Chapter 10
Cyberterrorism:
Using the Internet as a Weapon of Destruction

Leevia Dillon
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

ABSTRACT

The cyber threat landscape has continued to evolve with time and enhanced technology. With the advent of new breeds of terrorists and cybercriminals, the cyberterrorism debate has again wielded global attention. In this chapter, the author will attempt to delve deeper into the concept of cyberterrorism. Firstly, it will discuss the related issues which include the definition consensus, perception, and media abuse problems. The next section draws on parallels from research on cyber threats and terrorism based on six themes (i.e., modus operandi, domain, targets, impact, antagonists and motivations) to formulate a cyberterrorism conceptual framework. The third section will provide a hypothetical four-step cyberterrorism attack sequence and suggestions for countering cyberterrorism. This chapter will then conclude by highlighting several implications of interest.

INTRODUCTION

The rapid progression of new technological advancements and its concomitant benefits has brought about a digital era in which people are so deeply embedded in. This is even more so with the advent of social media. However with such innovations, security vulnerabilities that can be exploited by individuals (i.e., equipped with the necessary systems and human manipulation skills) are inevitably introduced into the systems (Dillon, Neo, Ong, & Khader, 2015; Furnell & Warren, 1999). In other words, manipulations of the systems and/or the human operators are the common modus operandi used to execute cyber threats. Cyber threats are potential online events that may cause detrimental outcomes (e.g., massive payouts, reputational concerns, loss of lives, severe economic damages) to individuals, organisations, and countries (World Economic Forum, 2012).

Research has highlighted two types of cyber threats: non-kinetic and kinetic (Applegate, 2013). Non-kinetic threats do not precipitate violence but undermine confidentiality, integrity and availability of

DOI: 10.4018/978-1-5225-7912-0.ch010

data. The cyber espionage campaigns conducted by 'The Mask' would be an example that falls under this category. The Mask is a digital tool (*Careto* in Spanish slang, meaning 'ugly face' or 'mask') designed by Spanish-speaking perpetrators with the sole objective of conducting international cyber espionage. This tool was involved in such operations since 2007 ("Mask malware takes", 2014). Examples of its operations include web and Wi-Fi traffic interceptions, keystroke and Skype conversations monitoring, obtaining information from Nokia devices (Warren, 2014).

The main targets of The Mask fell into several categories amongst which were government institutions, diplomatic embassies, research institutions and critical infrastructure involving energy, oil and gas. Its targets included the regions of the Middle East, Europe, Africa, and North and South America. Of note, its operations ceased shortly after the publication of 'The Mask' by Kaspersky Lab, an international cybersecurity organisation (Warren, 2014). The discovery and global reach of this tool led the U.S. President Barack Obama to declare cyber threats as the next pronounced threat to national security (Harress, 2014). This example highlighted the problems with the interconnectivity brought about by advancements in online technology as physical limitations imposed by geographical boundaries become increasingly irrelevant (Dillon et al., 2015). Fortunately, there were no reported damage or injuries but it is not hard to imagine that such a tool can be used to achieve kinetic effects (Applegate, 2013).

Kinetic cyber threats result in violence or deaths through not only the exploitation of data but also of critical infrastructure. An example of which is cyberterrorism, which will be the main focus of this chapter. Though met with scepticism (see CATO Institute, 2010; Conway, 2002; Green, 2002), cyberterrorism can be a possible future threat due to the following reasons:

- The financial capabilities of terrorist organisations like Al-Qaeda (AQ) or the Islamic State in Iraq and Syria (ISIS) may enable the respective organisations to potentially purchase equipment and expertise required to execute cyber threats (Hardy & Williams, 2014; Paganini, 2012; Sherlock, Samaan, & Samaan, 2014);
- The growing interdependencies between and within critical infrastructures of a nation (Acharya, 2004; Idaho National Laboratory, 2006; Zimmerman, 2009); and
- The documented isolated cases of critical infrastructure breaches (Applegate, 2013; Dillon et al., 2015).

The objective of this chapter will present cyberterrorism as a potential threat faced by authorities. The next section of this chapter will discuss several features of cyberterrorism by exploring similarities from research on cyber threats and terrorism to determine a conceptual framework encompassing cyberterrorism. This will be followed by an outline of a hypothetical sequence of a cyberterrorism attack and suggestions for countering cyberterrorism. The chapter will then conclude by delineating several implications about cyberterrorism.

ISSUES SURROUNDING CYBERTERRORISM

The term cyberterrorism took root in 1980s by Barry Collin who had argued the term signified the combination of the physical world and cyberspace (Collin, 1997). The usage of this term gained traction during the post-Cold War period where national security was undergoing dramatic changes. During this period, the introduction of the Internet provided a global platform for people to connect with one another