ADVANCES IN INFORMATION SECURITY

Global Initiatives to Secure Cyberspace

An Emerging Landscape

Edited by

Michael Portnoy

Seymour Goodman

Springer

Global Initiatives to Secure Cyberspace

An Emerging Landscape

Advances in Information Security

Sushil Jajodia

Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SECURE KEY ESTABLISHMENTS by Kim-Kwang Raymond Choo; ISBN: 978-0-387-87968-0
SECURITY FOR TELECOMMUNICATIONS NETWORKS by Patrick Traynor, Patrick McDaniel and Thomas La Porta; ISBN: 978-0-387-72441-6
INSIDER ATTACK AND CYBER SECURITY: Beyond the Hacker edited by Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclaire, Sean W. Smith; ISBN: 978-0-387-77321-6
INTRUSION DETECTION SYSTEMS edited by Robert Di Pietro and Luigi V. Mancini; ISBN: 978-0-387-77265-3
VULNERABILITY ANALYSIS AND DEFENSE FOR THE INTERNET edited by Abhishek Singh; ISBN: 978-0-387-74389-9
BOTNET DETECTION: Countering the Largest Security Threat edited by Wenke Lee, Cliff Wang and David Dagon; ISBN: 978-0-387-68766-7
PRIVACY-RESPECTING INTRUSION DETECTION by Ulrich Flegel; ISBN: 978-0-387-68254-9
SYNCHRONIZING INTERNET PROTOCOL SECURITY (SIPSec) by Charles A. Shoniregun; ISBN: 978-0-387-32724-2
SECURE DATA MANAGEMENT IN DECENTRALIZED SYSTEMS edited by Ting Yu and Sushil Jajodia; ISBN: 978-0-387-27694-6
NETWORK SECURITY POLICIES AND PROCEDURES by Douglas W. Frye; ISBN: 0-387-30937-3

Additional information about this series can be obtained from http://www.springer.com

Global Initiatives to Secure Cyberspace

An Emerging Landscape

Edited by

Michael Portnoy
Georgia Institute of Technology
Atlanta, GA, USA

Seymour Goodman
Georgia Institute of Technology
Atlanta, GA, USA

Contributors:

Michael Portnoy, Kathleen Minor, Andrew Howard,
William Lee, Richard Givens, Irene Liscano,
Delphine Nain, Seymour Goodman

Springer

Editors:
Michael Portnoy
Georgia Institute of Technology
Georgia Tech Information Security Center
Sam Nunn School of Int'l Affairs
Center for International Strategy,
Technology, & Policy
781 Marietta St.
Atlanta GA 30332
mportnoy@gatech.edu

Seymour Goodman
Georgia Institute of Technology
Georgia Tech Information Security Center
Sam Nunn School of Int'l Affairs
Center for International Strategy,
Technology, & Policy
781 Marietta St.
Atlanta GA 30332
goodman@cc.gatech.edu

ISBN-13: 978-0-387-09763-3 e-ISBN-13: 978-0-387-09764-0

Library of Congress Control Number: 2008936298

Printed on acid-free paper

springer.com

Preface

As cyberspace continues to rapidly expand, its infrastructure is now an integral part of the world's economy and social structure. Given this increasing interconnectivity and interdependence, what progress has been made in developing an ecosystem of safety and security? This study is the second phase of an initial attempt to survey and catalog the multitude of emerging organizations promoting global initiatives to secure cyberspace.

The authors provide a breakdown and analysis of organizations by type, including international, regional, private-public, and non-governmental organizations. Concluding with a discussion of the progress made in recent years, the study explores current trends regarding the effectiveness and scope of coverage provided by these organizations and addresses several questions concerning the overall state of international cyber security.

