SSI
STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH—WISDOM

CYBER INFRASTRUCTURE PROTECTION
VOLUME III

Tarek Saadawi
John D. Colwell, Jr.

Editors

The Cyber Infrastructure Protection (CIP) colloquium for the academic year 2015-16 was focused on strategy and policy directions relating to cyberspace; and how those directions should deal with the fast-paced technological evolution of that domain. Topics addressed by the colloquia included: a cooperative international deterrence capability as an essential tool in cybersecurity; an estimation of the costs of cybercrime; the impact of prosecuting spammers on fraud and malware contained in email spam; cybersecurity and privacy in smart cities; smart cities demand smart security; and, a smart grid vulnerability assessment using national testbed networks.

The colloquium was organized into three main parts. Part I discusses policy, strategy, and cybercrime; Part II presents cybersecurity of smart cities; and Part III provides discussion on cyber infrastructure security and technical issues.

PART I: CYBERSECURITY POLICY, STRATEGY, AND CYBERCRIME

The first chapter recommends the establishment of an International Cyber Union (ICU) to monitor, collect, and verify international cyber-illegalities and hacks, take necessary legal actions, and provide a platform for international cooperation in the cyber domain. The ICU would be an international independent body that will oversee how to deal with addressing international cybercrimes, cyberattacks, cyberespionage, cybervandalism and sabotage, as well as cyberwarfare. It discusses the need to strengthen cybersecurity technologies with advanced mechanisms that help determine where attacks originate from and help identify the attackers' identities, as becoming increasingly vital to ensure uninterruptable use of cyberspace. In addition, this chapter touches on a potential new threat of using cyber as a weapon by states. This chapter also proposes an organizational model for the ICU that will lead to an increase in collaboration and trust amongst nations and minimize cybersecurity threats.

The second chapter focuses on limitations and possibilities of estimating the costs of cybercrime. Cybercrimes present a clear threat to individuals, industry, and government alike. The chapter discusses that there are, however, substantial limitations to our understanding of both the offenders and victims of this form of crime. The lack of knowledge is due in part to an absence of quantifiable data on both the number of incidents that occur, as well as the ways that victims must remediate and repair infections and attacks. There is also minimal research considering the labor and capital costs that offenders encounter when attempting to engage in cybercrimes, as well as their potential profits. This chapter will discuss these limitations as well as explore potential models to account for offender profits using various data sources. Finally, the implications of this chapter for public policy and research are examined in depth.

The third and final chapter in Part I focuses on malicious spam and the impact of prosecuting spammers for fraud and the malware contained in email spam. Spam can be more than just a nuisance; it can also be fraudulent and malicious. Spam is one of the most common attack vectors for perpetrators of fraud and distributors of malware. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN SPAM Act) is U.S. federal legislation that was passed in response to the growing spam problem. Current research suggests that prosecutions under the CAN SPAM Act appear to reduce overall spam volume, as well as increase certain types of spam law compli-

ance. However, it is uncertain to what degree of impact the CAN SPAM Act might have had on more serious forms of cybercrime contained in spam, such as malware and fraud. The chapter seeks to address this question by assessing the impact that prosecutions of spammers has had on a sample of 5,490,905 spam emails sent between 1998 and 2013. Machine learning and data mining techniques were used to build one measure of fraud and two measures of malware distribution contained in the spam sample.

PART II: CYBERSECURITY OF SMART CITIES

The fourth chapter presents cybersecurity and privacy issues that smart cities face. The development of smart cities has been a major global trend. From the perspective of a smart city, an obvious and alarming trend is that cyberattacks have been capable of causing physical damage to plants and equipment. This chapter identifies and analyzes the unique challenges faced by smart cities from the privacy and cybersecurity standpoint. Since big data is a key component of smart city initiatives, the chapter examines how various characteristics of big data are linked to privacy and cybersecurity in the context of smart cities. It also compares cyberattacks targeting smart cities and other forms of cyberattacks in terms of various criteria and parameters such as seriousness of threats, likely perpetrators and their modus operandi, and possible defense responses. The chapter also reviews how privacy issues in smart cities are shaped by enduring cultural models of privacy protection and the political discourses that revolve around this issue. Also discussed are implications for policymakers, developers of smart city technologies, residents of smart cities, and consumers. Overall the chapter argues that smart cities' overreliance on digital technologies would prove to be devastating to their economic and overall welfare in case of severe cyberattacks.

The fifth chapter argues that the smart city absolutely demands smarter security, even as we struggle to define what that means. The lack of a coherent approach toward the identification and remediation of attacks on nodes of security will only mean growth in open targets. The leadership of private and nongovernmental organizations, academies, and core governmental agencies are vital to building the foundations for protection. This must be embraced by all the entities and organizations of the city. This requires a strong political effort to implement and maintain a safe and secure smart city.

The sixth and final chapter in Part II deals with anticipating the nature and likelihood of a cyberterror community. Today, we see even more profound and unexpected effects of digital technology on our social world. In particular, one of the more interesting consequences of this technological progression is the formation of unique social communities centered on these emerging technologies. This chapter examines the mechanisms surrounding the appearance of specialized communities, technology-centered communities specifically, as well as investigating some of the unique characteristics that make these subpopulations a special interest to social scientists, as well as policymakers and information security professionals.

PART III: CYBER INFRASTRUCTURE SECURITY

The seventh and final chapter deals with smart grid vulnerability assessment using national test bed networks. In this chapter, we discuss the smart grid as part of the critical infrastructure of the energy sector; the chapter also assesses various smart grid vulnerabilities and provides a better understanding of the threats associated with them. Using the Defense Technology Experimental Research (DETER) Laboratory network test bed environment, the authors perform cyberattack scenarios and evaluate various vulnerabilities of smart grid protocols.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *ssi.armywarcollege.edu*.

*****

This Publication SSI Website USAWC Website