THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 2 Article 8

2007

Back Matter

BOOK REVIEWS

Gary C. Kessler
Editor
Champlain College
Burlington, VT 05401
gary.kessler@champlain.edu

INTRODUCTION

This is the Book Review column for the JDFSL. It is an experiment to broaden the services that the journal provides to readers, so we are anxious to get your reaction. Is the column useful and interesting? Should we include more than one review per issue? Should we also review products? Do you have suggested books/products for review and/or do you want to write a review? All of this type of feedback -- and more -- is appreciated. Please feel free to send comments to Gary Kessler (gary.kessler@champlain.edu) or Glenn Dardick (gdardick@dardick.net).

BOOK REVIEW

Libicki, M.C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press. 323 pages, ISBN: 978-0-521-69214-4 (paper), US$80

Reviewed by Gary C. Kessler (gary.kessler@champlain.edu)

Many books -- and even movies ("Live Free or Die Hard") -- are based upon the premise of an impending information war. In these scenarios -- made all too plausible by the increased frequency with which we read about and experience major information security incidents -- a Bad Guy exploits known computer security vulnerabilities in order to control major national infrastructures via the Internet so as to reap financial, economic, and/or personal power.

Martin Libicki's book takes a different, broader, and possibly more realistic view of the classic infowar scenario. Libicki -- a senior policy analyst at the RAND Corp. -- argues that hostile conquest of the global network is not as big a threat as some believe because of the incredible difficulty to taking control of information systems owned by others, corrupting their data, and/or shutting those systems down. He also argues that the globally connected cyberspace presents an excellent opportunity to drive the actions and attitudes of others.

This is not a head-in-the-sand analysis that suggests that cyberattacks are not possible; Libicki's premise is more about the practicality and efficacy of such efforts and, therefore, the book is about policy as much as it is about technology. The Internet was developed as the result of U.S. Department of

Defense (DoD) research efforts yet has realized its greatest success as means for peaceful commerce and personal intercourse. Its success is the very reason that we even think of the possible impact of hostile actions that might occur. Yet this book is very clearly about hostile conquest *in* -- rather than *of* -- cyberspace, suggesting that while isolated attacks within the Internet can and do occur, what do such attacks mean to the physical world?

Chapter 1 sets the stage and describes the loose organization of the three parts of book. Part I is comprised of four chapters that discuss hostile conquest. One basic premise is that computer systems, by and large, generate information so that humans can make decisions. Despite the number of automated processes, the claim here is that there are very few systems that are so automated and autonomous as to have taken humans out of the decision loop.

Chapter 2 addresses the issue of hostile attacks via cyberspace. The DoD did not really start to think of the Internet as an attack vector -- i.e., one to be utilized and defended -- until the 1990s. If the Internet represents the Global Information Age then it becomes a valuable asset for military organizations that depend so heavily upon information. Although information operations for both defense and offense is taken seriously by the DoD, it does not necessarily follow that actual conquest of an enemy can be accomplished via cyberspace. Indeed, an attack on information systems is not the same as an attack on the information stored on those systems.

Chapter 3 is aptly titled "Information Warfare as Noise." If information is *signal*, then an attack on information is *noise*. While *error* is to believe something to be true that is, in fact, actually false -- or vice versa -- *noise* is to not know that the something is even known. If an attacker throws a lot of bad information at an adversary, the response will be to make decisions more slowly and deliberately, perhaps drawing on multiple sources for validation. While noise, then, can complicate decision-making, it is not a vector for taking over control of information systems. Furthermore, the design and purpose of the target systems has a direct impact on how noise-tolerant they are and how "well" they fail, and this also affects the difficulty of any attack on those systems.

Chapter 4 discusses infowar against defense systems. The primary point of this chapter is that it is impossible to state with certainty whether an information warfare attack would -- or would not -- succeed. Even though system vulnerabilities abound that allow an attacker to get into other people's systems and wreak havoc, there is no attack vector that will always work and be consistently repeatable. Chapter 5 finishes off this part of the book by questioning the premise that infowar is about destroying information. Indeed, one information warfare attack vector might be to inundate an adversary with worthless information. Information overload is not *conquest* although the varying strategies with which an adversary copes with the situation can

certainly be disabling -- for some period of time and/or in some sectors. Indeed, that hesitation can enable *physical* conquest but the point is really that cyberspace-based conquest alone is harder than it looks.

The next two chapters comprise Part II, describing friendly conquest in cyberspace. Friendly conquest, as described in Chapter 6, focuses on allies, neutrals, and those that are not enemies and suggests that if owners of information systems freely and reliably share information, others eventually grow dependent upon those systems. Over time, the relationship between the users and owners of the information resource become intertwined and a symbiotic -- if not friendly, at least not adversarial -- relationship emerges. Chapter 7 shows how this relationship can expand beyond mere access to information, to include merging and bundling other systems, from financial and educational to social and cultural. One could argue that the Internet has already fostered some level of friendly conquests merely by allowing individuals to communicate more freely and widely than ever before; friendly conquests are also longer lasting and more solid than hostile ones.

Part III, comprising the final four chapters, observes that hostile and friendly conquest might actually go hand-in-hand -- and, in fact, friendly conquest can ease the road of hostile conquest.