The authors would like to thank Mr. Anthony Rutkowski for generously providing his time, guidance, and support. The authors would also like to thank the International Telecommunication Union (ITU) Telecommunication Development Sector (ITU-D) and the United States National Science Foundation (NSF Grant R3772) for partially supporting the research conducted in this study. In addition, the authors would like to thank the Georgia Institute of Technology’s Center for International Strategy, Technology, and Policy (CISTP) for assistance in hosting the Cyber Security Organization Catalog, and the Georgia Tech Information Security Center (GTISC) for cooperation and promotion of this study.

Table of Contents

1 The International Landscape of Cyber Security

Cyberspace – the "worldwide open IP-enabled network infrastructure for communications, commerce, and government" [1]– continues to expand rapidly. The average number of Internet users has increased an estimated 304 percent between 2000 and 2008 and is now quickly approaching 1.5 billion. The majority of relative growth has occurred in developing regions such as the Middle East, Africa, and Latin America, while close to half of the absolute growth has occurred in Asia.[2]

A function of this ever-increasing interconnectivity and interdependence, cyberspace has now become an integral part of the world's economy and social structure. Individuals, industry, and government all rely on information and communication technologies (ICTs) for a wide variety of needs, such as banking, electric power, emergency services, transportation, education, telecommunication, social networking, military operations, and critical infrastructure control.[3]

However, this substantial growth in cyberspace usage has not been accompanied by an adequate increase in security. In the nascent days of the Advanced Research Projects Agency Network (ARPANET), the predecessor of today's Internet, security was not a primary concern. Rather, leading computer scientists focused on developing network protocols with an openness that would allow many applications to be developed without constraint.[4] While this openness has generally resulted in many benefits, such as user-generated content, social networking, and e-commerce, cyberspace today is consequently plagued with a growing number of security vulnerabilities that can be, and often are, exploited by hackers, criminals, spies, terrorists, and even rogue nation states. Computer users in every domain are at risk for targeted computer attacks, identity theft, online fraud, spam, malware, denial of service, espionage, cyber terrorism, information warfare, and a growing number of other malicious cyber threats.

The ease of access, relative anonymity, and borderless nature of the Internet have allowed widespread computer-based crime – or cybercrime – to proliferate rapidly. Law enforcement and international security organizations, along with governments and the private sector, have only recently begun to appreciate the scope, severity and transnational nature of this problem. Additionally, with the dynamic growth and recent popularity of ICTs in developing countries around the world, these countries will likely experience a similarly steep learning curve in appreciating and combating this increasingly global proliferation of cyber threats.

In recent years, organizations have begun to emerge and evolve in a progressively collaborative ecosystem of vested international bodies seeking to address these challenges in unique, innovative ways. Such organizations today consist of international and regional telecommunication regulatory agencies, intergovernmental policymaking bodies, national homeland security agencies, regional law enforcement organizations, and various private-public and non-governmental organizations (NGOs) around the world. While many of these organizations are heavily focused on outreach, general education, and awareness-raising, some are also pursuing global collaboration, harmonization of statutory and regulatory provisions, and the development of incident readiness and response programs.[5]

This study attempts to address a series of questions regarding the current state of cyber security. What does the international landscape of cyber security look like today? What are these organizations actually doing? Are they succeeding? What measureable progress has been made in developing a supportive ecosystem of global cyber security? Are these organizations presenting practical, innovative, collaborative, and sustainable solutions to address these issues?

This study is the second phase of an initial attempt to survey and catalog the international, regional, private-public, and non-governmental organizations leading the global effort to secure cyberspace through local and regional policy initiatives, international harmonization of laws, basic research and technological innovation, law enforcement, education and training, incident response, and proliferation of secure ICTs.[6] This study focuses on categories of organizations which have to this date received little attention and exposure in the emerging international landscape of cyber security. Due to the sheer number of private organizations, national organizations, and infrastructure administration, maintenance, and operations organizations also active in the effort to secure cyberspace, the authors have chosen to omit discussion of these organizations at this time.

