



## **Chapter XXII**

# **The Use of the Internet by Terrorists and its Impact upon Electronic Commerce**

Matthew Warren  
Deakin University, Australia

William Hutchinson  
Edith Cowan University, Australia

### **INTRODUCTION**

In the developed world, the influence of information systems can now be seen in most operational areas of business. A significant result of these advances is that organizations have become increasingly dependent upon the availability of systems and reliant upon the data that they hold.

In recent years the Internet has grown from a solely military/academic network to one that can be used by business or individuals. In the years since the first WWW applications were developed, there has been an explosion in the global use of the Internet. With this growth has come an increasing usage of the medium by criminal and terrorist groups (Rathmell, 1997).

The term terrorist or terrorism is a highly emotive term. Generally it is used to denote “revolutionaries who seek to use terror systematically to further their views or to govern a particular area” (Warren, 1998). ‘Cyber-terrorism’ is a different form of terrorism since physical systematic terror does not usually occur (although it can if it causes disruption to a critical system), but a widespread destruction of information resources can. The problem of defining the term ‘terrorist’ relates to the fact that a terrorist group could easily be perceived as a resistance group carrying out lawful or morally legitimate actions. In the context of the chapter the term cyber-terrorist/terrorism will refer to all terrorist/resistance groups in order to give a neutral perception of their activities and aims.

Another new term related to the Information Society is ‘electronic commerce.’ The notion of ‘electronic commerce’ is proposed as a means of drawing together a wide range of business support services. It includes such elements as inter-organizational e-mail; on-line directories; trading support systems for commodities, products, customised products and custom-built goods and services; ordering and logistic support systems; settlement

support systems; and management information and statistical reporting systems (Warren et al, 1999).

Business around the world has become more of a target of cyber terrorism due to the fact that they are increasingly dependent upon information technology (Howard, 1997). Therefore there are many more high technology targets to prey upon. Increasingly in the future, businesses will use electronic commerce and on-line systems as a method of conducting trade. These on-line methods are very vulnerable to attacks. In a recent, informal survey of Australian IT managers (Hutchinson and Warren, 1999), 80% of replies said that their sites had never been attacked, 66% do not feel their competitors would attack their site, and 66% had no policy about dealing with an attack.

This chapter will explain why and how cyber-terrorists attack these services. The aims of the chapter are to:

- describe the background of cyber-terrorism;
- describe what cyber-terrorism is;
- describe the vulnerabilities of electronic commerce to cyber-terrorism;
- discuss the future of electronic commerce and cyber-terrorism.

## **DEVELOPMENT OF CYBER-TERRORISM AND CURRENT STATUS**

The term 'information warfare' (IW) is used in the context of cyber-terrorism. One definition of IW is that it relates to the struggle for control over information activities. The reason for the IW's recent rise to prominence is the perception that human activities are now much more reliant on information than in the past. Therefore, these information activities are a more tempting and significant target than in the past (Rathmall, 1998). Offensive information warfare operations produce win-lose outcomes by altering the availability and integrity of information resources to the benefit of the offence and to the detriment of the defence (Denning, 1999).

The term 'cyber-terrorist' is a recent addition to the computer security vocabulary and is used to describe a number of different individuals and groups. The convergence of the new technological and socio-political trends suggests that cyber-terrorism may be the terrorist activity of the future. If warfare is going to be conducted in cyber-space and if the combatants of the future are going to be irregulars, then cyber-terrorism is the logical paradigm of future conflict (Schwartau, 1996). Cyber-terrorists will be the 'irregular troops' of future cyber-wars, as they will attack what they see as more accessible targets. Cyber-terrorists will attack electronic commerce systems, since they will represent an easier target than conventional government or military systems. In the future this will result in some dramatic occurrences and will make the computer security sector re-think its strategy towards cyber-terrorist attacks.

## **CYBER TERRORISTS ON THE INTERNET**

We are now facing a situation where terrorist/resistance groups are now developing Internet sites and using Internet technologies. At the moment, the areas where terrorist/resistance groups are using the Internet consist of:

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/use-internet-terrorists-its-impact/9644](http://www.igi-global.com/chapter/use-internet-terrorists-its-impact/9644)

## Related Content

---

### Loyalty Differences in the Effect of Negative Critical Incidents and Quality Attributes Satisfaction: An Empirical Study of Online Shopping

Kwoting Fang, Ya-Yueh Shih and Duen-Ren Liu (2004). *E-Commerce and M-Commerce Technologies* (pp. 185-206).

[www.irma-international.org/chapter/loyalty-differences-effect-negative-critical/8926](http://www.irma-international.org/chapter/loyalty-differences-effect-negative-critical/8926)

### Measuring the Value of Refining a Web Presence

Raquel Benbunan-Fich and Eliezer M. Fich (2005). *Journal of Electronic Commerce in Organizations* (pp. 35-52).

[www.irma-international.org/article/measuring-value-refining-web-presence/3449](http://www.irma-international.org/article/measuring-value-refining-web-presence/3449)

### The Virtual Agency as a New Force in the Promotions Industry

R. Zachary Finney and Angeline Grace Close (2008). *Electronic Commerce: Concepts, Methodologies, Tools, and Applications* (pp. 2240-2246).

[www.irma-international.org/chapter/virtual-agency-new-force-promotions/9617](http://www.irma-international.org/chapter/virtual-agency-new-force-promotions/9617)

### Development and Testing of an E-Commerce Web Site Evaluation Model

Luiz A. Joia and Luiz C. Barbosa de Oliveira (2008). *Journal of Electronic Commerce in Organizations* (pp. 37-53).

[www.irma-international.org/article/development-testing-commerce-web-site/3515](http://www.irma-international.org/article/development-testing-commerce-web-site/3515)

### Inter-Organizational IT Capability in China: An Empirical Analysis of Dimensions and Influences

Jinnan Wu, Lin Liu, Nianxin Wang and Zhining Wang (2012). *Journal of Electronic Commerce in Organizations* (pp. 56-71).

[www.irma-international.org/article/inter-organizational-capability-china/72898](http://www.irma-international.org/article/inter-organizational-capability-china/72898)