SEMINAR ABOUT

CYBER TERRORISM
"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives"
CYBERTERRORISM:

➢ This broad definition was created by Kevin G. Coleman of the Technolytics Institute.

➢ The term was coined by Barry C. Collin.
Overview

- As the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. with membership based on ethnicity or belief), communities and entire countries, without the inherent threat of capture, injury, or death to the attacker that being physically present would bring.

- As the Internet continues to expand, and computer systems continue to be assigned more responsibility while becoming more and more complex and interdependent, sabotage or terrorism via cyberspace may become a more serious threat.
Public interest in cyberterrorism began in the late 1980s. As the year 2000 approached, the fear and uncertainty about the millennium bug heightened and interest in potential cyberterrorist attacks also increased.

- However, although the millennium bug was by no means a terrorist attack or plot against the world or the United States, it did act as a catalyst in sparking the fears of a possibly large-scale devastating cyber-attack.
- Commentators noted that many of the facts of such incidents seemed to change, often with exaggerated media reports.
- The high profile terrorist attacks in the United States on September 11, 2001 lead to further media coverage of the potential threats of cyberterrorism in the years following.
- Mainstream media coverage often discusses the possibility of a large attack making use of computer networks to sabotage critical infrastructures with the aim of putting human lives in jeopardy or causing disruption on a national scale either directly or by disruption of the national economy.
Effects

- Cyberterrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries' economy greatly, thereby stripping it of its resources and making it more vulnerable to military attack.

- Cyberterror can also affect internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals.
What is being done?

- In response to heightened awareness of the potential for cyber-terrorism President Clinton, in 1996, created the Commission of Critical Infrastructure Protection. The board found that the combination of electricity, communications and computers are necessary to the survival of the U.S., all of which can be threatened by cyber-warfare.
- Most other government organizations have also formed some type of group to deal with cyber-terrorists and created its own group, the Information Warfare Center, staffed with 1,000 people and a 24-hour response team.
- The FBI investigates hackers and similar cases.
- The Secret Service pursues banking, fraud and wiretapping cases. The Air Force created its own group, Electronic Security Engineering Teams, ESETs.
The Secret Service pursues banking, fraud and wiretapping cases. The Air Force created its own group, Electronic Security Engineering Teams, ESETs.

Teams of two to three members go to random Air Force sites and try to gain control of their computers. The teams have had a success rate of 30% in gaining complete control of the systems.
How can we protect ourselves?

- Currently there are no foolproof ways to protect a system. The completely secure system can never be accessed by anyone. Most of the militaries classified information is kept on machines with no outside connection, as a form of prevention of cyber terrorism. Apart from such isolation, the most common method of protection is encryption.

- The widespread use of encryption is inhibited by the governments ban on its exportation, so intercontinental communication is left relatively insecure.
Here are few key things to remember to protect yourself from cyber-terrorism:

- All accounts should have passwords and the passwords should be unusual, difficult to guess.
- Change the network configuration when defects become known.
- Check with vendors for upgrades and patches.
- Audit systems and check logs to help in detecting and tracing an intruder.
- If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.
What would the impact be?

- The intention of a cyber terrorism attack could range from economic disruption through the interruption of financial networks and systems or used in support of a physical attack to cause further confusion and possible delays in proper response.
- Direct Cost Implications
- Loss of sales during the disruption
- Staff time, network delays, intermittent access for business users
- Increased insurance costs due to litigation
- Loss of intellectual property - research, pricing, etc.
- Costs of forensics for recovery and litigation
- Loss of critical communications in time of emergency
- Indirect Cost Implications
Indirect Cost Implications

- Loss of confidence and credibility in our financial systems
- Tarnished relationships & public image globally
- Strained business partner relationships - domestic and internationally
- Loss of future customer revenues for an individual or group of companies
- Loss of trust in the government and computer industry
Who are cyber terrorists?

- From American point of view the most dangerous terrorist group is Al-Qaeda which is considered the first enemy for the US.
- According to US official’s data from computers seized in Afghanistan indicate that the group has scouted systems that control American energy facilities, water distribution, communication systems, and other critical infrastructure.
- After April 2001 collision of US navy spy plane and Chinese fighter jet, Chinese hackers launched Denial of Service (DoS) attacks against American web sites.
  A study that covered the second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks.
why do they use cyber attacks?

