Cyber-Terrorism in Australia

Christopher Beggs
Monash University, Australia

INTRODUCTION

Cyber-terrorism has evolved as a new form of terrorism since the development of new information and communication technologies (ICTs) such as the Internet. It has become an issue of concern to the Australian government as well as a global issue since the impact of the September 11, 2001, tragedies, the Bali bombings in 2002, and the London bombings of 2005. Australia, together with other leading nations such as the U.S., currently faces the threat of conventional terrorism; however, we also now face the possibility of a new digital form of terrorism: cyber-terrorism. This article explores this new form of terrorism and provides examples of possible cyber-terrorism and closely related cases. It also highlights vulnerabilities within Australian computer systems and provides an overview of the future trends of this new emerging threat within the Australian context.

CYBER-TERRORISM DEFINED

There are varying definitions of cyber-terrorism. Dorothy E. Denning, during her appearance before the U.S. Special Oversight Panel on terrorism, described it as:

...the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. (Denning, 2000)

Similarly, Sofaer (2000, p. 32) suggests that cyber-terrorism is the "international use or threat of use, without legally recognized authority, of violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder or significant economic harm." Lewis (2002, p. 1) takes this definition one step further, claiming that cyber-terrorism is "the use of computer network tools to shut down critical infrastructure such as energy, transportation, government operations or to coerce or intimidate a government or civilian population."

The author defines cyber-terrorism as the use of ICTs to attack and control critical information systems with the intent to cause harm and spread fear to people, or at least with the anticipation of changing domestic, national, or international events (Beggs, 2005, p. 1). For example, penetrating a system controlling gas pressure in a gas plant by manipulating the pipeline and causing an explosion would be classified as cyber-terrorism.

It is important to note that cyber-terrorism is not the same as hacking, even though they are closely related. Hacking generally involves a hacker taking a delight in experimenting with system hardware, software, and communications systems in an attempt to gain unauthorized access into a computer system. Unlike the cyber-terrorist, a hacker does not spread fear or cause harm to people, rather he/she demonstrates his/her prowess, as well as revealing the fallibility of computer security (Warren, 1999). According to Warren (1999), both hackers and cyber-terrorists utilize an arsenal of techniques in order to breach the security of the targeted system. However, from a motivation perspective, a cyber-terrorist is different in that he/she operates with a specific political or ideological agenda to support his/her activities. For example, a cyber-terrorist may attack specific systems or infrastructures such as water, gas, and power in an attempt to cause or spread harm to innocent people.

Also it is important to note that cyber-terrorism is different from information warfare. Janczewsk and Colarik (2005) suggest that information warfare attacks are planned by nations or by agents. These types of attacks are against information and computer systems, programs, or data that result in enemy losses.

The major difference between the two concepts is that cyber-terrorism is about causing fear and harm to anyone in the vicinity such as bystanders, while information warfare has a defined or declared target in a war. For example, if two nations launch cyber-based attacks against each other in efforts to destroy data or infrastructure, this type of attack would be classified as information warfare. On the other hand an attack against an infrastructure that spread fear and harm to innocent people within a community would be classified as cyber-terrorism.

CYBER-TERRORISM: POSSIBLE SCENARIOS

Rapid technological developments based on the Internet and other information infrastructures create an attractive environment for groups who cannot directly confront the Australian government, yet are willing to use death, destruction, and disruption to achieve their objectives. Increasingly, a cyber-terrorist (a person with malicious intent using ICT to spread fear or harm to civilians) can achieve impact in Australia from nearly anywhere around the globe. Terrorist groups such as Al-Qaeda can access global information infrastructures owned and operated by the government and corporations they want to target. Therefore digital attacks have a wide variety of means to cause disruption or destruction (Rattray, 2000). For example, the more developed a country becomes, the greater the vulnerability in the area of ICT. Terror attacks against communication systems are relatively easy to implement. The means required for these attacks are not particularly costly, and after the act the perpetrators are difficult to find (Schweitzer, 2003).

Cyber-terrorists can exploit vulnerabilities through achieving unauthorized access and control over a targeted system through a vast array of intrusive tools and techniques, commonly referred to as hacking. Means for successful intrusion range from comprised passwords to sophisticated software for identifying and exploiting known vulnerabilities in operating systems and application software. If control over a targeted computer or network is achieved, a cyber-terrorist could inflict a wide range of destruction. Possibilities could range from the changing of graphics on a Web page, to corrupting the delivery schedules for medical supplies or military equipment, or denying access to 000 (emergency) services, air traffic control data, or disrupting telecommunication networks. A main advantage of intrusion for cyber-terrorism is the ability of tight control over the timing of the attack (Rattray, 2000). For example, if a cyber-terrorist was to change the flight path of an aircraft, this change could be made with precision because of the electronic magnitude of the tools being used.

Cyber-space presents countless opportunities to commit acts that cause significant disruption to society without discreet loss of life, injury, or harm to material objects. For example, digital attacks might cause stock market disruptions by denying service to computer and communication systems. This analysis of cyber-terrorism includes both acts that involve physical violence and those causing significant social disruption based on attacking information systems and infrastructure (Rattray, 2000).

Collin (2000) highlights the following examples of potential cyber-terrorist acts:

- Attacking an aircraft control system, causing two planes to collide
- Altering the formulas of medication at pharmaceutical manufacture, causing several lethal dosages
- Changing the pressure in the gas lines causing a valve failure, resulting in an explosion
- Contaminating water supplies, causing many deaths
- Attacking the share market, causing economic chaos and disrupting the economy
- Attacking electrical power supplies, causing blackouts

There are many more possible examples of cyber-terrorism, however it should be noted that many cyber-terrorist attacks would generally aid conventional terrorism. For example, if a bomb was to be exploded in the Rialto building in Melbourne, Australia in conjunction with a cyber-attack such as blocking the emergency phone lines (000) and disabling power supplies in the CBD, the number of casualties would be increased, because rescue teams could not assist wounded casualties. Such an attack would support the terrorists' motives and goals.

Lewis (2005) claims that if cyber-terrorism occurred, it would be possible to coincide with a conventional attack. He claims that these types of multiple