Chapter 71
Mitigating Unconventional Cyber-Warfare:
Scenario of Cyber 9/11

Ashok Vaseashta
Norwich University Applied Research Institutes, USA & Molecular Science Research Center, USA

Sherri B. Vaseashta
Trident Technical College, USA

Eric W. Braman
Norwich University Applied Research Institutes, USA

ABSTRACT

Advances in S&T coupled with universal access to cyberspace have motivated both state and non-state sponsored actors to new levels in the development of novel and non-traditional modes of attack to coerce, disrupt, or overthrow competing groups, regimes, and governments using unconventional warfare strategies. Threat vectors, caused directly or indirectly are asymmetric, kinetic, and unconventional. Current national and defense strategies in Cyberspace are mostly reactive and defensive, rather than pro-active and offensive. The web-crawlers research innovative ways to target security breaches. Securing critical infrastructure requires a top tier protection. This chapter is focused on ways to understand and combat unconventional warfare in cyber-space from CIS standpoint. This is crucial in avoiding a potential Cyber 9/11. To provide accurate intelligence, surveillance, preparedness and interdiction of such combative postures, ongoing studies of the ways that advance S&T may be employed so as to remain aware, alert and proactive for any/all such contingencies of use, are advocated.

1. INTRODUCTION

The geopolitical landscape of the 21st century has become relatively complex, dynamic, and unpredictable than that in the previous century. Even with limited technological capabilities and unsophisticated operation procedures (USOP) and capabilities, adversaries and terrorists groups have demonstrated a strong resolve and interest to wage unconventional warfare (UW) against others. In fact, the unconven-

DOI: 10.4018/978-1-5225-5634-3.ch071

tional *modus operandi* of USOP of adversaries offers unforeseen challenges in developing effective countermeasures. Since there are no rules of engagement and standard operating procedures (SOP), our collective capability to engage in such a war theater is limited due to the lack of case studies, design/ development of best practices playbook on capacity building, and all-out preparedness for an "unknown" event. Furthermore, the rapid advances in both science and technology coupled with universal access to cyberspace have inspired both state and non-state sponsored actors to new levels of creativity in the development of novel and non-traditional modes of attack to coerce, disrupt, or overthrow competing groups, regimes, and governments using UW strategies. In a conventional battlefield, conventional ROE apply. However, the cyberspace theatre expands the battlefield without boundaries thus the threat vectors are asymmetric, kinetic, and unconventional, where the ROE are virtually unknown and non-existent.

Securing digital assets is an extremely difficult and strategic challenge worldwide that requires the latest technology, cooperation between the public and private sector, military and civilian education and training, and legal and policy framework (Vaseashta, Susmann, & Braman, 2014). Unfortunately, cyber-crime and cyber–terrorism are on the rise and the perpetrators operate in shadows and without boundaries. This is compounded by the fact that the world today relies on the interconnectivity and cyber-criminals exploit everyone's basic necessity for their own personal gain – may it be financial, vengeance, or gaining personal notoriety or thrills. The threat of a catastrophic cyber-attack is very real. Attacks are currently taking place and the annual cost of cyber-crime worldwide has climbed to more than $1 trillion globally." All aspects of our society have become increasingly dependent on the Internet, may it be personal, the government, the military or businesses - both small and large. While in most cases this powerful technology has transformed our daily lives for the better, unfortunately bad actors – from common criminals to foreign terrorists - have identified cyberspace as a realm for a *cyber-caliphate* that are (mis-) used as recruiting venues for the 21st century battlefield.

The New York Times reported that a speech delivered by United States Secretary of Defense Leon E. Panetta warned that

… the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government.

In another speech at the Intrepid Sea, Air and Space Museum in New York,

An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches.

Mr. Panetta said.

They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.

Mr. Panetta painted a dire picture of how such an attack on the United States might unfold, while reacting to increasing aggression and technological advances by the nation's top adversaries, which officials identified as China, Russia, Iran and several militant groups out of the middle-east. This opens