While the study currently catalogs approximately seventy organizations, it is by no means an exhaustive list. Only a dedicated research team can hope to maintain a comprehensive, up-to-date database of international cyber security organizations. Given the evolving nature of the Internet and global network infrastructures, as well as increasing public demand for information assurance and data privacy, the material in this study may very likely be out-of-date no sooner than the initial publication has been released. This study is also, by necessity, heavily reliant on information provided by the cataloged organizations' own websites, publications, articles, and meeting minutes from regional and international cybercrime conventions and public conferences. The authors invite readers to provide updates, corrections, omissions, and information on emerging organizations in order to continue and improve upon this repository.

To assist with forthcoming cataloging efforts, the authors of this book have collaborated to develop an initial web-based database of documented cyber security organizations. This catalog, which can be accessed online at http://www.cistp.gatech.edu/catalog/, is currently hosted by the Georgia Institute of Technology Center for International Strategy, Technology, and Policy (CISTP) and features a detailed description of each organization, including website links, relevant associations, and contact information. In addition, a full listing of abbreviations referenced throughout this book, as well as background and history of the current research initiative, can be accessed through the online catalog.

2 A Brief History of Global Responses to Cyber Threats

When the earliest implementations of packet switching networks were first developed by the United States government in the 1970s and early 1980s, certain researchers and computer scientists made substantial initial advances on securing these networks from cyber attacks and malicious exploits. However, as much of this research was conducted independently from the Advanced Research Projects Agency Network (ARPANET), many of these early ideas on network security and host authentication were neglected when ARPANET was transformed during the 1980s into what we call the Internet today. Following a 1983 study on the "possibility of an international application and harmonization of criminal laws to address the problem of computer crime and abuse," the Organisation for Economic Co-operation and Development (OECD, see Chapter 3) published *Computer-related Crime: Analysis of Legal Policy* in 1986.[7] The survey examined existing laws in member states, offered proposals for reforms, and recommended a "minimum list of abuses that countries should consider prohibiting and penalizing by criminal laws," attempting to serve as a common denominator between the different approaches taken by the member OECD countries.[8]

Following publication of the OECD report, the United Nations (UN, see Chapter 3) in 1990 adopted a resolution on computer crime legislation at its eighth Congress on the Prevention of Crime and Treatment of Offenders in Havana, Cuba.[9] This resolution was one of the first international efforts that addressed criminal laws related to computer crime. The resolution called upon member states to intensify their efforts to combat computer crime by modernizing national criminal laws, improving computer security and prevention measures, conducting adequate training, and collaborating on future efforts. Finally, the resolution called for the United Nations to promote international efforts in the development and dissemination of a comprehensive framework and standards that would assist the member states in dealing with computer-related crime.[10]

The first important international effort toward developing such a framework began in 1992 when the OECD issued *Guidelines for the Security of Information Systems and Networks*, intended for use by both the government and the private sector.[11] The framework document focused on nine principles: awareness, risk assessment, responsibility, response, security design and implementation, security management, reassessment, ethics, and democracy. The guidelines were reviewed in 1997 and 2001 by the OECD's Working Party on Information Security and Privacy (WPISP, see Chapter 3), and publication was accelerated in the aftermath of the September 11 attacks. The most recent guidelines were adopted in July 2002.[12]

In 2000, UN Resolution 55/63 was adopted by the General Assembly to combat the criminal misuse of information technology. Together with Resolution 56/121, passed in 2002, the UN called for the creation of measures to combat information technology misuse by stating: "…states should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies…" and "…legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure the criminal abuse is penalized." [13] UN Resolutions 57/239 (2002) and 58/199 (2004) were later adopted to create "a global culture of cybersecurity and the protection of critical information infrastructures." [14]

2.1 World Summit on the Information Society (WSIS)

In 2001, the UN General Assembly called for the creation of a World Summit on the Information Society (WSIS, the Summit) in Resolution 56/183, where both public and private industries could "…harness synergies and create cooperation among the various information and communication technologies initiatives, at the regional and global levels." The International Telecommunication Union (ITU, see Chapter 3) was selected to serve in a managerial role over the Summit. The World Summit was held in two phases: in Geneva in December 2003 and Tunis in November 2005.[15] Reports from each summit were produced, with the latest update published in June 2007.[16]