- Cyber terrorist prefer using the cyber attack methods because of many advantages for it.
- It is Cheaper than traditional methods.
- The action is very difficult to be tracked.
- They can hide their personalities and location.
- There are no physical barriers or check points to cross.
- They can do it remotely from anywhere in the world.
- They can use this method to attack a big number of targets.
- They can affect a large number of people.
Forms of cyber terrorism

(I) Privacy violation:
The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate. The right to privacy as an independent and distinctive concept, under which a new cause of action for damages resulting from unlawful invasion of privacy was recognized.

In recent times, however, this right has acquired a constitutional status, the violation of which attracts both civil as well as criminal consequences under the respective laws.

Man under the refining influence of culture, has become sensitive to publicity, so that solitude and privacy have become essential to the individual.

Certain acts have been categorized as offences and contraventions, which have tendency to intrude with the privacy rights of the citizens.
(II) Secret information appropriation and data theft:

- The information technology can be misused for appropriating the valuable Government secrets and data of private individuals and the Government and its agencies.
- A computer network owned by the Government may contain valuable information concerning defence and other top secrets, which the Government will not wish to share otherwise.
- The same can be targeted by the terrorists to facilitate their activities, including destruction of property.

NOTE: The definition of property is not restricted to moveables or immovable.
(III) Demolition of e-governance base:

The aim of e-governance is to make the interaction of the citizens with the government offices hassle free and to share information in a free and transparent manner. It further makes the right to information a meaningful reality. In a democracy, people govern themselves and they cannot govern themselves properly unless they are aware of social, political, economic and other issues confronting them. To enable them to make a proper judgment on those issues, they must have the benefit of a range of opinions on those issues.
(IV) Distributed denial of services attack:

The cyber terrorists may also use the method of distributed denial of services (DDOS) to overburden the Government and its agencies electronic bases. This is made possible by first infecting several unprotected computers by way of virus attacks and then taking control of them. Once control is obtained, they can be manipulated from any locality by the terrorists. These infected computers are then made to send information or demand in such a large number that the server of the victim collapses.
(V) Network damage and disruptions:

The main aim of cyber terrorist activities is to cause networks damage and their disruptions. This activity may divert the attention of the security agencies for the time being thus giving the terrorists extra time and makes their task comparatively easier. This process may involve a combination of computer tampering, virus attacks, hacking, etc.
E. The danger of cyber terrorism-

- Cyber terrorists can destroy the economy of the country by attacking the critical infrastructure in the big towns such as electric power and water supply, still the blackout of the North Western states in the US in Aug. 15, 2003 is unknown whether it was a terrorist act or not, or by attacking the banks and financial institutions and play with their computer systems.

- Cyber terrorists can endanger the security of the nation by targeting the sensitive and secret information (by stealing, disclosing, or destroying).
Here are few key things to remember to protect from cyber-terrorism:

1. All accounts should have passwords and the passwords should be unusual, difficult to guess.
2. Change the network configuration when defects become known.
3. Check with vendors for upgrades and patches.
4. Audit systems and check logs to help in detecting and tracing an intruder.
5. If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.
Indian law & Cyber terrorism-

In India there is no law, which is specifically dealing with prevention of malware through aggressive defense. Thus, the analogous provisions have to be applied in a purposive manner. The protection against malware attacks can be claimed under the following categories:

(1) Protection available under the Constitution of India, and
(2) Protection available under other statutes.
Conclusion:

The problem of cyber terrorism is multilateral having varied facets and dimensions. Its solution requires rigorous application of energy and resources. It must be noted that law is always seven steps behind the technology. This is so because we have a tendency to make laws when the problem reaches at its zenith. We do not appreciate the need of the hour till the problem takes a precarious dimension. At that stage it is always very difficult, if not impossible, to deal with that problem. This is more so in case of offences and violations involving information technology. One of the argument, which is always advanced to justify this stand of non-enactment is that “the measures suggested are not adequate to deal with the problem”.
The ultimate solution to any problem is not to enact a plethora of statutes but their rigorous and dedicated enforcement.

It must be appreciated that it is not the “enactment” of a law but the desire, will and efforts to accept and enforce it in its true letter and spirit, which can confer the most strongest, secure and safest protection for any purpose.

The enforcement of these rights requires a “qualitative effort” and not a “quantitative effort”.

Thus, till a law dealing expressly with cyber terrorism is enacted, we must not feel shy and hesitant to use the existing provisions
QUERIES?