Executive Summary

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

CYBER INFRASTRUCTURE PROTECTION
VOLUME II

Tarek Saadawi
Louis H. Jordan, Jr.
Vincent Boudreau

The Cyber Infrastructure Protection conference for academic year 2010-11 focused on strategic and policy directions, and how these policy directions should cope with fast-paced technological evolution. Topics addressed by the conference attempted to answer some of these questions: How serious is the cyber threat? What technical and policy-based approaches best suit securing Telecommunications Networks and Information Systems Infrastructure security? What role will government and the private sector play in homeland defense against cyber attack on critical civilian infrastructure, financial, and logistical systems? What legal impediments exist to efforts to defend the nation against cyber attacks, especially in the realm of preventive, preemptive, and retaliatory actions?

The Colloquium was organized into three main sessions. Session 1 discussed the economic and social aspects of cyber security, covering the economics of malicious software and stolen data markets as well as the emergence of the civilian cyber warrior. Session 2 dealt with laws and cybercrime, covering social and justice models for enhanced cyber security, and provided an institutional and developmental analysis of data breach disclosure laws. Session 2 also provided solutions for critical infrastructure that protected civil liberties, enhanced security, and explored the utility of open source data. Session 3 presented the technical aspects of the cyber infrastructure and presented monitoring for Internet service provider (ISP) grade threats, as well as the challenges associated with cyber issues.

Part 1: Economics and Social Aspects of Cyber Security.

The first two papers provide a framework for the economic and social aspects of cyber security. The first paper explains how hackers utilize data from a sample of active publicly accessible web forums that traffic in malware and personal information. To explore and expand the understanding of the economics of cybercrime in general, this section utilized a qualitative analysis of a series of threads from publicly accessible Russian web forums. These forums facilitate the creation, sale, and exchange of malware and cybercrime services. The findings explore the resources available within this marketplace and the costs related to different services and tools. Using these economic data, coupled with loss metrics from various studies, this analysis considers the prospective economic impact of cybercrime campaigns against civilian and business targets. The findings provide insight into the market dynamics of cybercrime and the utility of various malware and attack services in the hacker community.

The second paper focuses on the civilian cyber warrior, who poses perhaps the most significant emerging threat to domestic and foreign critical infrastructures. The chapter provides some

basic background for a schema that outlines six motivational factors believed to encourage malicious online behaviors.

The key concept is that perhaps for the first time in history, a regular civilian can effectively attack a nation-state, in this case, through a cyber attack on some component of that nation-state's critical infrastructure. In this use, "effective" means that the attack can cause significant widespread damage, has a reasonably high probability of success, and a low probability of the perpetrator being apprehended. One of the first things that one might want to investigate in the chain of actions for a cyber attack is the initial starting point where individuals begin thinking about and rehearsing in their minds the nature, method, and target for the attack. Perhaps the key point of the historical and social significance of the emergence of civilian cyber warriors can be found in the social psychological significance of the event. The re-assessment of the usual assumptions of the inequalities of the levels of power between nation-states and citizens establishes new relationships between institutions of society, government, and individuals.

Part 2: Law and Cybercrime.

Part 2 of the colloquium explores the law and cybercrime. The first chapter argues that to change the game in cyber security, we should consider criminal justice and social education models to secure the highly distributed elements of the information network, extend the effective administration of justice to cybercrime, and embed security awareness and competence in engineering and common computer practice. Safety and security require more than technical protections and police response. They need a critical blend of those elements with individual practice and social norms. Social norms, matched with formal institutions, enhance public safety—including in the cyber realm. Informal and formal modes of controlling and limiting deviant behavior are essential for effective security.

The second chapter considers the state data breach disclosure laws recently enacted in most U.S. states. The state data breach disclosure laws are of interest because of the rapid growth of this policy. This is the first instance of informational regulation for information security. These laws are also important responses to identity theft and privacy, which are areas of growing concern.

