Chapter 10
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those that wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists there has been an overwhelmingly abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world. This chapter discusses emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

INTRODUCTION

Cyber security has become an important subject of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the early 90s users have exploited vulnerabilities to gain unauthorized access to networks for malicious purposes. In recent years the number of attacks on United States (U.S.) 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 U.S. and other countries have come to understand that this is

DOI: 10.4018/978-1-5225-5634-3.ch010

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

an issue and has developed policies to handle this in an effort to mitigate the threats (Dawson, Omar, & Abramson, 2015).

In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government's digital infrastructure useless (Dawson, Omar, & Abramson, 2015). The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the rapid development of cyber defense organizations throughout Europe which has raised the profile of cyber attacks to include awareness to the potential severity of attacks (Dawson, Omar, & Abramson, 2015).

MOBILE NETWORKS

Mobile networks are found in large cities in America to villages in West Africa. Thus the importance of security in mobile networking is essential to maintaining security and privacy for everyday citizens. Mobile devices have become the preferred device for web browsing, emailing, using social media and making purchases (Wright et al, 2012). Many individuals rely on their mobile devices for texting, checking email, making online purchases, and even remote controlling their home alarm system. Thus attackers have developed malware to specifically target these platforms. Understanding the Human Computer Interaction (HCI) and behavioral issues with mobile devices is a start in understanding human pitfalls in security.

DIGITAL CURRENCY

Digital currency has become a new commerce that is growly quickly and gaining the attention of large financial institutions. This crypto currency has been termed "memory" in monetary economics literature (Luther & Olson, 2013). Bitcoin is a peer to peer electronic cash system in which no one controls and there are not an associated printed currency(Nakamoto, 2008). Bitcoin allows for anonymity to occur in this peer to peer electronic currency systems (Reid & Harrigan, 2013). Some argue that the main benefits are lost if a trusted third party is necessary to prevent the action of double spending (Nakamoto, 2008). The technical infrastructure of this decentralized digital currency relies on several cryptographic technologies.

Luther and Olson state that the principle finding of the money and memory literature is that both devices are capable of facilitating exchange (Luther & Olson, 2013). What is missing from the literature is data concerning the use of Bitcoin for illicit activities. However some researchers attempt to assess potential damages and threats to national security, banking industry, child pornography, drug trade, financial fraud, and more. In relation to cyber warfare Bitcoin could pose as an enabler for plausible deniability of foreign governments and institutions for involvement in cyber attacks (Hilse, 2013). Further cyber criminals could store stolen digital funds on any device that can be used as storage (Hilse, 2013). This could pose a threat as laundered, stolen, or self generated funds can be taken anywhere on a storage device such as a micro Secure Digital (SD) that can hold up to 64 Giga Bytes (GB). This could pose an issue in terms of search and seizure of assets as many police forces have inadequate training and personnel to pull off such measures of cyber forensics on a large scale.

6 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/a-brief-review-of-new-threats-and-countermeasures-in-digital-crime-and-cyber-terrorism/203503

Related Content

Measuring the Progress of a System Development
Marta (Plaska) Olszewskaand Marina Waldén (2012). *Dependability and Computer Engineering: Concepts for Software-Intensive Systems (pp. 417-441).*
www.irma-international.org/chapter/measuring-progress-system-development/55337

Opportunities and Challenges in Porting a Parallel Code from a Tightly-Coupled System to the Distributed EU Grid, Enabling Grids for E-sciencE
Fumie Costenand Akos Balasko (2012). *Handbook of Research on Computational Science and Engineering: Theory and Practice (pp. 197-217).*
www.irma-international.org/chapter/opportunities-challenges-porting-parallel-code/60361

Mitigating Unconventional Cyber-Warfare: Scenario of Cyber 9/11
Ashok Vaseashta, Sherri B. Vaseashtaand Eric W. Braman (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 1415-1437).*
www.irma-international.org/chapter/mitigating-unconventional-cyber-warfare/203569

Ontology-Based Open Tourism Data Integration Framework: Trip Planning Platform
Imadeddine Mountasser, Brahim Ouhbi, Ferdaous Hdioudand Bouchra Frikh (2020). *AI and Big Data's Potential for Disruptive Innovation (pp. 44-70).*
www.irma-international.org/chapter/ontology-based-open-tourism-data-integration-framework/236334

Code Clone Detection and Analysis in Open Source Applications
Al-Fahim Mubarak-Ali, Shahida Sulaiman, Sharifah Mashita Syed-Mohamadand Zhenchang Xing (2018). *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications (pp. 1112-1127).*
www.irma-international.org/chapter/code-clone-detection-and-analysis-in-open-source-applications/192915