SEMINOR REPORT ON CYBER TERRORISM

SUBMITTED TO
MS. SHEWTA GUPTA
LECTURER V.I.T.S.

SUBMITTED BY
NIDHI KUMARI
ROLL No:- 0214IT081032
INFORMATION TECHNOLOGY
The term cyberterrorism is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyberterrorism.
Cyberterrorism is defined as “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.”
Background information

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.

THE TERRORISM MATRIX

When terrorism is examined in view of these definitions, there are some pervasive elements: people (or groups), locations (of perpetrators, facilitators, victims), methods/modes of action; tools, targets, affiliations, and motivations

<table>
<thead>
<tr>
<th>Perpetrator</th>
<th>Group</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place</td>
<td>Sri Lanka</td>
<td>Japan</td>
</tr>
<tr>
<td>Action</td>
<td>Threats/Violence</td>
<td>Violence</td>
</tr>
<tr>
<td>Tool</td>
<td>Kidnapping/Harassment</td>
<td>Nerve Gas</td>
</tr>
<tr>
<td>Target</td>
<td>Government Officials/Recruits</td>
<td>!=AUM</td>
</tr>
<tr>
<td>Affiliation</td>
<td>Actual/Claimed</td>
<td>Actual/Claimed</td>
</tr>
<tr>
<td>Motivation</td>
<td>Social/Political Change</td>
<td>World Domination</td>
</tr>
</tbody>
</table>
PERPETRATOR

Interactions between human beings are complex; while the obvious solutions gravitate toward monitoring, we are concerned with virtualization of interactions, which can lead to relative anonymity and desensitization.

PLACE

Location exists as an element, but is not a ‘required’ element in traditional terrorism in that an event does not have to occur in a particular location. Thus, whether an act is virtual/virtual, virtual/real world or real world/virtual is of interest only as factor in modeling solutions.

ACTION

In traditional scenarios, terrorist scenarios typically are violent or involve threats of violence. While there have been many studies of violence in the physical world, more research is called for in terms of ‘violence’ as a virtual phenomenon.
TOOL

There are an almost uncountable number of ways that the terrorist can use the computer as a tool. Facilitating identity theft, computer viruses, hacking, use of malware, destruction or manipulation of data all fall under this category. These uses of the computer, when combined with ‘computer as target’ form the ‘traditional’ picture of cyberterrorism. These will be discussed in more detail later in the section Computers: The Weapon of the Cyberterrorist.

TARGET

There are a large number of potential targets that involve, either directly or indirectly, computers. Consider, for example, the impact of Personal Identity Theft.
AFFILIATION

It is possible for a person to read all about a given cause and chat with proponents of the cause without ever leaving the safety of his or her own home. New recruits can thus become affiliated with a terrorist group, commit to carrying out given actions, all without ever actually coming into contact with another human being.

MOTIVATION

Political, social, and economic changes are the motivations present in real-world terrorism. Combining a dependence on Internet-connected systems for banking and Ecommerce with the ability of anyone with a desire and readily available tool to disrupt these areas, results in a situation that is all too clear: unless steps are taken to significantly reduce risks, disaster is inevitable. Even with the best risk reduction, there are still likely to be problems.

PURE CYBERTERRORISM

The concept of ‘pure’ cyberterrorism — that is, terrorism activities that are carried out entirely (or primarily) — in the virtual world is an interesting one. The Internet provides many different ways of anonymously meeting with ‘like minded’ individuals in a (comparatively) safe way.
THE NEW TERRORISM

New terrorist organizations are highly funded, technologically articulate groups capable of inflicting devastating damage to a wide range of targets.

COMPUTERS — THE WEAPONS OF THE CYBERTERRORIST

Following on from the discussions above, it becomes obvious that the most likely ‘weapon’ of the cyberterrorist 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.
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 originated in the field of Tort law, under which a new cause of action for damages resulting from unlawful invasion of privacy was recognised.

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.
III) 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.

(IV) 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.
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.

Examples

One example of cyberterrorists at work was when terrorists in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. However, the culprits were stopped before damage actually occurred.
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.

Methods of Protection: No Easy Answers

We must consider the following elements when building a counter-CyberTerrorist program:

- We must accept that while the theories of terrorism stand true, the way in which we approach counter-terrorism, in this case, counter-CyberTerrorism, must change.
- We must cooperate and share intelligence in ways we have never have before.
- We must enlist the assistance of those individuals who understand the weapons we are facing and have experienced fighting these wars.
The Present, and The Future

Compared to the other terrorism weapons, is the threat of cyber terrorism for real or is it just hyped and exaggerated? Since the 9/11 attacks in the United States, FBI warnings of potential terror attacks through the Internet spawned diverse reactions from different groups. Some believe that the threat is real and possible at any given moment, while some countered that it is not that easy, and is almost impossible with all of our security systems. Should the threat of cyber terrorism be for real, what damage can it bring to humankind and how bad can it get?

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.
THANK YOU