The objective of the Geneva phase was to develop and foster a clear statement of political will and develop a plan for the foundations of an "…Information Society for all…" and a general plan of action ("Geneva Action Plan"). Following the meeting, two major areas were seen as important, "…building confidence, trust and security…" and "…establishing stable regulatory frameworks." [17] The WSIS Declaration of Principles, emphasizing a common vision and key principles for the Information Society, stated that "strengthening the trust framework, including information security and network security, authentication, privacy, and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs." In order to achieve these objectives, a global culture of cyber security would need to be "actively promoted, developed, and implemented in cooperation with all stakeholders and international expert bodies." [18]

The ITU held a WSIS Thematic Meeting on Cybersecurity, hosted in Geneva from June 28 - July 1, 2005, to examine WSIS recommendations from the Geneva Summit (including the Action Plan and Declaration of Principles) related to building confidence and security in the use of ICTs and promotion of a global culture of cybersecurity. The meeting, open to all UN Member States, international organizations, WSIS accredited non-governmental organizations, ITU sector members, and civil society and accredited business entities, was structured to "consider and debate six broad themes in promoting international dialogue and cooperative measures among governments, the private sector, and other stakeholders, including:

- information sharing of national approaches, good practices and guidelines;
- developing watch, warning, and incident response capabilities;
- technical standards and industry solutions;
- harmonizing national legal approaches and international legal coordination;
- privacy, data and consumer protection;
- and developing countries and cybersecurity." [19]

At the Tunis Summit, WSIS reviewed and evaluated the progress on the Geneva Action Plan and devised the *Tunis Commitment* and the *Tunis Agenda for the Information Society*, which contained a comprehensive set of action items for involved parties. The identified action items initiated work to promote the spread of ICTs and clarify roles of public governance. Conference attendees planned to address a total of eleven broad action "lines." Action Line C5 ("Building confidence and security in the use of ICTs") reflects direct interest in cyber security and has been a focal point for many international and regional organizations, including the ITU and the Asia-Pacific Economic Cooperation (APEC, see Chapter 4).

Following the WSIS Tunis Summit in November 2005, the ITU presented a report on WSIS stocktaking and created a publicly accessible database of all WSIS-related implementation activities, including a number of projects related to cyber security and Action Line C5. The purpose of the WSIS Stocktaking Database was to be an "effective tool for the exchange of information on the projects fostering development of the information society, structured according to the eleven WSIS action lines." All WSIS stakeholders were encouraged to contribute information to the database, which would be continuously updated and maintained by the ITU.[20] The WSIS Stocktaking Database also complemented the ITU's *Golden Book: Stakeholder Commitments and Initiatives,* released in October 2005 to promote new commitments and initiatives announced by stakeholders at the Tunis Summit. The *Golden Book* database was frozen in January 2006, and a final report was published in February 2006.[21]

In addition to the WSIS Stocktaking Database and *Golden Book*, the ITU has since conducted annual facilitation meetings on WSIS Action Line C5 at its headquarters in Geneva. The first meeting, which took place in May 2006, was organized in line with WSIS paragraph 108 and the Annex of the Tunis Agenda for the Information Society, and was structured around the first five themes identified at the WSIS Thematic Meeting on Cybersecurity.[22] The second facilitation meeting, hosted in May 2007, was held in conjunction with several other events around the World Telecommunication and Information Society Day and focused on the issues of national strategies, legal frameworks, incident response, and spam and related threats.[23]

In May 2008, a third WSIS facilitation meeting- "Building Confidence and Security in the Use of ICTs"- was held at ITU headquarters in Geneva and focused on the legal, technical, and organizational challenges of cyber security, in addition to capacity building and international cooperation. The meeting's final report noted "a general view that ITU Global Cybersecurity Agenda was the appropriate framework for multi-stakeholder cooperation in cybersecurity and to concretize the role of ITU in this domain." In addition, proposals were made to ensure trust through technical solutions, establish frameworks in all domains, raise awareness, promote cooperation, and nominate "a centralized organization like the ITU with a structured framework" in the focus areas described above." [24]

