Chapter VI
Terrorism and the Internet

M. J. Warren
Deakin University, Australia

ABSTRACT

The new millennium has had a major impact, the world in which we live is changing. The information society is becoming a global society, the growth of electronic businesses is developing new industrials markets on a global basis. But the information society is built on a very fragile framework—the Internet. The Internet is at risk from attacks, historically it was sole hackers, but we are now seeing the development of cyber terrorist organisations. This chapter will explore the ways in which terrorist organizations use the Internet and builds upon a number of case studies focusing upon the middle east.

INTRODUCTION

Many aspects of our modern society now have either a direct or implicit dependence upon information technology (IT). As such, a compromise of the availability or integrity in relation to these systems (which may encompass such diverse domains as banking, government, health care, and law enforcement) could have dramatic consequences from a societal perspective.

In many modern business environments, even the short-term, temporary interruption of Internet and e-mail connectivity can have a significantly disruptive effect, forcing people to revert to other forms of communication that are now viewed as less convenient. Imagine, then, the effect if the denial of service was over the long-term and also affected the IT infrastructure in general. Many governments are now coming to this realisation.

The term terrorist or terrorism is a highly emotive term. But the general term, terrorist, is used to denote revolutionaries who seek to use terror systematically to further their views or to govern a particular area (Wilkinson, 1976).

Cyber terrorism is a different form of terrorism since physical systematic terror does not occur (unless, for example, the attack causes a critical system to fail),

but systematic wide spread destruction of information resources can occur. The problem relates to the fact that a terrorist group could easily be perceived as a resistance group carrying out lawful actions. In the context of this chapter all groups will be defined as terrorist/resistance groups in order to give a neutral perception of their activities and aims.

This chapter sets out to consider the scenario in which technology infrastructures or services are targeted deliberately by "cyber terrorists."

THE CYBER TERRORIST

Recent years have seen the widespread use of information technology by terrorist-type organisations. This has led to the emergence of a new class of threat, which has been termed *cyber terrorism*. This can be viewed as distinct from "traditional" terrorism since physical terror does not occur and efforts are instead focused upon attacking information systems and resources. (Hutchinson & Warren, 2001).

When viewed from the perspective of skills and techniques, there is little to distinguish cyber terrorists from the general classification of hackers. Both groups require and utilise an arsenal of techniques in order to breach the security of target systems. From a motivational perspective, however, cyber terrorists are clearly different, operating with a specific political or ideological agenda to support their actions. This in turn may result in more focused and determined efforts to achieve their objectives and more considered selection of suitable targets for attack. However, the difference does not necessarily end there and other factors should be considered. Firstly, the fact that cyber terrorists are part of an organised group could mean that they have funding available to support their activities. This in turn would mean that individual hackers could be hired to carry out attacks on behalf of a terrorist organisation (effectively subcontracting the necessary technical expertise). In this situation, the hackers themselves may not believe in the terrorist's "cause," but will undertake the work for financial gain (Verton, 2003).

Propaganda and Publicity

Terrorist groups have difficulty in relaying their political messages to the general public without being censored: They can now use the Internet for this purpose. Different terrorist groups and political parties are now using the Internet for a variety of different purposes. Some examples are:

- **Tupac Amaru Revolutionary Movement (MRTA):** In 1997, a Peruvian terrorist group know as MRTA took over the Japanese embassy in Peru taking a number of hostages. During this time, the Web Site of the MRTA contained messages from MRTA members inside the embassy as well as updates and pictures of the drama as it happened.
- **Chechen rebels:** Chechen rebels have been using the Internet to fight the Russians in a propaganda war. The rebels claimed to have shot down a Russian fighter jet, a claim refuted by the Russians until a picture of the downed jet was shown on www.Kavkaz.org, the official Web site of the Chechen rebels. The Russians were forced to admit their jet had in fact been shot down.
- **Fundraising:** Azzam Publications, based in London and named after Sheikh Abdullah Azzam, a mentor of Osama bin Laden; is a site dedicated to Jihad around the world and linked to Al Qaeda. It is alleged that the Azzam Publications site, which sold Jihad related material from books to videos, was raising funds for the Taliban in Afghanistan and for guerrillas fighting the Russians in Chechyna. After September 11, Azzam Publications came under increased pressure to the point where its products could no longer be purchased through their site. In a farewell message published on their site they