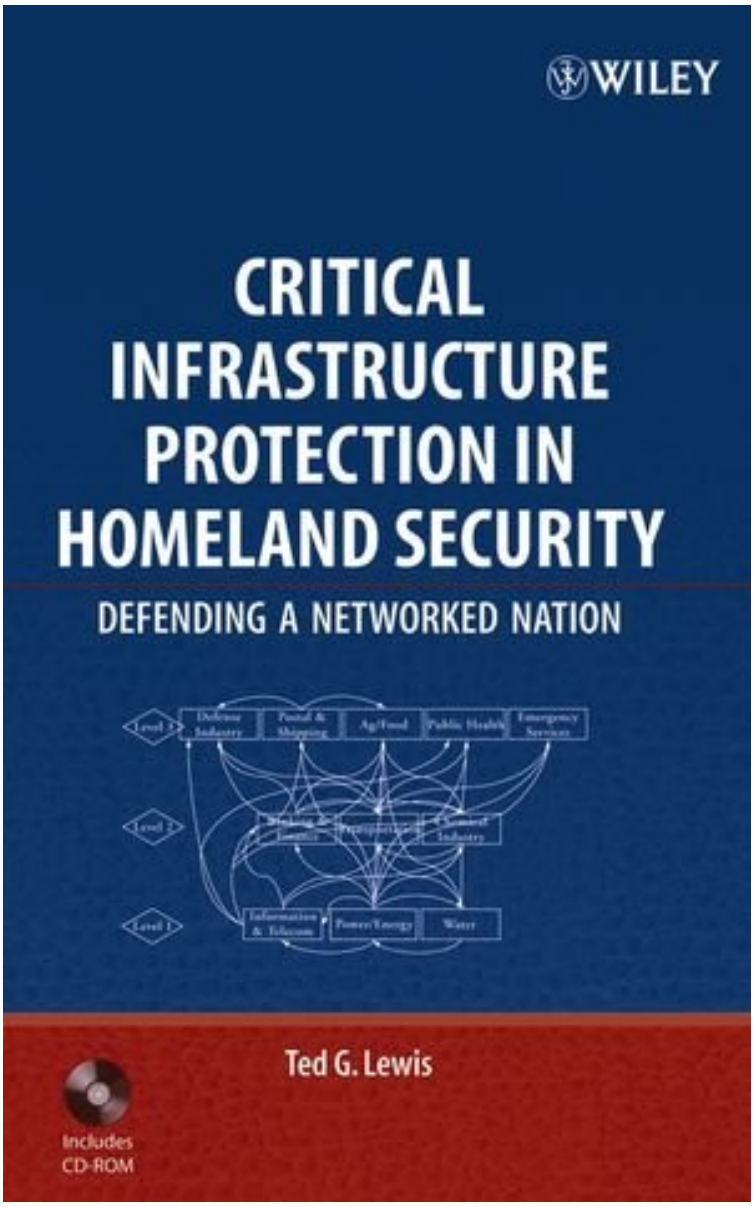
Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation

Ted G. Lewis



#1015918 in Books 2006-04-21Ingredients: Example IngredientsOriginal language:EnglishPDF # 1 9.50 x 1.12 x 6.50l, 1.85 #File Name: 0471786284486 pages | File size: 53.Mb

Ted G. Lewis : Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation before purchasing it in order to gage whether or not it would be worth my time, and all praised Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation:

1 of 1 people found the following review helpful. Decent textbook for advanced learners in the field, awful for entry-level college studentsBy RebekahThis textbook is long, occasionally rambling, and at times focuses more on the author's personal beliefs and views on where the United States needs to be versus where they are.The author is also inconsistent with his presentation of facts. For example, he states that FEMA was established in 1988. He doesn't mention that FEMA was actually created in 1979 (this is according to FEMA's website) and that the Stafford Act of 1988 amended a previous act and created the system that is in place today. While his information is accurate, his presentation leaves room for error.If you are familiar with critical infrastructure, the various federal, state, and local agencies, and business practices of emergency management, you might get this book. If this is your first exposure to the field, I would not recommend it at all.2 of 2 people found the following review helpful. An okay book on CIP, but lacks many thingsBy Britton J. HoldawayI used this book for a graduate course through the University of Washington. I purchased it new and used the CD in the back for my class. The course's reading schedule did not comprise the whole book (excluded some two or three chapters), but covered enough of it that I feel justified in posting my opinions about it here.First, the book is in strong need of an editorial review. Grammatical errors and contradictory statements run throughout the book. It seems as though the material was put together rather quickly and little to no effort was spent giving it a professional appearance or delivery.Second, the author fails to provide sources for many of the things he includes in the book. (To give him credit, all quotes and direct references were given citations.) I can handle a lack of sources to an extent, but have a difficult time accepting that a Computer Scientist has the requisite knowledge of, say economics, to pontificate and exrapolate his books principles across multiple fields of study. Also, the lack of sources means that the author left his book without any anchors for context in the greater scheme of critical infrastucture protection, homeland security, and emergency management.Third, the questions at the end of each chapter are in need of a *serious* overhaul. Not only are they incredibly ambiguous, but there were several instances where the answer to a question was found in a succeeding chapter. I have no problem with questions referencing material already covered, but it goes against reason to ask questions regarding material that has not yet been covered.Fourth, the programs provided on the CD, and which are meant to aid the student in applying the principles of the book, are buggy. (Which is interesting, considering the author is a computer programmer ... but anyway.) Once again, it seems as though the author was more interested in putting the book on the shelves than on ensuring that his material was coherent, cogent, and professionally finished.Now for some positives:The overall premise of the book is sound. For those with any familiarity with the government's funding mechanism vis-a-vis homeland security, the author's argument for identifying and hardening CI hubs is extraordinarily poignant. Looking past all of the book's faults, and they are many, government officials would do well to learn from Lewis's call for more scientific rigor in how the country goes about protecting itself.0 of 0 people found the following review helpful. Four StarsBy CustomerGreat

