CYBER SECURITY

C.Subramanian

Political Science & Public Administration Wing- DDE, Annamalai University

ARTICLE INFO

ABSTRACT

Cyber attacks and cyber terrorism are the new looming threats on the horizon and the country needs to focus on specific areas to guarantee cyber security. Cyber security is very important to protect the IT services in corporate establishments, government organisations as well as the ones used by the general public. Cyber terror is a relatively new term. The Federal Bureau of Investigation (FBI) defines cyber terror as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives...through the exploitation of systems deployed by the target.” In the fast developing countries where information technology (IT) has reached the apex, the security of data compiled, stored and transmitted is of utmost important. In this context, this paper makes an attempt to explore about cyber crimes in India, effects of cyber terrorism and its counter measures.

INTRODUCTION

Cyber terror is a relatively new term. The Federal Bureau of Investigation (FBI) defines cyber terror as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives...through the exploitation of systems deployed by the target.”

There are two views that exist for defining cyber terrorism; effects-based and internet-based. In an effects-based situation cyber terrorism exists when computer attacks result in a situation where fear is generated which is similar to a traditional terrorist attack. In an internet-based situation attacks are done to cause harm or severe economic damage. “The objective of a cyber attack includes four areas: Loss of integrity, loss of availability, loss of confidentiality, and physical destruction”.(Army.U)” Cyber terrorism 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.”

Effects of Cyber Terrorism

Experts are of the view that an increased reliance on computer controlled means of manufacturing has heightened the possibilities of an act of cyber terrorism. In the developed countries there is a fear that a cyber attack on computer programs controlling the mixture of ingredients for food products and pharmaceuticals could lead to a national disaster”(Scott Berinato). In countries like India the threat is more likely on public information systems like the print and electronic media. As computer controlled entertainment programs and print designs are becoming more frequently used the threat of a cyber attack to delete crucial information or add unsolicited material to the program could cause public fear and dismay.

Secondly, Cyber terrorists could target airline and railway information systems. Air traffic control and railway signaling are now-a-days run on computer programs. A cyber attack on them could lead to mid air collision or train smash up. On a more possible scale, air and railway announcement systems could come under attack. Public announcement apparatus could be hijacked by a cyber terrorist to create panic in order to achieve a more conventional objective.

Thirdly, cyber terrorists are feared to have manufactured computer bombs. Bombs are controlled by a computer program. A cyber terrorist ‘instructs’ the bombs to detonate or not to detonate in a desired sequence with probability content programmed into them as well(Ronald L.Dick).

Fourthly, a cyber attack on financial transactions is the widely feared form of cyber terrorism. E-trading of stocks
could come to a standstill if cyber terrorists could break the security codes of a stock exchange (Susan W. Brenner, and Marc D. Goodman). Public money could be at risk if electronic money transfers are blocked and diverted to terrorist accounts all over the world. But one of the most potent form of cyber terror regarding finance is the lack of data mining capabilities of security agencies.

217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006) thereby reporting an increase of 52.8% in 2007 over 2006. 22.3% cases (49 out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

**Table** Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2004-2007

<table>
<thead>
<tr>
<th>Crime Heads</th>
<th>Cases Registered</th>
<th>% Variation in 2007 over 2006</th>
<th>Persons Arrested</th>
<th>% Variation in 2007 over 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Tampering computer source documents</td>
<td>2</td>
<td>10</td>
<td>11</td>
<td>10.0</td>
</tr>
<tr>
<td>2. Hacking with Computer System</td>
<td>14</td>
<td>33</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>i) Loss/damage to computer resource/utility</td>
<td>12</td>
<td>41</td>
<td>34</td>
<td>46</td>
</tr>
<tr>
<td>ii) Hacking</td>
<td>34</td>
<td>88</td>
<td>69</td>
<td>99</td>
</tr>
<tr>
<td>3. Obscene publication/transmission in electronic Form</td>
<td>44</td>
<td>99</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>4. Failure</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>i) Of compliance/orders of Certifying Authority</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ii) To assist in decrypting the information intercepted by Govt. Agency</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5. Un-authorsised access/attempt to access to protected computer system</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6. Obtaining licence or Digital Signature Certificate by of fact</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7. Publishing false Digital Signature Certificate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8. Fraud Digital Signature Certificate</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>9. Breach of confidentiality/privacy</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>10. Other</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>179</td>
<td>142</td>
<td>217</td>
</tr>
</tbody>
</table>

