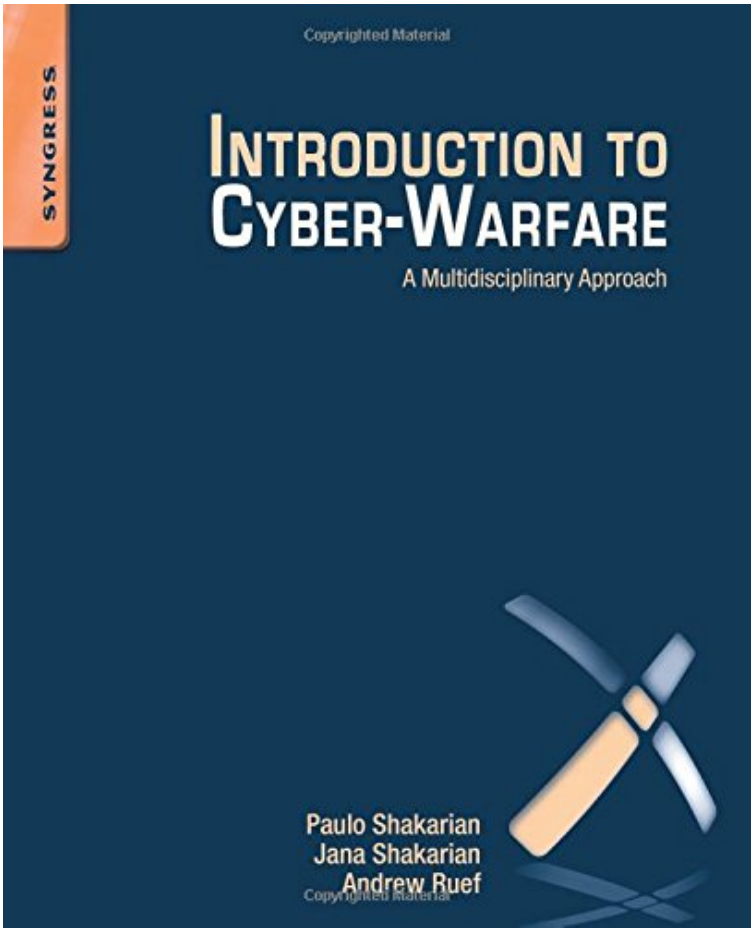
Introduction to Cyber-Warfare: A Multidisciplinary Approach

Paulo Shakarian, Jana Shakarian, Andrew Ruef
**Download PDF | ePub | DOC | audiobook | ebooks*



#247096 in Books Syngress 2013-06-18 2013-06-04Original language:EnglishPDF # 1 9.25 x .76 x 7.50l, 1.50 #File Name: 0124078141336 pages | File size: 29.Mb

Paulo Shakarian, Jana Shakarian, Andrew Ruef : Introduction to Cyber-Warfare: A Multidisciplinary Approach before purchasing it in order to gage whether or not it would be worth my time, and all praised Introduction to Cyber-Warfare: A Multidisciplinary Approach:

5 of 7 people found the following review helpful. Mostly great content, unreadably small Kindle font sizingBy D. RosenbauerOver the past couple of years, I've read most of the IT security books published by Syngress. With only a few minor exceptions, they are uniformly well-written, up to date, and informative. This book was no exception.The three authors are extremely knowledgeable about their subject matter, and, for the most part, write clearly and concisely. One of the authors is a major in the US Army, one is a private-sector security consultant, and one is an academic researcher. This is truly a "multi-disciplinary approach". The book begins with examples of cyber-incidents, including attacks on Estonia and Georgia (the country) during the late 2000s. After a brief segue through Anonymous and other non-state actors (see below), they get into cyber-espionage and cyber-attacks. Reading through this book during the ongoing NSA scandal helped me see things from the cyber-warfare perspective.The content is (mostly)

