Chapter 73
Battlefield Cyberspace: Exploitation of Hyperconnectivity and Internet of Things

Maurice Dawson
University of Missouri – St. Louis, USA

Marwan Omar
Saint Leo University, USA

Jonathan Abramson
Post University, USA

Brian Leonard
Alabama A&M University, USA

Dustin Bessette
National Graduate School of Quality Management, USA

ABSTRACT

The threat of cyber terrorism has become a reality with recent attacks such as Stuxtnet, Flame, Sony Pictures, and North Korea's websites. As the Internet of Things (IoT) continues to become more hyperconnected it will be imperative that cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, embedded systems, and even wearable displays. The futures of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from exploitation of vulnerabilities it is essential to understand current and future threats to include the laws that drive their need to be secured. Examined within this chapter are the potential security related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality.

DOI: 10.4018/978-1-5225-5469-1.ch073

BACKGROUND ON RESEARCH

For years, experts and government officials have warmed of cyber terrorism as a threat to nation security (Cavelty, 2008). These malicious attacks can affect one single person to entire government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications, which track system weaknesses and vulnerabilities. As the United States government has stated, an act of cyber terrorism is an act of war; it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

Information assurance (lA) is defined as the practice of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation. This definition also encompasses disaster recovery, physical security, cryptography, application security, and business continuity of operations. To survive and be successful, an enterprise must have a disaster recovery strategy and response plan in place to mitigate the effects of natural disasters (e.g., floods, fires, tornadoes, earthquake, etc.), inadvertent actions by trusted insiders, terrorist attacks, vandalism, and criminal activity. In order to lay the groundwork for this review properly, it is essential to detail current processes techniques being utilized by officials within the government to accredit and certify systems to include their TA enabled products (Dawson, Jr., Crespo, & Brewster, 2013).

Cyber security has become a matter of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years, the number of attacks on United States networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The United States (U.S.) and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

ln Estonia and Georgia there were direct attacks on government cyber infrastructure (Beidleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the development of cyber defense organizations that drive laws and policies within Europe.

LAWS AND POLICIES TO COMBAT TERRORISM

The events of 9/ll not only changed policies with the U.S. but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security.