Fifthly, a cyber terrorist could cause deep dents on the public sentiment. In today’s telecommunication industry almost all communications are computer controlled networks. The common man’s increasing dependence on such modes of communications makes him vulnerable to a cyber terror attack. A mobile phone virus could render thousands of cell phones useless. On a more grand scale, anti national and anti social messages could be generated through SMS and MMS and entire networks could come under attack. This could seriously dent the public sentiment which is so fragile in a developing country like ours.

On the whole the above hypothetical situations of cyber terror attacks may not be considered an impossibility. Though such occurrences are unheard of outside the law enforcement circles in India, examples of cyber attacks in the US have been cited here so as to present the possibility of such attacks. In order to appreciate the seriousness of cyber terrorism, it is important to discuss what cyber terrorists can do by examining incidents that have actually occurred in the past. Most of the following incidents cannot be classified as cyber terrorist acts because most were not done to further any political or social goals.

45.6% (99 cases) of the total 217 cases registered under IT Act 2000 were related to Obscene publication / transmission in electronic form, normally known as cyber pornography. 86 persons were arrested for committing such offences during 2007. There were 76 cases of Hacking with Computer System during the year wherein 48 persons were arrested. Out of the total (76) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were 39.5% (30 cases) whereas the cases related to Hacking under Section 66(2) of IT Act were 60.5% (46 cases). Maharashtra (19) and Kerala (4) registered maximum cases under Sec 66(1) of the IT Act out of total 30 such cases at the National level. Out of the total 46 cases relating to Hacking under Sec. 66(2), most of the cases (31 cases) were reported from Karnataka followed by Kerala (7) and Andhra Pradesh (3).

29.9% of the 154 persons arrested in cases relating to IT Act, 2000 were from Maharashtra (46) followed by Karnataka and Madhya Pradesh (16 each). The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 showed that 63.0% of the offenders were in the age group 18 – 30 years (97 out of 154) and 29.9% of the offenders were in the age group 30 - 45 years (46 out of 154). Tamil Nadu reported two offenders whose age was below 18 years.
Further details on the State/UT-wise and age-group wise profiles may be seen in Table-18.2.

Crime head-wise and age-group wise profile of the offenders arrested under IT Act, 2000 revealed that 55.8% (86 out of 154) of the offenders arrested under ‘Obscene publication / transmission in electronic form’ of which 70.9% (61 out of 86) were in the age-group 18 – 30 years. 50% (24 out of 48) of the total persons arrested for ‘Hacking with Computer Systems’ were in the age-group of 18-30 years.

CYBER TERRORISM COUNTERMEASURES

A statement of fact is given by an expert on cyber terrorism in the US. “Cyber terrorism is a fairly recent threat, therefore, there is still speculation as to who is ultimately responsible for controlling cyber terrorism. However, the government’s inability to deal with cyber terrorism is part of the problem. For every fifty complaints given to the law enforcement agencies by private corporations, only one was prosecuted. This is due to the government’s lack of resources, both of human specialists and financial funding. The fact is especially frustrating to private corporations who lose an estimated 10 billion dollars a year to electronic crime”. In the US there is now a debate as to what constitutes an act of cyber terror and what is a cyber crime. Cyber crime drains on the exchequer and has adverse impact on the economy but it does not pose a threat to the national security of the country. Whereas cyber terrorism affects the society, polity as well as the economy. The US information system’s vulnerabilities were dramatized during a 1997 Joint Chiefs of Staff exercise, code-named “Eligible Receiver.” The purpose of the exercise was to test the United States’ ability to respond to cyber attacks. The results opened the eyes of skeptics. Using software widely available from hacker websites, the thirty-five-person team showed how they could have disabled elements of the U.S. electric power grid by exploiting Supervisory Control and Data Acquisition (SCADA) systems (which allow remote control of the systems). They also demonstrated how to incapacitate portions of U.S. military command-and-control systems in the Pacific and Emergency-911 systems in the United States.