In the 2007 *World Information Society Report: Beyond WSIS*, the ITU and the UN Conference on Trade and Development (UNCTAD) charted progress in building the Information Society and tracked the dynamics driving digital opportunity worldwide.[25] In chapter five, the report outlined primary challenges to building a safe and secure Information Society, including the recent evolution and increasing sophistication of threats such as spam, malware, and identity theft. The report identified primary mechanisms for taking action against these threats, as well as a roadmap for cyber security and the roles of different stakeholders, and encouraged themes such as information sharing, improvements in cyber security for developing economies, and promoted the ITU's Partnerships for Global Cybersecurity multi-stakeholder platform.[26]

2.2 Council of Europe Convention on Cybercrime

The Council of Europe's (COE, see Chapter 4) Convention on Cybercrime was the first international treaty of its kind seeking to address cybercrime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Created by the Council of Europe in 2001, the Convention represents the most prominent attempt at international harmonization of computer crime laws and procedures. According to the preamble, the main aim of the Convention is to pursue "…a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation." [27]

The Convention on Cybercrime took over four years and twenty-two substantive drafts before final approval by the Council of Europe in 2001. Significantly, it contains a series of powers and procedures, such as the search of computer networks and interception of network intruders. Containing forty-eight articles, the main focuses of the Convention are the normalization of definitions for computer-related offenses and the creation of a system for international cooperation. Additionally, the Convention includes definitions of investigation and prosecution procedures for use with global networks and multinational computer crimes. In particular, the convention includes a list of crimes that each signatory state must integrate into its own laws.

The criminalization of activities such as hacking, offenses related to child pornography, and specific intellectual property violations must be included.[28] The explanatory report associated with the Convention provides an interpretation that provides a basis for understanding. The following, based on the explanatory report, describe the contents of the Convention:

- Articles 2-13 address criminal law. Parties must domestically criminalize cybercrime, and offenses are divided into five categories. First, there are offenses against the confidentiality, integrity, and availability of computers, data, and systems (also known as CIA crimes). The second category involves the computer-related traditional offenses of forgery and fraud. Third are the content-related offenses of child pornography. The fourth category includes offenses related to copyright infringement and intellectual property. The final group consists of privacy infringement.
- Articles 14-22 address procedural law. Electronic evidence can be difficult to secure and can be quickly altered, moved, or deleted. The Convention requires each party to provide authorities with appropriate powers and procedures for use in investigations, including system search and seizure, real-time collection of traffic data, interception of content data, and the preservation and rapid disclosure of computer-stored data relating to traffic.
- Articles 23-35 address international cooperation. The Convention's provisions for international cooperation are subject to the domestic laws of the parties, as well as existing international agreements, such as MLATs (Mutual Legal Agreement Treaty). The Convention seeks to provide mechanisms for mutual assistance, in the event that existing international agreements are not applicable, or to expedite existing agreements. The 24/7 Network, intended to handle requests for mutual assistance quickly and efficiently (Art. 35), attempts to expedite international cooperation. Each party is required to designate a point of contact to facilitate rapid investigation of cybercrimes, similar to the Group of Eight's (G8, see Chapter 3) High-Tech Crime 24/7 Point-of-Contact Network. The 24/7 networks are expected to communicate rapidly with their peers in other locations, and the parties must ensure that trained and equipped personnel are available to staff the network.
- Articles 36-42 are largely administrative and address declarations and reservations with the treaty, for which the drafters have allowed considerable flexibility in interpretation in order to ensure wide acceptance. Through "declarations," parties may propose additional elements in their interpretations of offenses and procedural obligations, and through "reservations" parties may limit or qualify those same obligations. [29]