Technological advancements are considerably changing the information security and privacy landscape. Yet, these policies are blunt instruments, which are not well suited for the careful excision of these ills. Some advocates who call for the modification of existing laws assert that the outcome of data breach disclosure should be to motivate large-scale reporting so that data breaches and trends can be aggregated, which allows a more purposeful and defensive use of incident data.

The third chapter addresses the problems of identity determination, which raises some of the most complicated unresolved issues in cyber security. Industry and government are pursuing a number of approaches to identify communicants in order to secure information and other assets. As part of this process, some policymakers have recommended fundamental changes to the way in which the Internet transmits identity information. Attribution is the analysis of information associated with a transaction or series of transactions to determine the identity of a sender of a stream of traffic. Information collection and analysis are the goals of attribution. This chapter focuses on authentication and attribution. Two issues that are closely related to identity and are critical elements of any secure system are authorization and auditing. The chapter considers these issues and concludes that authentication-oriented solutions are more likely to provide significant security benefits and less likely to produce undesirable economic and civil liberties consequences.

The fourth and final chapter of Part 2 focuses on the value of open reporting for malware creation and distribution. The author considers how this information may combine with other measures to explore the country-level economic, technological, and social forces that affect the likelihood of malware creation. The speaker proposes that online repositories containing data on malicious software can be valuable to study the macro-level correlates of malware creation.

The chapter concludes that the diverse and sophisticated threats posed by hackers and malicious software writers require significant investigation by both the technical and social sciences to understand the various forces that affect participation in these activities. The author suggests that there is a strong need for greater qualitative and quantitative examinations of hacker communities around the world. Research on hacker subcultures in the United States, China, and Russia suggests that there are norms, justifications, and beliefs that drive individual action.

Part 3: Cyber Infrastructure.

The first chapter is a comprehensive view of network security in light of several years of research conducted at Telcordia, focusing mainly on the problem of monitoring large-scale networks for malicious activity. The goal of the system that was developed is to detect various types of network traffic anomalies that could be caused by distributed denial-of-service (DDoS) attacks, spamming, IP address spoofing, and botnet activities. Currently three types of anomaly detectors are provided to collect data and generate alerts: (a) Volume Anomaly Detectors; (b) Source Anomaly Detectors; and (c) Profile Anomaly Detectors. The goal of source anomaly detectors is to identify instances of source IP address spoofing in observed flows. In this case, data for the monitored ISP is acquired via NetFlow/sFlow data feeds from three flow agents. The profile anomaly detectors are intended to detect any behavioral anomalies pertaining to hosts within the monitored network. One profile anomaly detector that is currently part of the system identifies potential spammers, which use flow data and spammer blacklists. The Telcordia system incorporates an efficient real-time volume anomaly detector designed to give early warning of observed volume anomalies. The volume anomaly detector operates by considering a near-term moving window of flow records when computing traffic volumes for a destination address. The system incorporates a correlation engine used to compare the relationship of alerts that are generated by the different types of anomaly detectors. A significant issue with many anomaly detection-based approaches is their potentially high false-positive rate. The correlation engine component is designed to reduce the possibility of generating false-positives. Finally, the use of an alert correlation component can be very valuable to a network operator who would be interested in lowering false-positive rates.

The goal of the final chapter is to explore the state-of-the-art in our ability to assess cyber issues. To illuminate this issue, the author presented a tentative decomposition of the problem into manageable subsets. Using that decomposition, the author identified potential cyber policy issues that warrant further analysis and identified and illustrated sample Measures of Merit (MoMs). Subsequently, participants discussed some of the more promising existing cyber assessment capabilities that the community is currently employing, and the author provides an identification of several cyber assessment capabilities that will be needed to support future cyber policy assessments. The chapter concludes with a brief identification of high priority cyber assessment efforts that warrant further action.

*****

This Publication

SSI Website

USAWC Website