Chapter 32

Cyber Terrorism Taxonomies:
Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies

Ali Al Mazari
Alfaisal University - Jeddah, Saudi Arabia

Ahmed H. Anjariny
Alfaisal University - Jeddah, Saudi Arabia

Shakeel A. Habib
Alfaisal University - Jeddah, Saudi Arabia

Emmanuel Nyakwende
Alfaisal University - Jeddah, Saudi Arabia

ABSTRACT

The aim of this paper is to identify common features in: the definition of cyber terrorism, cyber terrorism targets, cyber terrorism crimes and then develop effective mitigation strategies and countermeasures to tackle this phenomenon. Through rigorous analysis of literature covering academic articles and official reports, we develop cyber terrorism definition taxonomy which includes five elements: target, motive, means, effect and intention; cyber terrorism targets taxonomy identified from the following target areas: military forces, government cyber and physical infrastructures, critical national infrastructures, social and national identity, and private industry and entities. The cyber terrorism risk factors are classified into main five categories: national security, financial, social and cultural, operational disruption and physical destructions risks. The following identified patterns constituted the cyber terrorism targets taxonomy: incursion, destruction, service interruption, disinformation and web sites defacement. The authors categorized effective strategic approaches to tackle cyber terrorism as: administrative, technological, national and local alliances, international alliances, and education, training and psychological approach. They developed cyber terrorism taxonomies which represent a systematic organization and classification of knowledge that improves scientific awareness of cyber terrorism definition, boundaries, potential targets, crime patterns and effective mitigation strategies.

DOI: 10.4018/978-1-5225-5634-3.ch032

INTRODUCTION

The UK Government predicted that there would be more interconnected electronic devices on the planet than living humans by 2015 (UK-Government, 2010). The average of computing capacities at homes by 2030 would be one million times greater than what humans had in 2010 (US-JFC, 2010). In this cyber world, a wide range of critical national, military, governmental and private infrastructures are becoming vulnerable to cyber-attacks because they still rely on outdated conventional security solutions with no comprehensive and sophisticated cyber protection measures (Dogrul, Aslan, & Celik, 2011). Cyber-crimes, Cyber Terrorism and Cyber Warfare are now popular topics in the cyber environment or domain. Physical terrorism and cyber terrorism have been reported to share same key elements and a common denominator, i.e., terrorism (Flemming & Stohl, 2000). Cyber terrorism, however, remains a nebulous concept with lots of debates in terms of its definition, aims, risks, characteristics, deterrence strategies and other attributes (DCSINT, 2006). Existing deterrent and mitigation cyber terrorism models have not managed to contain cyber terrorism as it is still listed as one of the highest priority risks to national security in all countries (FBI, 2012; Macdonald, Jarvis, & Chen, 2013). Cyber terrorism is evolving due to the availability of low cost and effective development tools for the cyber terrorists to conduct attacks and cause damages to their targets (Jalil, 2003).

This paper contributes to cyber terrorism body of knowledge by developing cyber terrorism taxonomies. These taxonomies are crucial in this domain as they work as a systematic knowledge organization, and as a tool for the classification and presentation of attributes and features of cyber terrorism targets, risks and mitigation strategies.

CYBER-TERRORISM DEFINITION

Cyber terrorism is a new phenomenon or form of cybercrime which has its own aims, characteristics and other attributes (DCSINT, 2006). The concept of cyber terrorism has been defined differently by researchers and industry reporters. In the early eighties, cyber terrorism was seen as a combination of the physical and cyber world threats involving online computer and network interactions where users can exchange information in a real time (Samuel, Osman, Al-Khasawneh, & Duhaim, 2014). Cyber terrorism was defined as shutdown due to attacks on critical national infrastructures or intimidation of civilians or governmental employees, with the use of computer networks and technologies (Lewis, 2002). Cyber terrorism was also seen as unlawful attacks against computers, communication networks, information systems and stored information with the purpose of intimidating a government or its people in furtherance of political or social objectives. The attacks resulted in violence against individuals, groups or properties, or harm which generated fear (Denning, 2000).

Cyber terrorism was also defined as an electronic attack from cyberspace conducted using internal and external networks with different motives and directed at a particular target (Warren, 2002). This definition highlights the source of the attack which can be from inside or outside an organization. It has been reported that attacks are much more dangerous when done by insiders as internal terrorists have considerable access to the networks and systems as employees (Jalil, 2003). The US Federal Bureau of Investigation (FBI) defines cyber terrorism as a criminal act perpetrated by the use of computer systems and telecommunication networks causing violence, destruction and/or disruption of services to create fear due to confusion and uncertainty within a given group or population, with the goal of motivating a