Chapter I
Cyber Terrorism Attacks

Kevin Curran
University of Ulster, UK

Kevin Concannon
University of Ulster, UK

Sean McKeever
University of Ulster, UK

ABSTRACT

Cyber terrorism is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents. The possibilities created for cyber terrorism by the use of technology via the internet are vast. Government computer networks, financial networks, power plants, etc are all possible targets as terrorism may identify these as the most appropriate features to corrupt or disarm in order to cause havoc. Manipulation of systems via software with secret "back doors", theft of classified files, erasing data, re-writing web pages, introducing viruses, etc are just a few examples of how terrorism can penetrate secure systems. This chapter provides a brief overview of previous cyber terrorism attacks and government responses.

INTRODUCTION

Terrorism can be defined as "The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons" (Denning, 2000, pp. 54-55). To date there has been no serious act of cyber terrorism, but computer networks have been attacked in recent conflicts in Kosovo and the Middle East. As terrorists have a limited amount of funds, cyber attacks are more tempting as they would require less people and less resources (meaning less funds). Another advantage of cyber attacks is that it enables the terrorist to remain unknown, as they could be far away from the actual place where the terrorism

is being carried out. As terrorists normally set up camp in a country with a weak government, the cyber terrorist could set up anywhere and remain anonymous (Oba, 2004). A combination of both physical terrorism and cyber terrorism is thought to be the most effective use of cyber terrorism. For example, disrupting emergency services in which the emergency was created by physical terrorism would be a very effective way to combine both. The possibilities created for cyber terrorism by the use of technology via the Internet are vast. Government computer networks, financial networks, power plants, and so forth, are all possible targets as terrorists may identify these as the most appropriate features to corrupt or disarm in order to cause the most havoc. Manipulation of systems via software with secret "back doors," theft of classified files, erasing data, rewriting Web pages, introducing viruses, and so forth, are just a few examples of how terrorism can penetrate secure systems. Terrorist attacks made possible by the use of computer technology could also be demonstrated via air traffic control hijacking systems, or corrupting power grids from a remote destination (Gordon & Loeb, 2005).

Terrorist groups are increasingly using new information technology (IT) and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. In his statement on the worldwide threat in the year 2000, Director of Central Intelligence, George Tenet testified that terrorist groups, "including Hezbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization were using computerised files, e-mail, and encryption to support their operations." Convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy U.S. airliners on encrypted files on his laptop computer (Kosloff, Moore, Keller, Manes, & Shenoi, 2002, p. 22).

Terrorist organizations also use the Internet to target their audiences without depending on overt mechanisms such as radio, television, or the press. Web sites are presented as a way of highlighting injustices and seeking support for political prisoners who are oppressed or incarcerated. A typical site will not reveal any information about violent activities and will usually claim that they have been left with no choice but to turn to violence. They claim they are persecuted, their leader's subject to assassination attempts and their supporters massacred. They use this tactic to give the impression they are weak, and they portrait themselves as the underdog (Berinato, 2002). This public relations exercise is a very easy way of recruiting supporters and members. Alongside the propaganda aspect terrorists often present Web sites withinformation on how to build chemical and explosive weapons. This allows them to identify frequent users who may be sympathetic to their cause and therefore it is a cost effective recruitment method. It also enables individuals who are acting on their own to engage in terrorist activity. In 1999, a terrorist called David Copeland killed 3 people and injured 139 in London. This was done through nail bombs planted in three different locations. At his trial it was revealed the he used the *Terrorist Handbook* (Forest, 2005) and *How to Make Bombs* (Bombs, 2004) which were simply downloaded from the Internet.

CYBER TERRORIST ATTACKS

Terrorists use cyber space to cause disruption. Terrorists fight against governments for their cause, and they use every means possible to get what they want. Cyber attacks come in two forms; one against data, the other, control systems (Lemos, 2002). Theft and corruption of data leads to services being sabotaged and this is the most common form of Internet and computer attack. Attacks which focus on control systems are used to disable or manipulate physical infrastructure. For example, the provision of electrical networks, railroads, or water supplies could be infiltrated to have wide negative impacts on particular geographical areas. This is done by using the Internet to send data or by penetrating security systems. These weak spots in the system were highlighted by an incident in Australia in March 2000 where a disgruntled employee (who failed to secure full-time employment) used the Internet to release 1 million litres of raw sewage into the river and coastal waters in Queensland (Lemos, 2002).