impeccable, and if I was rating it on the content alone, I would give it four and a half stars. I'm giving this book three stars instead for two reasons:First, the chapter I mentioned above, on Anonymous and "hacktivism", was unexpectedly different. Many of the paragraphs read like they'd been cobbled together at the last minute from previously-written, unrelated writings. The author(s) re-introduced and repeatedly cited the same few individuals (specifically the PLF's "Commander X") and organizations a dozen times throughout the chapter, with no sense that they'd already been introduced to the reader earlier. Occasionally, a source would be quoted without identification, and then introduced several pages later. The chapter also has a somewhat uneven scolding tone, as though the author(s) couldn't decide whether to be amused or offended by hacktivists. Since the other chapters were much higher quality, I would recommend that somebody go back and edit Chapter 6 for clarity and consistency.Second, the Kindle edition was formatted very strangely on both my Paperwhite and Kindle for PC. As you progress through the first few chapters, the paragraph font becomes progressively smaller and smaller. By chapter 8, the paragraph text is small enough that the Kindle's controls won't increase it above the Kindle's absolute minimum font size unless you set it to one of the top three settings. Setting the font to a readable size makes the chapter headings and table of contents so large that only a few words fit on a single page. As a lesser (and maybe related) issue, the whole book appears inside of a gray box, like you'd see used for a call-out section in other Syngress books.If the publisher updates this book so that the later chapters are readable without 3x reading glasses, I'll update my review to five stars on content alone. Keep up the good work, Syngress.2 of 4 people found the following review helpful. Good Compilation of Material - Kindle version Needs to be FixedBy BillThis is a very useful compilation of cyber warfare material and helped me a great deal to connect into various resources through good footnotes. The most negative thing about the book is the very poor Kindle formatting (I used the iPad Kindle app.) The font size changes radically from chapter to chapter and some chapters were very difficult to read, even on the maximum font size. Obviously, the formatting needs to be fixed. This would be four stars if the formatting was fixed.1 of 1 people found the following review helpful. Provides a great introduction to cyberwarfareBy Ben RothkeCyberwarfare is a most controversial topic. At the 2014 MISTI Infosec World Conference, noted security curmudgeon Marcus Ranum gave a talk on Cyberwar: Putting Civilian Infrastructure on the Front Lines, Again. Be it the topic or Marcus being Marcus, a third of the participants left within the first 15 minutes. They should have stayed, as Ranum, agree with him or not, provided some riveting insights on the topic.While a somewhat broad term, in Wikipedia, cyberwarfare (often called information warfare) is defined as politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare.The authors define cyber war as an extension of policy by actions taken in cyber space by state or nonstate actors that either constitute a serious threat to a nation’s security or are conducted in response to a perceived threat against a nation’s security.As to a book on the topic, for most readers, cyberwarfare is something that they may be victims of, but will rarely be an actively part of.In Introduction to Cyber-Warfare: A Multidisciplinary Approach, authors Paulo Shakarian, Jana Shakarian and Andrew Ruef provide an excellent overview of the topic. The book takes a holistic, or as they call it multidisciplinary, approach to the topic. It looks at the information security aspect of cyberwarfare, as well the military, sociological and other aspects of the topic.The book is divided into 3 parts and 13 densely packed and extremely well-researched and footnoted chapters, namely:Part I: Cyber AttackChapter 2: Political Cyber Attack Comes of Age in 2007Chapter 3: How Cyber Attacks Augmented Russian Military OperationsChapter 4: When Who Tells the Best Story Wins: Cyber and Information Operations in the Middle EastChapter 5: Limiting Free Speech on the Internet: Cyber Attack Against Internal Dissidents in Iran and RussiaChapter 6: Cyber Attacks by Nonstate Hacking Groups: The Case of Anonymous and Its AffiliatesPart II: Cyber Espionage and ExploitationChapter 7: Enter the Dragon: Why Cyber Espionage Against Militaries, Dissidents, and Nondefense Corporations Is a KeyComponent of Chinese Cyber StrategyChapter 8: Duqu, Flame, Gauss, the Next Generation of Cyber ExploitationChapter 9: Losing Trust in Your Friends: Social Network ExploitationChapter 10: How Iraqi Insurgents Watched U.S. Predator Video—Information Theft on the Tactical BattlefieldPart III: Cyber Operations for Infrastructure AttackChapter 11: Cyber Warfare Against IndustryChapter 12: Can Cyber Warfare Leave a Nation in the Dark? Cyber Attacks Against Electrical InfrastructureChapter 13: Attacking Iranian Nuclear Facilities: StuxnetThe book provides numerous case studies of the largest cyberwarfare events to date. Issues around China and their use of cyberwarfare constitute a part of the book. Chapter 7 details the Chinese cyber strategy and shows how the Chinese cyber doctrine and mindset is radically different from that of those in the west.The book compares the board games of chess (a Western game) and Go (a Chinese game) and how the outcomes and strategies of the games are manifest in each doctrine.The chapter also shows how the Chinese government outlawed hacking, while at the same time the military identified the best and most talented hackers in China, and integrated them into Chinese security firms, consulting organizations, academia and the military.One of the more fascinating case studies details the cyber war against the corporate world from China. The book provides a number of examples and details the methodologies they used, in addition to providing evidence of how the Chinese were involved.For an adversary, one of the means of getting information is via social networks. This is often used in parallel by those launching some sort of cyberwarfare attack. LinkedIn is one of the favorite tools for such an effort. The authors write of the dangers of transitive trust; where user A trusts user B, and user B trusts user C. Via a transitive trust, user A will then trust user C

