) Act 2008.
* Amendments under the Information Technology Act, 2000 has defined the term “Cyber terrorism” U/Sec. 66F (1).
* Punishment for Cyber terrorism

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life. (Section 66F (2))

* Section 69 gives power to the state to issue directions for interception or monitoring or decryption of any information through any computer source.

Section 70 A and 70 B- Agency for critical information and Indian Computer Emergency response team (CERT-In) for incident response.

**7.1 Why Cyber law in India ?**

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India.

**7.2 What is the importance of Cyber Law?**

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

**7.3 Cyber Law Awareness Program**

Are your electronic transactions legally binding and authentic? Are you verifying your customers' identities to prevent identity theft? Does your online terms and conditions have binding effect? Are you providing appropriate information and clear steps for forming and concluding your online transactions? How are you ensuring data protection and information security on your web site? Are you recognizing the rights of your data subjects?

Transacting on the Internet has wide legal implications as it alters the conventional methods of doing business. To build enduring relationships with your online customers the legal issues of e-transactions need to be addressed from the onset.

This Awareness program will cover the basics of Internet Security basic information on Indian Cyber Law Impact of technology aided crime Indian IT Act on covering the legal aspects of all Online Activities Types of Internet policies required for an Organization. Minimum hardware and software, security measures required in an organization to protect data.

**CHAPTER 8**

**COMPARATIVE STUDY OF INDIAN IT ACTS AND FOREIGN IT ACTS**

**OBJECTIVES**

* To understand the concept of Data Protection.
* To understand the impact of Data Protection Laws on society.
* To analyze various data protection laws in India.
* To compare the different laws in foreign countries related to data protection.

|  |  |
| --- | --- |
| **Indian Data Protection Law**  Under IT Act, 2000  · **Section 43**  This section provides protection against unauthorized access  of the computer system by imposing heavy penalty up to 1 crore. The unauthorized downloading, extraction and copying of data are also covered under the same penalty. Clause ‘c’ of this section imposes penalty for unauthorized introduction of computer viruses of contaminants. Clause ‘g’ provides  penalties for assisting the unauthorized access.  · **Section 65**  This section provides for computer source code. If anyone knowingly of intentionally conceals, destroys, alters or causes  another to do as such shall have to suffer a penalty of imprisonment or fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents.  **· Section 66**  Protection against hacking has been provided under this section.  As per this section hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss of damage.  **Section 72**  This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied  rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.  **Law of Contract**  These days’ companies are relying on the contract law as a useful means to protect their information. The corporate houses enters into several agreements with other companies clients, agencies or partners to keep their information secured to the extent they want to secure it. | **Foreign Data Protection Laws**  **U.K LAW**  U.K. parliament framed its Data Protection Act (DPA) in the year 1984 which thereafter repealed by the DPA of 1998. This Act is basically instituted for the purpose of providing protection and privacy of the personal data of the individuals in UK. The Act covers data which can be used to identify a living person. This includes names, birthday, anniversary dates, addresses, telephone numbers, fax numbers, e-mail addresses etc. It applies only to the data which is held or intended to be held, on computers or other equipments operating automatically in response to instructions given for that purpose or held in a relevant filing system.  **U.S Law**  Though both U.S and the European Union focus on enhancing privacy protection of their citizens, U.S takes a different approach to privacy from that of the European Union. US  adopted the sectoral approach that relies of mix of legislation, regulation, and self regulation. In U.S, data are grouped into several classes on the basis of their utility and importance.  Thereafter, accordingly a different degree of protection is awarded to the different classes of data. Several Acts were also passed in order to stabilize the data protection laws in the United States.  The privacy Act was passed in the year 1974 which provided for establishing standards for when it is reasonable, ethical and justifiable  for government agencies to compare data in different databases. Another Electronic Communications Privacy Act was passed for restricting the interception of electronic communications and prohibiting the access to stored data without the consent of the user or the communication service. |

**CHAPTER 9**

**WAYS ON HOW TO PREVENT CYBER TERRORISM FROM HAPPENING.**

**9.1 Beware of Mail Attachments**

This is one of the most common methods of causing damage. Many email applications today allow for the execution of code in email attachments. Many 'worms' have been released in this manner over the past few years, with effects ranging from relatively harmless propagation of the worm to massive file damage. Users should disable features of their mail application that allow for indiscriminate execution of active code attachments and use a reliable virus scanner that understands email attachments.

**9.2 Engage Anti-Virus Software**

This software has the ability to scan files on a local computer and, in some cases, to monitor inbound and outbound traffic from applications such as email attachments. This software requires constant updating in order to be effective, and the best applications will automatically download updated virus definition files at predetermined intervals.

**9.3 Establish Rules**

Establish rules regarding your child’s Internet, social media and cellular phone activity, and then thoroughly explain these rules to your child. Include rules on how much time your child can spend online and what activities you do not allow. In addition, be firm about any consequences that may occur if your child fails to follow these rules.

**9.4 Explain Appropriate Behavior**

Explain that online behavior should mirror traditional social behavior. Children must understand that the same social interaction rules apply, whether in the schoolyard or on a social networking website. Explaining to your child that he should not engage in any behavior online that he would not engage in during a face-to-face confrontation may help to prevent cyber bullying.

