Reviewing the Works of Bruce Schneier and Michael G. McLaughlin & William Holstein

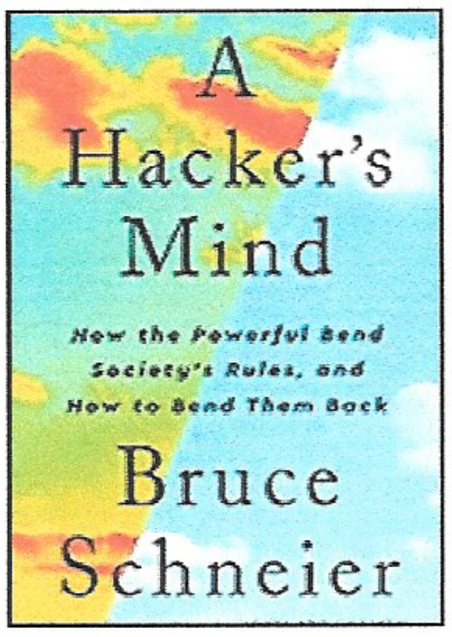
By: William J. (Jay) Carson, ISSA Member Colorado Springs Chapter

Disclaimer: These are the author's subjective opinions, and do not necessarily reflect the opinions of any organization or other individual. A human prepared this article, with assistance from Microsoft Editor and Grammarly.

I was a fanatical reader of science fiction in my youth and may have stopped too soon. Books like Douglas Adam's *The Hitchhiker's Guide to the Galaxy* (1997), seem to be formative influences for the movers and shakers in IT like Bruce Schneier, and they use them as communication shorthand. Expect a review in the future of that book, along with George Orwell's *1984,* another common reference. But on to this month's column:

Book #1:

Schneier, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Ben Them Back*. W.W. Norton & Company (2023).



Sound Bite: Fully understanding hacking as a concept will help us, particularly as AI becomes more pervasive.

Opinion on Primary Audience: World, but extremely valuable background for future CISOs.

If you are or aspire to be a CISO, read this book early in your journey. I often see writings that tell us technical people do not understand business. After this book, you will be stronger and smarter in your dealings with business leaders, and I can almost guarantee it!

I read twice all the books I review. I was especially glad of that technique when I read Bruce Schneier's new book. After the first read, I might have said "Well, bless his heart, the old master is fading. This is just a collection of his wandering thoughts on various topics; nothing new." How horribly wrong I would have been! First, Schneier hacks your reading habits. Most of you do not have an hour or more to read without any distractions. So he wrote a series of interesting story essays of only a few pages, and you can finish at least one chapter in a few minutes. Second, the value for cyber practitioners is in understanding the overall cognitive action of hacking. He says, "That's what a hack is: an actively allowed by the system that subverts the goal or intent of the system."

The Author

Bruce Schneier continues his excellence. Like other famous names in cybersecurity, hearing "Bruce Schneier" will stimulate the neurons of cybersecurity professionals. His credentials are mainly in his many books, and certainly, if you have an interest in cryptography, you have read at least some of his work. I have only read two of his books: *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,* and *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Currently an adjunct lecturer at Harvard, his academic credentials include a BS in physics and a master's degree in computer science.

The Metadata

A ***2023*** publishing date! The online ordering cost, including shipping, is under $15, about the same with an e-reader. The hardcover book is about 250 pages, plus notes pages. My local public library system has multiple copies, but an extensive 'hold' list.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the readability is high school level. There was about 15% passive voice in my sample. This article is about 2% passive voice.

Table of Contents (Just a few chapters listed with comments annotated in bold font (inside parenthesis) by me. Note: My comments are few, as the other chapter titles are self-explanatory)

Part 1 Hacking 101
1 What is Hacking **(Important to think broadly)**
4 The Hacking Life Cycle **(Eternal Blue)**

Part 2 Basics Hacks and Defenses **(Great stories you will enjoy - Good Hacks - Bad Hacks)**
11 Defending Against Hacks **('Hotfix' type of patching)**
14 The Economics of Defense **(Threat Modeling)**

Part 3 Hacking Financial Systems **(Current and Aspiring CISOs take note!)**
19 Hacking Computerized Financial Exchanges **(High Frequency Trading)**
25 Hacking and Wealth **(Private Equity)**

Part 4 Hacking Legal Systems
28 Hacking Bureaucracy **(Goodhart's Law)**

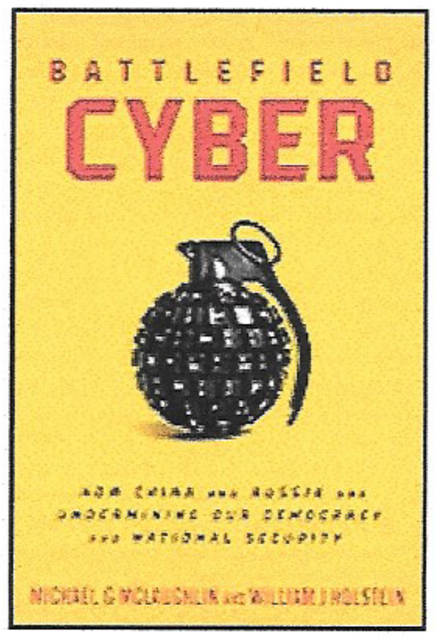
Part 5 Hacking Political Systems
37 Delegating and Delaying Legislation **(Japanese 'Ox Walking')**

Part 6 Hacking Cognitive Systems

Part 7 Hacking AI Systems
52 The **(AI)** Explainability Problem **(Possibly the most important chapter)**
56 When AIs Become Hackers **(AI in 'Capture the Flag')**
60 Governance Systems for Hacking **(His subtitles are: Speed, Inclusivity, transparency, Agility)**

Book #2:

McLaughlin, Michael G. and William Holstein. *Battlefield Cyber: How China and Russia Are Undermining Our Democracy and National Security.* Rowman & Littlefield (2023.)



