1. Record Nr. UNINA9910463519003321

Autore	Lewis T. G (Theodore Gyle), <1941->
Titolo	Critical infrastructure protection in homeland security : defending a networked nation / / Ted G. Lewis
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Inc., , 2015 ©2015
ISBN	1-118-81766-4 1-118-81770-2
Edizione	[Second edition.]
Descrizione fisica	1 online resource (399 p.)
Disciplina	005.8
Soggetti	Computer networks - Security measures - United States Computer security - United States - Planning Terrorism - United States - Prevention Terrorism - Government policy - United States Civil defense - United States Public utilities - Protection - United States Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation; Copyright; Contents; Preface; How to Use this Book; Acknowledgment; Part I Origins of Homeland Security and Critical Infrastructure Protection Policy; Chapter 1 Origins of Critical Infrastructure Protection; 1.1 Recognition; 1.2 Natural Disaster Recovery; 1.3 Definitional Phase; 1.4 Public-Private Cooperation; 1.5 Federalism: Whole of Government; 1.6 Infrastructure Protection within DHS; 1.7 Implementing a Risk Strategy; 1.7.1 Risk-Informed Decision-Making; 1.7.2 Resilience-Informed Decision-Making 1.7.3 Prevention or Response? 1.8 Analysis; 1.8.1 The PPP Conundrum; 1.8.2 The Information-Sharing Conundrum; 1.8.3 Climate Change Conundrum; 1.8.4 The Funding Conundrum; 1.8.5 Spend 80% on 20% of the Country; 1.9 Exercises; References; Part II Theory and Foundations; Chapter 2 Risk Strategies; 2.1 EUT; 2.1.1 Threat-Asset

Pairs; 2.2 PRA and Fault Trees; 2.2.1 An Example: Your Car; 2.3 MBRA and Resource Allocation; 2.3.1 Another Example: Redundant Power; 2.4 PRA in the Supply Chain; 2.5 Protection versus Response; 2.6 Threat Is an Output; 2.7 Bayesian Belief Networks; 2.8 A BN for Threat
2.9 Risk of a Natural Disaster 2.10 Earthquakes; 2.11 Black Swans and Risk; 2.12 Black Swan Floods; 2.13 Are Natural Disasters Getting Worse?; 2.14 Black Swan al Qaeda Attacks; 2.15 Black Swan Pandemic; 2.16 Risk and Resilience; 2.17 Exercises; References; Chapter 3 Theories of Catastrophe; 3.1 NAT; 3.2 Blocks and Springs; 3.3 Bak's Punctuated Equilibrium Theory; 3.4 TOC; 3.4.1 The State Space Diagram; 3.5 The U.S. Electric Power Grid; 3.6 POE; 3.6.1 The Great Recessions; 3.6.2 Too Much Money; 3.7 Competitive Exclusion; 3.7.1 Gause's Law; 3.7.2 The Self-Organizing Internet; 3.7.3 A Monoculture
3.8 POR 3.9 Resilience of Complex Infrastructure Systems; 3.9.1 Expected Utility and Risk; 3.9.2 SOC; 3.9.3 TOC; 3.9.4 POE and nonlinearity; 3.9.5 CEP and loss of redundancy; 3.9.6 POR and percolation; 3.10 Emergence; 3.10.1 Opposing Forces in Emergent CIKR; 3.11 Exercises; References; Chapter 4 Complex CIKR Systems; 4.1 CIKR as Networks; 4.1.1 Emergence; 4.1.2 Classes of CIKR Networks; 4.1.3 Self-Organized Networks; 4.2 Cascading CIKR Systems; 4.2.1 The Fundamental Resilience Equation; 4.2.2 Targeted Attacks; 4.3 Network Flow Resilience; 4.4 Paradox of Redundancy
4.4.1 Link Percolation and Robustness 4.4.2 Node Percolation and Robustness; 4.4.3 Blocking Nodes; 4.5 Network Risk; 4.5.1 Crude Oil and KeystoneXL; 4.5.2 MBRA Network Resource Allocation; 4.6 Exercises; Reference; Part III Individual Sectors; Chapter 5 Communications; 5.1 Early Years; 5.2 Regulatory Structure; 5.3 The Architecture of the Communication Sector; 5.3.1 Physical Infrastructure; 5.3.2 Wireless Networks; 5.3.3 Extraterrestrial Communication; 5.3.4 LESs; 5.3.5 Cellular Networks; 5.3.6 Generations; 5.3.7 Wi-Fi Technology; 5.4 Risk Analysis; 5.4.1 Importance of Carrier Hotels
5.4.2 Network Analysis

Sommario/riassunto

""...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 Reviews.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)While the emphasis is on the development of policies that lead to successful prevention of terrorist attacks on the nation's infrastructure, this book is the first scientific