Chapter 11
Cyberterrorism:
Can Terrorist Goals be Achieved Using the Internet?

ABSTRACT

Cyberterrorism is a subject which has gained considerable interest from both researchers and media, particularly since the attacks on the United States of America on September 11th 2001. Nevertheless, there is a considerable lack of empirical research in the area, with most writings based on theoretical or anecdotal accounts, despite many calls by leaders in the field for more empirically sound methods. This is further complicated by the difficulty in even finding consensus as to what does and does not constitute cyberterrorism. This chapter aims to determine if cyberterrorism is a likely strategy to be used by terrorists, and if so, how it might be used to strike terror into the hearts of citizens. Following some illustrative scenarios of terrorist activity online, some of the conflicting definitions of the subject will be considered. The methods used by terrorists online will then be outlined, including both an examination of the possibility of using the internet for a large scale attack, and using the internet for more conventional activities such as recruitment and fundraising. The psychology of terrorism will then be examined, including investigations of the personalities and psychiatric health of terrorists, and it will be examined as to whether or not the findings relating to 'traditional' terrorists can also be applied to online terrorist activity. The potential effects of an attack on victims will also be considered. Consideration will be given as to how terrorist activity online could be prevented, while also recognising that the increasing online presence of terrorist organisations may be a double-edged sword, enabling counter-terrorism agencies to employ new strategies in their work.

DOI: 10.4018/978-1-61350-350-8.ch011

BACKGROUND

In order to illustrate the potential of the Internet for terrorist causes, two fictional scenarios are presented below.

A government has a strong online presence, maintaining official websites along with several profiles on a variety of social networking websites. One afternoon, a 'Denial of Service' attack renders their official websites useless. No legitimate user can gain access to the information or services available online, including taxation, health care appointments and corporation services. Simultaneously, unofficial access is gained to the government run social networking profiles, and status messages are posted which include insulting comments that are offensive to many members of the society, particularly those in the armed services. The government realizes that they have been the victim of an attack by a terrorist organization. While it only takes a few days to restore their online presence to its previous status, there is significant damage to the public confidence in the government. The people are worried that terrorists may have accessed their personal information, and that they are at risk of identity theft. They also have concerns that the government is unable to properly defend their online resources appropriately.

A young man is beginning to feel disillusioned. He feels that society is not treating him as well as it should, and that the regime he lives under is unfair, particularly to his ethnic group. He spends some time searching the internet, and finds the website of a terrorist organization. The website is filled with information and propaganda. There are messages from the terrorists, explaining their reasons for fighting, and the young man finds that he agrees with their position. He views pictures on the website of women and children being mistreated by the regime, and he becomes angry. He finds instructions on the website for making bombs, but is still unsure if he wants to become violent for his cause. The website includes a chat facility, within which he makes contact with members of the terrorist organization. He finds they hold the same beliefs as he does, and although he is still a little unsure, he finds their arguments very persuasive. For the first time in many years he feels that others understand his perspective. After a vetting process, he joins their organization.

In addition to these, there have been several fictional depictions of cyberterrorism in the popular media. One of the most famous of these is the 2007 film *Live Free or Die Hard* (released as *Die Hard 4.0* outside of the United States), which depicted a scenario where a terrorist organization employed computer hackers to develop code that was used to take control of various critical systems, including traffic lights and the stock market (Fottrell & Wiseman, 2007). While the above scenarios are fictional, and the world has not experienced an attack similar to that portrayed in the *Die Hard* film, terrorists are making increased use of modern technology for their causes. In September 2010 the *Stuxnet* worm (a form of malware) infiltrated some of the personal computers at Iran's first nuclear power station (BBC News, 2010a). If it ever reaches the computers designed to control the industrial machinery, such as motors and coolers, it may be able to instruct the equipment to turn on or off at given signals or equipment status settings. It is a highly tailored worm, searching for very specific configurations. While it is not yet known who the developer of the worm was, or whether their motive is cyberterrorism or something else, this case provides evidence that there is potential for cyberterrorists to cause significant harm to critical systems.

The first two scenarios, while fictional, are based on strategies that some terrorist organizations are already known to employ. For example, Denning (2001) describes an "email bombing" by the Internet Black Tigers against the Sri Lankan embassies in 1998, which flooded their system by filling staff in-boxes with spam emails that