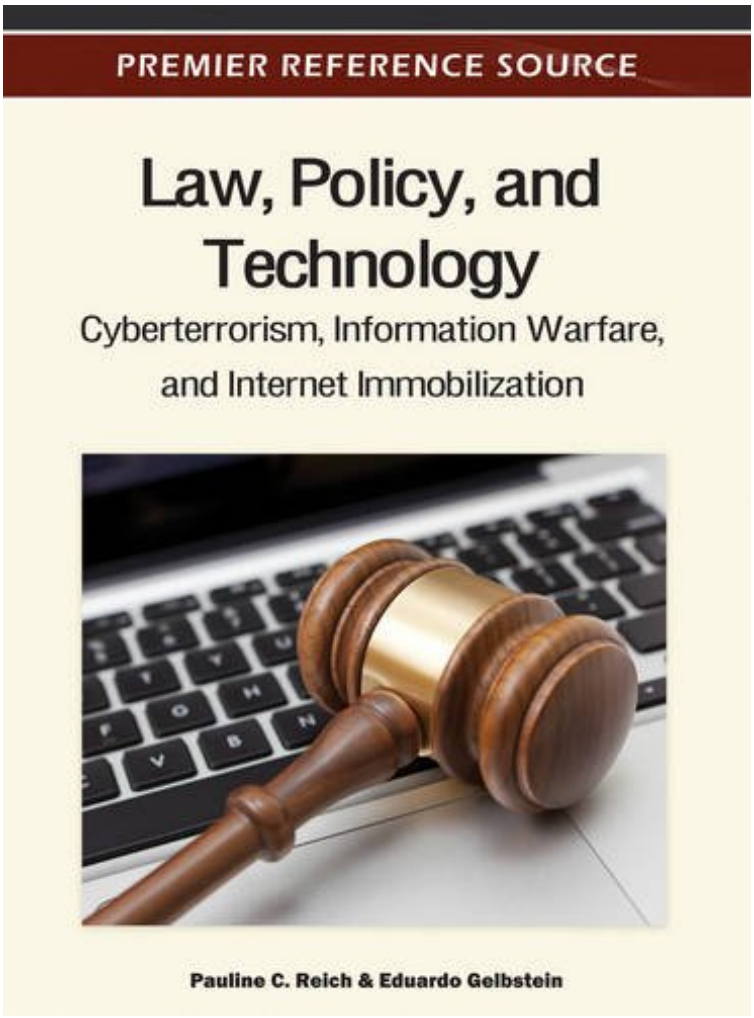
Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization

Pauline C. Reich
*ePub | *DOC | audiobook | ebooks | Download PDF*



#4512883 in Books 2012-02-29Original language:EnglishPDF # 1 11.02 x 1.13 x 8.50l, 3.20 #File Name: 1615208313512 pages | File size: 45.Mb

Pauline C. Reich : Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization before purchasing it in order to gage whether or not it would be worth my time, and all praised Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization:

0 of 0 people found the following review helpful. Understanding cybersecurityBy Kenneth KrechmerThis 2012 book is an excellent source of information and references covering the broad and complex field of cybersecurity. The two authors/editors address the two major perspectives - information and communications technology and legal and then address policy issues from each perspective. This balance between the two major components of any serious study of