A scientific approach to the new field of critical infrastructure protection This book offers a unique scientific approach to the new field of critical infrastructure protection: it uses network theory, optimization theory, and simulation software to analyze and understand how infrastructure sectors evolve, where they are vulnerable, and how they can best be protected. The author demonstrates that infrastructure sectors as diverse as water, power, energy, telecommunications, and the Internet have remarkably similar structures. This observation leads to a rigorous approach to vulnerability analysis in all of these sectors. The analyst can then decide the best way to allocate limited funds to minimize risk, regardless of industry sector. The key question addressed in this timely book is: What should be protected and how? The author proposes that the answer lies in allocating a nation's scarce resources to the most critical components of each infra-structure--the so-called critical nodes. Using network theory as a foundation, readers learn how to identifya small handful of critical nodes and then allocate resources to reduce or eliminate risk across the entire sector. A comprehensive set of electronic media is provided on a CD-ROM in the back of the book that supports in-class and self-tutored instruction. Students can copy these professionally produced audio-video lectures onto a PC (Microsoft Windows(r) and Apple Macintosh(r) compatible) for repeated viewing at their own pace. Another unique feature of the book is the open-source software for demonstrating concepts and streamlining the math needed for vulnerability analysis. Updates, as well as a discussion forum, are available from www.CHDS.us. This book is essential for all corporate, government agency, and military professionals tasked with assessingvulnerability and developing and implementing protection systems. In addition, the book is recommended for upper-level undergraduate and graduate students studying national security, computing, and other disciplines where infrastructure security is an issue.

"...excellent for use as a text in information assurance or cyber-security courses...I strongly advocate that professors...examine this book with the intention of using it in their programs." (Computing s.com, March 22, 2007) "The book is written as a student textbook, but it should be equally valuable for current practitioners...this book is a very worthwhile investment." (Homeland Security Watch, August 17, 2006)From the Back CoverA scientific approach to the new field of critical infrastructure protection This book offers a unique scientific approach to the new field of critical infrastructure protection: it uses network theory, optimization theory, and simulation software to

analyze and understand how infrastructure sectors evolve, where they are vulnerable, and how they can best be protected. The author demonstrates that infrastructure sectors as diverse as water, power, energy, telecommunications, and the Internet have remarkably similar structures. This observation leads to a rigorous approach to vulnerability analysis in all of these sectors. The analyst can then decide the best way to allocate limited funds to minimize risk, regardless of industry sector. The key question addressed in this timely book is: What should be protected and how? The author proposes that the answer lies in allocating a nation's scarce resources to the most critical components of each infra-structurethe so-called critical nodes. Using network theory as a foundation, readers learn how to identifya small handful of critical nodes and then allocate resources to reduce or eliminate risk across the entire sector. A comprehensive set of electronic media is provided on a CD-ROM in the back of the book that supports in-class and self-tutored instruction. Students can copy these professionally produced audio-video lectures onto a PC (Microsoft Windows and Apple Macintosh compatible) for repeated viewing at their own pace. Another unique feature of the book is the open-source software for demonstrating concepts and streamlining the math needed for vulnerability analysis. Updates, as well as a discussion forum, are available from www.CHDS.us. This book is essential for all corporate, government agency, and military professionals tasked with assessingvulnerability and developing and implementing protection systems. In addition, the book is recommended for upper-level undergraduate and graduate students studying national security, computing, and other disciplines where infrastructure security is an issue.About the AuthorTED G. LEWIS, PHD, is Professor of Computer Science and Academic Associate of the Homeland Defense and Security curriculum at the Naval Postgraduate School. Dr. Lewis is the former senior vice president of Digital Development for Eastman Kodak.