**9.5 Live By Example**

Once you explain appropriate online behavior to your child, you should follow those rules yourself. A child may be less likely to follow proper online etiquette if he does not see his parents behaving in the same fashion. Therefore, you should refrain from harassing others online, even if you make the comment in a joking fashion.

**9.6 Monitor**

The best way to know what your child sees and does online is to monitor his activity. This includes general supervision of, and participation in, his time spent online. Another option includes the installation of monitoring software on your computer to track the activity. The Cyber bullying Research Center warns against secretly spying on your child because this may cause him to focus on hiding what he does online.

**9.7 Filter**

Installation of filtering software on your computer can help protect your child from viewing inappropriate content online. This includes sexually explicit and verbally vulgar text and images. The Cyber bullying Research Center does not recommend relying on this software alone, however, because many children have found ways around this form of protection.

**9.8 Look for Warning Signs**

Parents should look for any changes in their child’s cyber activity. This includes spending more or less time than usual using online forums. A child that suddenly spends a great deal of time online may be bullying another child, whereas a child that becomes withdrawn and avoids the Internet may be a victim of cyber bullying.

**9.9 Communicate**

According to the Cyber bullying Research Center, communication is crucial in protecting your child from potential cyber bullying incidents. Speak with your child regularly to establish an open line of communication. This may make it easier for your child to come forward and tell you he is the victim of a cyber bully.

**9.10 Talk to School Personnel**

Speak with school personnel to learn the school’s policy regarding cyber bullying and share this information with your child. If you become aware of any instances of cyber bullying, contact the school right away to report them. This notifies school personnel of the problem and gives them the opportunity to deal with the situation.

**9.11 Remain Vigilant**

Remain vigilant about enforcing house rules regarding Internet and cell phone usage, even if your child complains. In addition, vigilance when it comes to watching for the warning signs of cyber bullying can mean the difference between stopping the bullying in its early stages and having your child suffer endlessly in silence. Once you report an incident, continue to follow up with school personnel or the police department. This ensures you remain aware of any actions taken against the cyber bully.

**9.12 Contact the Police**

If your child falls victim to cyber bullying and you fear for his safety due to escalating threats, do not hesitate to contact the police. Reporting the incidents may protect your child from additional bullying, and may prevent the incidents from escalating from cyber threats to physical danger. Save any text messages, social media posts and other examples of the bullying to show the police. They can use this information as evidence against the bully.

**9.13 Develop a strong password.**

**9.14 Keep software up to date.**

**9.15 Maintain the accurate browser security settings.**

**9.16 Compile strong firewalls**.

**What Can We Do?**

Go on the defensive *now*

* Educate senior management on risks of cyber warfare
* Make infosec a top priority
* Beef up your security technology
* Insist on flawless execution: compliance to security standards in all areas

Work with other companies, government agencies

* NIPC
* IT ISAC
* SAINT

**Some Specifics: Be Prepared**

* **Maintain high alert & vigilance**
* **Update OS and applications regularly**
* **Enforce strong passwords**
* **“Lock down" systems**
* **Keep anti-virus software installed and up-to-date**
* **Employ intrusion detection systems and firewalls**

****

**CHAPTER 10**

**CONCLUSION**

The Internet was developed primarily as an unregulated, open architecture. Not only are we observing a predictable backlash to the ‘corporatization’ of the network, where the tools of destruction can easily be placed in the hands of the dissatisfied or malevolent people, we must also deal with the fact that the infrastructure is ideally suited to criminal activities. Some of these activities are being promoted as cyber terrorism; however, the loose use of the term is actually undermining the defense capabilities of the very corporations and governments who are at risk. Events can be analyzed in terms of their critical factors, and only if these factors all exist can the event legitimately be called terrorism. With regard to cyber terrorism, that is, the use of hacking tools and techniques to inflict grave harm such as loss of life, few conclusions can be drawn about its potential effect on foreign policy, because there have been no reported incidents that meet the criteria. What can be said is that the threat of cyber terrorism, combined with hacking threats in general, is influencing policy decisions related to cyber defense at both a national and international level. If we look at terrorism in general for insights into the potential effects of cyber terrorism, we find that the effect of terrorism on the foreign policy issues at hand is similarly difficult to assess, but here again, the threat of terrorism, particularly chemical, biological, and nuclear terrorism, is having a significant effect on national defense policy.

**REFERNCES**

* [**https://www.google.co.in/search?q=cyber+warfare+depth&rlz=1C1RNNN\_enIN400IN400&espv=210&es\_sm=93&source=lnms&tbm=isch&sa=X&ei=yqSiUrGaAc2UrAepuoG4Aw&ved=0CAkQ\_AUoAQ&biw=1212&bih=695**](https://www.google.co.in/search?q=cyber+warfare+depth&rlz=1C1RNNN_enIN400IN400&espv=210&es_sm=93&source=lnms&tbm=isch&sa=X&ei=yqSiUrGaAc2UrAepuoG4Aw&ved=0CAkQ_AUoAQ&biw=1212&bih=695)
* Berkowitz, Bruce, “Information Warfare: Time to Prepare.” Issues in Science and Technology, Winter, 2000. <http://www.nap.edu/issues/17.2/berkowitz.htm>
* “Cyber Attacks During the War on Terrorism:-   
  A Predictive Analysis.” Dartmouth Institute for Security Technology Studies.<http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>