In response to the emerging threat of cyber terrorism, on May 22, 1998, Presidential Decision Directive (PDD-63) authorized the creation of a National Infrastructure Protection Center (NIPC). The NIPC is now housed within the Federal Bureau of Investigation (FBI) and serves as a lookout for attempted intrusions and to monitor cyber attacks. PDD-63 also led to the establishment of the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce to serve as a policy coordination staff for infrastructure assurance issues within the Executive Branch6 (Frank Cilluffo & Paul Byron Pattak).

For a country like India what are the implications? Cyber terror threats are not different in quality and quantity for any particular country. They are all the same nature. The CBI in India is vested with powers to check cyber crime. The state police in the various states are also responsible for the prevention of cyber crimes. How far have the Indian law enforcement agencies been able to differentiate between cyber crime and cyber terrorism remains to be seen. Keeping in view the rise of incidents of cyber crime the CBI was bestowed with certain specialized agencies. The Cyber Crime Investigation Cell (CCIC) was notified on 3.3. 2000. The cell is headed by a Superintendent of Police. The jurisdiction of this cell is all India. Another unit under the CBI is the Cyber Crime Research And Development Unit (CCRDU). It was set up in August 2000 to collect and collate information on cyber crimes reported from different parts of the country. The function of this is to liaise with state police and other enforcement agencies and to collect information on cases of cyber crime reported to them for investigation and also to find out about the follow up action taken in each case. The unit liaises with software experts to identify areas which require attention of state police for prevention and detection of such crimes with a view to train them for the task. It collects information on latest cases reported in other countries and the innovations employed by police forces in those countries to handle such cases. The unit maintains close rapport with the Union Ministry of Information Technology and the Interpol HQ at Lyons for achieving its objective of giving needed thrust for collection and dissemination of information on cyber crime. The CBI has apart from the CCIC and the CCRDU a Cyber Forensics and Digital Analysis Centre and two Computer Emergency Response Teams, to address the growing problem of cyber crime.

The law enforcement agencies in India are responsible in maintaining the sanctity of the IT Act of 2000. The units under the CBI focus on chapter XI of this act. This chapter deals with a range of cyber crimes such as hacking with computer source documents, Hacking with computer systems, Publishing of information which is obscene in electronic form, Publishing digital signature certificates false in certain particulars, publishing for fraudulent purpose etc.

From the above it is evident that the focus is more on the concept of cyber crime whose motive is to disrupt public information systems for monetary gains. These crimes do not affect the national security of the country. A cyber terrorist however has an agenda to threaten national security. Cyber terrorism aims to infringe not only the legal apparatus of the political and economic aspects of the country, but also the Socio-Cultural ethos of the country. Beliefs and norms which govern social relationships and institutions come under attack by cyber terrorism in the form of dissemination of adverse information causing dismay and hurt to the mental psyche of the citizens. This leads to a disruption in socialization and identity formation among the public especially among the youth.

There are several key recommendations to improve the current U. S. cyber security posture:

- Accept cyberterrorism as a viable near-term threat
 Organize for success and establish the new Department of Cyber Security
 Debate the issues with the Parliament and the public to raise awareness
 Increase punishment for cyber crimes with terror or death as a motive
 Finalize the national cyber security plan and implement it
 Commit Parliamentary funding to improve cyber security
 Commit manpower and training to implement the plan effectively

CONCLUSION
The problem of cyber terrorism is multilateral having varied facets and dimensions. Perhaps the whole exercise of throwing light on the new forms of terrorism is to serve this purpose of making the common citizen of the country more aware of the threats and feel responsible by keeping the awareness levels at an optimum to meet unexpected contingencies as technology and its uses in every day life becomes more and more common.

References