based simply on the fact that user B does. This was most manifest in the Robin Sage exercise.This was where Thomas Ryan created a fictitious information security professional names Robin Sage. He used her fake identity and profile to make friends with others in the information security world, both commercial, federal and military and he was able to fool even seasoned security professionals. Joan Goodchild wrote a good overview of the experiment here.In chapter 10, the book details how Iraqi insurgents viewed Predator drones video feeds. Woody Allen said that eighty percent of success is just showing up. In this case, all the insurgents had to do was download the feed, as it was being transmitted unencrypted. Very little cyberwarfare required.When the drone was being designed, the designers used security by obscurity in their decision not to encrypt the video feed. They felt that since the Predator video feeds were being transmitted on frequencies that were not publically known, no access control, encryption or other security mechanisms would be needed.The downside is that once the precise frequency was determined by the insurgency, in the case of the Predator drone, the Ku-band, the use of the SkyGrabber satellite internet downloader made it possible for them to effortless view the video feeds.The only negative about the book is a minor one. It has over 100 pictures and illustrations. Each one states: for the color version of this figure, the reader is referred to the online version of the book. Having that after every picture is a bit annoying. Also, the book never says where you can find the online version of the book.How good is this book? In his review of it, Krypt3ia said it best when he wrote: I would love to start a kickstarter and get this book into the hands of each and every moron in Congress and the House. The reality is that this book should indeed be read by everyone in Washington, as they are making decisions on the topic, without truly understanding it.For most readers, this will be the book that tells them everyone they need to know that their congressman should know. Most people will never be involved with any sort of warfare, and most corporate information security professional will not get involved with cyberwarfare. Nonetheless, Introduction to Cyber-Warfare: A Multidisciplinary Approach is a fascinating read about a most important topic.

Introduction to Cyber-Warfare: A Multidisciplinary Approach, written by experts on the front lines, gives you an insider's look into the world of cyber-warfare through the use of recent case studies. The book examines the issues related to cyber warfare not only from a computer science perspective but from military, sociological, and scientific perspectives as well. You'll learn how cyber-warfare has been performed in the past as well as why various actors rely on this new means of warfare and what steps can be taken to prevent it.Provides a multi-disciplinary approach to cyber-warfare, analyzing the information technology, military, policy, social, and scientific issues that are in playPresents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents within a state (Russia, Iran)Explores cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and LulzSec Covers cyber-attacks directed against infrastructure, such as water treatment plants and power-grids, with a detailed account of Stuxent

"...an excellent overview of the topic…It looks at the information security aspect of cyberwarfare, as well the military, sociological and other aspects…this book should indeed be read by everyone in Washington, as they are making decisions on the topic, without truly understanding it."--Slashdot.org, RSAConference.com ,August 4 2014About the AuthorPaulo Shakarian, Ph.D. is a Major in the U.S. Army and an Assistant Professor of Computer Science at the U.S. Military Academy (West Point) teaching classes on computer science and information technology as wells as conducting research on cyber-security, social networks, and artificial intelligence. He has written over twenty papers published in scientific and military journals. Relating to cyber-warfare, he has written the paper “Stuxnet: Cyberwar Revolution in Military Affairs” published in Small Wars Journal and “The 2008 Russian Cyber-Campaign Against Georgia” published in Military . His scientific research has also been well received, featured in major news media such including The Economist and Nature. Previously, he has authored Geospatial Abduction: Principles and Practice published by Springer. Paulo holds a Ph.D. and M.S. in computer science from the University of Maryland, College Park, a B.S. in computer science from West Point, and a Depth of Study in Information Assurance also from West Point. Paulo has served two combat tours in Operation Iraqi Freedom. His military awards include the Bronze Star, Meritorious Service Medal, Army Commendation Medal with Valor Device, and Combat Action Badge. Paulo’s website is: http://shakarian.net/paulo.Jana Shakarian is a Research Fellow at the West Point Network Science Center conducting sociological research in support of various DoD-sponsored projects. Previously, Jana has worked as a research assistant at Laboratory for Computational Cultural Dynamics at the University of Maryland where she extensively studied terrorist groups in south-east Asia in addition to other research initiatives at the intersection of social and computational science applied to military and security problems. She has written numerous papers in addition to co-authoring the book Computational Analysis of Terrorist Groups: Lashkar-e-Tabia, to be published by Springer in the near future. Jana holds an M.A. in cultural and social anthropology and sociology from the Johannes Gutenberg University, Mainz where her thesis was on “new war” theory. Jana’s website is: http://shakarian.net/jana.Andrew Ruef is a Senior Systems Engineer at the firm Trail of Bits (New York, NY) where he conducts information security analysis. Andrew has nearly a decade of industry experience in computer network

security and software engineering, working on various projects including reverse-engineering of malware, analysis of computer network traffic for security purposes, system administration, and development of secure software products. Andrew has also written numerous white papers on information security and has spoken at various conferences such including a recent conference talk at the Dagstuhl computer research center in Germany. Currently, Andrew is working toward his B.S. in Computer Science at the University of Maryland, College Park. A sampling of some of Andrew's technical work can be found here: http://www.kyrus-tech.com/tag/andrew-ruef/.