Chapter 8 starts by discussing the vast quantity of personal information that is collected on just about every citizen and the myriad ways in which the custodians of that data protect or outright abuse the information in their care. Although the Internet can be used for all sorts of invasions of privacy, surveillance, and data mining (particularly as information becomes increasingly global), Libicki questions the long-term consequence as relates to hostile conquest. Indeed, digital signatures, virtual private networks (VPNs), and security features of Internet Protocol version 6 (IPv6) might actually see more widespread use if there continue to be egregious attacks on identity. And although there are vast resources on the Internet that support physical world reconnaissance that might expedite real world attacks, this does not enable conquest in cyberspace.

Friendly conquest requires not only the sharing of information between mutually dependent parties, but also trust between those parties. As Chapter 9 points out, such partnerships have their own special vulnerabilities. The closeness, for example, can make all partners prone to the system or policy weaknesses introduced by one party. In addition, an adversary of the partners can inject information into the common system in such a way as to create an atmosphere of distrust, eventually weakening the union.

Chapter 10 describes conquest in cyberspace in terms of human language; namely, phonology, syntax, semantics, and pragmatics. This is a very interesting take on the problem but demonstrates nicely that any conquest -- any significant activity, for that matter -- is complex and requires action at

many levels, be they human communication or computer communication. The particular point of this chapter is that both friendly and hostile conquest requires action at all levels and the complexity of the interactions between levels can both enable and frustrate such activities.

Chapter 11, "Managing Conquest in Cyberspace," closes out the body of the book and is devoted to the role of government and organizations in protecting their part of cyberspace to ward off hostile intent and how to extend their sphere of influence to exact friendly conquest. A fair amount of this chapter is a critique of Microsoft and Windows, a case study of attack vectors warranted by their dominance in the computer industry.

This book is very well-written, incredibly well-documented (the footnotes alone are worth reading), and compelling. We have been so inundated with the message that information warfare is possible and downright impending that it is beneficial to read a well-reasoned alternate perspective. Libicki provides a knowledgeable, broad look at the big picture and makes a good argument that the situation is a different, more complex one than we may have been discussing.

Subscription Information

The Journal of Digital Forensics, Security and Law (JDFSL) is a publication of the Association of Digital Forensics, Security and Law (ADFSL). The Journal is published on a non-profit basis. In the spirit of the JDFSL mission, individual subscriptions are discounted. However, we do encourage you to recommend the journal to your library for wider dissemination.

The journal is published in both print and electronic form under the following ISSN's:

ISSN: 1558-7215 (print)

ISSN: 1558-7223 (online)

Subscription rates for the journal are as follows:

Institutional - Print & Online: $395 (4 issues)

Institutional - Online only: $295 (4 issues)

Individual - Print & Online: $80 (4 issues)

Individual - Online only: $25 (4 issues)

Subscription requests may be made to the ADFSL.

The offices of the Association of Digital Forensics, Security and Law (ADFSL) are at the following address:

Association of Digital Forensics, Security and Law
Longwood University
201 High Street
Farmville, Virginia 23909
Tel: 434-395-2377
Fax: 434-395-2203
E-mail: editor@jdfsl.org
Website: http://www.adfsl.org

Announcements and Upcoming Events

5th Australian Digital Forensics Conference 2007 (ADFC2007)

ADFC2007 will be held Monday, December 3rd, 2007 at Edith Cowan University, Mount Lawley, Western Australia. The aim of ADFC 2007 is to bring together IT managers, system and network administrators, security specialists, academics, security solutions vendors, practitioners and anyone interested in:

- Computer forensics its role and application
- Techniques in detecting, responding and investigating computer and related security incidents
- Sharing their views, experiences and knowledge with those involved in the computer forensic field

All papers must be submitted via the conference website. For more detailed information regarding submissions requirements, please visit the website at
http://scissec.scis.ecu.edu.au/conferences2007

The 5th Australian Digital Forensics Conference will be run in conjunction with 8th Australian Information Warfare and Security, and the 5th Australian Information Security Management Conference jointly from 3rd - 4th December, 2007 at ECU Western Australia.

2008 Conference on Digital Forensics, Security and Law
Oklahoma USA
April, 2008

The ADFSL 2008 Conference on Digital Forensics, Security and Law will be held in Oklahoma in April 2008.

http://www.digitalforensics-conference.org

MFW08 – Mobile Forensics World 2008
www.MobileForensicsWorld.com
O'Hare Marriott, Chicago, Illinois, USA
May 8-10, 2008

Call for Papers on Mobile Device Forensics
Abstract Submission Deadline: January 31, 2008
Contact: Prof. Rick Mislan, Cyber Forensics Lab, Purdue University

Journal of Digital Forensics, Security and Law

Volume 2, Number 2

2007

Contents

Special Issue Editor's Note 2

Call for Papers 3

Call for Papers: Special Issue on Security Issues in Online Communities 4

Guide for Submission of Manuscripts 5

Computer Crimes: a Case Study of What Malaysia Can Learn from Others 7
Janaletchumi Appudurai and Chitra Latha Ramalingam

Monitoring and Surveillance in the Workplace: Lessons Learnt? – Investigating the International Legal Position 23
Verine Etsebeth

The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism 41
Murdoch Watney

Information Technology Act 2000 in India - Authentication of E-Documents 57
R. G. Pawar, B. S. Sawant and A. Kaiwade

Book Review: Conquest in Cyberspace: National Security and Information Warfare 67
Reviewed by Gary C. Kessler

Subscription Information 71

Announcements and Upcoming Events 72