cybersecurity is most welcome. The subtitle is, perhaps, overly dramatic. The book addresses both the commercial and governmental aspects of cybersecurity. There is a focus on US law, however the book includes views from other country's perspective, as well. Eleven other contributors provided different views, yet their material was well integrated into the book. This resulted in a readable book where common terminology allowed concepts to be addressed from multiple perspectives.The information and communications focus (Section 1, seven chapters) ably led by E. Gelbstein (Webster University, Switzerland) provides the technology view on cybersecurity, defining terms, describing technical threats, listing many useful web sites, and identifying the applicable international standards as well as consortia developed best cybersecurity practices. The explanation of how to employ the references, standards and specifications that bear on cybersecurity is outstanding. This information is very valuable for anyone looking to understand and manage the cybersecurity risks in an organization.The legal and policy focus (Section 2, nine chapters) ably led by P. Reich (Waseda University, Japan) provides a view on cybersecurity focused on US law but with considerable background on the legal issues associated with cybersecurity around the world. This section is very valuable for those wishing to understand the complex legal issues surrounding cybersecurity. There is a very interesting chapter on China's view of cybersecurity written by a retired US military officer. Ms Reich recognizes and explains the nascent state of the legal framework(s) to address cybersecurity. Chapters 10 through 13 provide considerable information, discussion and background on the very important issue of balancing cybersecurity with a free and open society. This reviewer is not a legal scholar, but the depth of information and references appeared to be significant. Anyone interested in developing or influencing policy on cybersecurity should consider this book a must read.This large 493 page book (8.5 x 11 inch pages) is listed as "premier reference source," a term that this reviewer finds accurate. However, being the reference for a topic as dynamic as cybersecurity deserves a more dynamic medium than a hard copy book. This reviewer recommends this book become a web site (for pay if desired) that is maintained and expanded by these editors. What they have to tell us about cybersecurity is worth reading. The book includes a 41 page alphabetic compilation of the 100's of references from the individual chapters and an index. Full disclosure: the author of this review received a free copy of this book.Ken KrechmerLecturerUniversity of ColoradoBoulder, CO USA

In the information society, technology has become ubiquitous, but its intrinsic vulnerabilities and the complexity of managing mission-critical systems create an attractive target for potential attackers.Law, Policy and Technology: Cyberterorrism, Information Warfare and Internet Immobilization provides relevant frameworks and best practices as well as current empirical research findings in the area. It is aimed at professionals who want to improve their understanding of the impact of cyber-attacks on critical infrastructures and other information systems essential to the smooth running of society, how such attacks are carried out, what measures should be taken to mitigate their impact and what lessons can be learned from the attacks and simulations of the last few years.

Reich (Waseda U., Japan) and Gelbstein (Webster U., Switzerland) compile 16 chapters by law, security, and information professionals from Europe, the US, and Asia, who examine issues in cyber and information security; initiatives in law, policy, and information security to address them; and how to address gaps in these areas. They consider the nature of the problem, the parties that have an interest in disrupting technology infrastructures and computer systems, how attacks take place and how organizations can prepare for them, and when, where, and why they occur. They discuss the main challenges facing security practitioners; the economic, political, and social consequences of information security disruption; the relationship between critical information infrastructure and cyberterrorism; managing risks associated with information assets; standards and best practices; key vulnerabilities; the application of law and policy to actual incidents; the academic literature on cyberterrorism; the nature of cyber threats to government and private computer systems; whether an international solution to cyberterrorism is needed; and case studies from India, China, and the UK. --Annotation 2012 Book News Inc. Portland, ORRecommended - This 2012 book is an excellent source of information and references covering the broad and complex field of cyber security. The two authors/editors address the two major perspectives - information and communications technology and legal. This balance between the two major components of any serious study of cyber security is most welcome. [...] Anyone interested in developing or influencing policy on cyber security should consider this book a must read. What they have to tell us about cyber security is worth reading. --Ken Krechmer, University of Colorado, USAAbout the AuthorProfessor Pauline Reich, American lawyer and professor, writer, arbitrator/mediator, consultant. Director, Asia-Pacific Cyberlaw, Cybercrime and Internet Security Institute, Tokyo, Japan, conducting research, producing publications, providing technical assistance and training for lawyers, judges, prosecutors, police, legislators, businesses, governments in the Asia-Pacific region and worldwide. Speaker at conferences in the United States, Europe and Asia, e.g. APEC Symposium on Information Privacy in E-Government and E-commerce, CSI 2008, RAISE (Regional Asia Information Security Exchange), Business Software Alliance, Cybersecurity Malaysia, Asian Institute of Technology, ITU regional Asia workshop on framework for Cybersecurity and CIIP, BILETA 2010.Dr. Eduardo Gelbstein, Adjunct Professor, Webster University Geneva, former advisor to the United Nations Board of (external) Auditors, former Director, United Nations International Computing Centre and I.T. Strategy Manager,

British Railways Network South East. Author of numerous articles and publications on Information Security and auditing and frequent speaker at international conferences on security and governance in Europe, the Middle East and Africa.