Sound Bite: Through cyber, ruthless national governments with external power ambitions are well on the way to victories, and the rest of the world had better suit up and join forces in defense.

Opinion on Primary Audience: Democracies and their thought-leaders.

If I were to suggest an alternative title for this book, it would be Sun Tsu Goes Cyber. You have read The Art of War, right? For Battlefield Cyber, I saw a recommendation months ago on LinkedIn by Robert Metzger, a particularly important person in cyber and a senior attorney. I do not know Mr. Metzger personally, but I have followed his LinkedIn posts and heard him speak. I notice really smart people stop talking and listen to him, and even defer to his opinions.

Cyber threats are included in many recent books on hostile-to-democracies foreign governmental threats. One book you may see lauded is Seth G. Jones' *Three Dangerous Men: Russia. China, Iran, and The Rise of Irregular Warfare.* W.W. Norton & Company (2021). That is a fine book, but it only touches on the cyber threat. *Battlefield Cyber* is much more focused.

On the first read-through, I thought the book's solutions to the cyber threats from national governments were extremist. For example, the authors want a Cyber National Guard. Read the book twice, and you will see the reasonableness of the authors' recommendations.

The Author
Michael McLaughlin is a cyber attorney, with a strong background in US cyber counterintelligence. William Holstein is primarily a writer/journalist/editor, with an extremely strong background on China. Author of several books, he lived in Hong Kong and Beijing, where he was UPI bureau chief. This is a very experienced and knowledgeable team.

The Metadata
A ***2023*** publishing date! The online ordering cost, including shipping, is under $20. You cannot cut that cost much if you use an e-reader. The hardcover version is about 250 pages including notes. My public library has no copies.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style measurement is graduate school level, and my honest criticism is that level is unnecessarily harder for all potential readers. There was around 33% passive voice in my sample. This article is about 2% passive voice, for comparison.

Table of Contents (abbreviated/modified and annotated in bold font (inside parenthesis) by me)

Part I: We Are at War
1. Cyber Warfare: The Enemy Inside the Gates **(Stuxnet, NotPetya, and Gerasimov Doctrine histories, also U.S. Cyber Command and Hunt Forward Operations)**
2. Water and Oil: Weaponized Ransomware, Digital Proxies, and the Threat to Critical Infrastructure
3. Chinese Cyber Espionage: The Greatest Transfer of Wealth in History
4. The New Oil: Data and China's Digital Silk Road Strategy **(APTs)**
5. Stoking the Flames: How Malign Influence Exacerbates America's Political Divides and Ethnics Tensions **(More APTs)**
6. Software Meltdown: The Problem with Trust **(Apache Log4j and Solar Winds/Orion details) (Trivia Question: Who was Linus Torvalds?)**
7. Someone Else's Server: The Vulnerabilities of Cloud Computing
8. Stealing the War: Cyber Threats to America's Defense Supply Chain **(People's Liberation Army Unit 61398 successes)**

Part II: The Response: What Must Be Done
9. Retreat from Globalization: Easing Corporate America's Addiction to China **(Really important words - thought-provoking on 'reshoring' possibilities)**
10. Social Disorder: Reining in Social Media and Big Tech **(The 1996 Communications Decency Act Section 230)**
11. Re-Architecting Security: What the Private Sector Must Do **(About canary files - very cool!)**
12 Government Action: What the Public Secor Must Do
13 Collective Defense: How the Public and Private Sectors Must Work Together

Happy Reading!

PS - If you have a book you want me to read & review, please use the email address in my bio to let me know!

For next month's reviews,

Miller, Chris. Chip War: The Fight for the World's Critical Technology. Simon & Schuster (2022).

Sharp, Matthew K., and Kyriakos (Rock) Lambros. The CISO Evolution: Business Knowledge for Cybersecurity Executives. Wiley (2022).

Additional sources used in the article:

1. https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests
2. https://en.wikipedia.org/wk/Bruce_Schneier
3. LinkedIn profiles for authors listed, where available.
4. https://riverjournalonline.com/news/local-authors-local-books-william-holstein-the new-art-of-war/17569/. October 24, 2019.
5. https://en.wikipedia.org/wiki/The_Art_of_War

About the Author

William J. (Jay) Carson, ISSA Senior Member, ISSA 2020 Volunteer of the Year, and a past ISSA-Colorado Springs Executive Vice President. He is the part-time 'Cyber Librarian' of Semper Sec, LLC. Holding Security+ and CIPP/E certifications, he is a former high school