Chapter 10
Cyberattacks, Cybercrime and Cyberterrorism

Saurabh Ranjan Srivastava
Malviya National Institute of Technology, India

Sachin Dube
Malviya National Institute of Technology, India

ABSTRACT

This chapter describes how with growing reliance of modern society over internet and web-based services in every nook and corner of our daily lives, the threats of disruption and damage to these services has also evolved at a parallel rate. One of these threats having a potential of severe and life-threatening devastations is 'Cyberterrorism.' Contrasting to non-lethal terms such as 'internet vandalism' and 'hacktivism,' cyberterrorism encompasses a daunting reach to destruction to the fabric of our modern society. Because of its nature, despite its rapid growth, contrary to conventional terror attacks, cyberterrorism still seems distant from creating a direct threat to civilian life and society. Due to this distance, there is a lack of attention and focus on counter mechanisms against cyberterrorism. By applying effective techniques and keeping our eyes open, establishments can go a long way to avert cyberterror attacks and also recover quickly in the occurrence of an attack. The conclusion of this chapter is that additional research is needed to identify the areas in which personal and professional functions on the internet are still vulnerable.

INTRODUCTION

A cyberattack or simply an attack on computer systems and services can be considered as an intentional and planned activity targeted to disrupt and/or damage the normal functioning of equipment, corruption or theft of stored data and alteration in process control of running systems (Collin, 2013). Cybercrime or more commonly 'internet crime' is the crime committed in the cyberspace, by making use of computer and internet services.

As mentioned by Gaub (2017), since several past years, terrorist organizations have aimed and struggled to build well-trained terror squads globally. On encountering the financial, organizational

DOI: 10.4018/978-1-5225-4100-4.ch010

and workforce difficulties, they started moving towards the sleeper cell and leaderless, low resistance models of operations.

In continuation of the search for such low resistance models of operation, the possibility of occurrence of a cyber-attack has increased greatly with modernization and computerization of civilian as well as army infrastructures. With the evolution of distributed systems and growing network capabilities, devices and equipment are now attaining the ability to communicate and respond to each other. Threats of a cyberterror attack may arise from militants, terrorist groups, professional criminals, disruptive anti-state bodies and even from governments of rogue nations. Such threat can eventually result in break-in and theft of government documents, corruption of databases or damage of financial data, which presents the possible impact of such threats.

But the technical know-how and even acceptance towards the existence of terror threats in cyberspace has yet to claim its space. Due to this gap, policies and mechanisms to counter cyberterrorism have yet to be created at national and international levels. Unlike physical terror attacks, expensive logistic trail and the organized workforce is not a compulsion for cyberterror activities. Even a single hacker with justified computer resources and practical sense of attack implementation skills is capable enough of committing a cyberterror attack across the borders from a distant country. An example of such attack can be capturing the control of traffic system of a city and manipulation of signaling services causing multiple accidents at numerous spots throughout the city.

In case of conventional terrorism, pre-planned groundwork and physically dynamic mediums such as explosives and suicide bombers are crucial to execute an attack. By invoking injuries, property destruction and civilian deaths, this class of attacks are generally successful in generating an environment of fear and anxiety among the targeted population. This environment of fear is in turn, used to demoralize and pressurize a government to adopt or abort a policy specific decision. An example of such attack is the Madrid terror bombings killing 191 people in the year 2004 that led to the departure of Spanish armed forces from Iraq (Sciolino, 2004).

Furnelb and Warren (1999) stated that, contrary to conventional terrorism, cyberterrorism utilizes the malicious internet and computer technologies to achieve similar ideological, religious or political goals. The activities for the achievement of these goals may involve stealing money, data or identities, rupturing services and infrastructures, shutting down functions of organizations and much more. In the current scenario, the targets and motivation of all cyberterrorists may not be clearly obvious. Instead of executing any financial scam or ransom, they target to disrupt social fabric and damage public confidence in its administrative mechanism.

For the major part of the world, the internet is not constrained by national borders. This leads to the possibility of a cyberterrorist conducting a computer hack from another country across the globe. Such a hack will consume only a few compromised systems in its track to hide the trail of the attack.

Apart from such transnational attacks, possibilities of insider threats are also existent. An insider such as an annoyed ex-employee can cause compromise of the considerable amount of information. Additional to data and identity theft, such insider compromise can inject malware into the system or can even leak details of the victim system or service to the attacker.

During a cyberterrorist attack, such compromised systems as discussed above may be private computer servers, public internet or even secure government networks. As compared to costs of arms and explosives, the purchase and scaling costs of computer and internet facilities are far less expensive. Additional to costs, the anonymity of attacker and the range of damage are the other benefits that make cyberterrorism an attractive option for the terrorist organizations.