1. Record Nr. UNINA9910962521303321

Autore	Cordesman Anthony H
Titolo	Cyber-threats, information warfare, and critical infrastructure protection : defending the U.S. homeland / / Anthony H. Cordesman with Justin G. Cordesman
Pubbl/distr/stampa	Westport, Conn. : , : Praeger, , 2001 London : , : Bloomsbury Publishing, , 2024
ISBN	9798400636509 9786610373864 9781280373862 1280373865 9780313016196 0313016194
Edizione	[1st ed.]
Descrizione fisica	1 online resource (192 p.)
Altri autori (Persone)	CordesmanJustin G
Disciplina	005.8
Soggetti	Electronic data processing - Security measures - United States Telecommunication - Defense measures - United States Computer networks - Security measures - United States Information warfare - United States
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"Published in cooperation with the Center for Strategic and International Studies, Washington, D.C."
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Cover -- Cyber-threats, Information Warfare, and Critical Infrastructure Protection -- Contents -- Acknowledgments -- Chapter 1 The Changing Nature of Critical Infrastructure Protection -- THE PROBLEM OF EVOLVING TECHNOLOGY -- THE UNCERTAIN BALANCE OF RISKS AND NON-RISKS IN CYBER-ATTACKS -- The Disconnect between Cyber-defense and Cyber-offense -- The Lack of Credible Risk and Vulnerability Assessments -- GOVERNMENTAL AND PRIVATE SECTOR EFFORTS TO RESPOND -- Chapter 2 Threat Assessment -- THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION CHARACTERIZATION OF THE THREAT -- THE NATIONAL INFRASTRUCTURE PROTECTION CENTER'S (NIPC) VIEW OF THE THREAT -- INTELLIGENCE COMMUNITY ASSESSMENTS OF THE THREAT -- CIA

Testimony on the Threat -- National Intelligence Council's Estimate of the Threat -- Incidents of "Cyber-warfare": The Kosovo Crisis -- Serbia's Role in Information Warfare -- NATO's Role in Information Warfare -- Is Information Warfare and Retaliation Legal and Worth Its Costs? -- Lower-Level Incidents of "Cyber-warfare" -- Moonlight Maze -- Solar Sunrise -- Rome Labs Incident -- THE COMPUTER SECURITY INSTITUTE'S SURVEY OF THE THREAT -- COMPUTER EMERGENCY RESPONSE TEAM'S (CERT) ASSESSMENT OF THREAT -- CHALLENGES IN IMPROVING THE ASSESSMENT OF THE THREAT -- Chapter 3 Evolving U. S. Policy and Response -- THE BEGINNINGS: THE COMPUTER SECURITY ACT AND CLINGER-COHEN ACT -- THE FEDERAL GOVERNMENT REDEFINES CRITICAL INFRASTRUCTURE AND AGENCY RESPONSIBILITIES -- Executive Order 13010 -- The President's Commission on Critical Infrastructure Protection -- Presidential Decision Directive-63 (PDD-63) -- Lead Agencies for Sector Liaison -- Lead Agencies for Special Functions -- A New Structure for Interagency Coordination -- National Infrastructure Protection Center (NIPC) -- Information Sharing and Analysis Center (ISAC).
National Infrastructure Assurance Council -- National Infrastructure Assurance Plan -- Studies and Research -- Cooperation with the Private and Civil Sectors -- Annual Report on Implementation -- NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION -- National Plan for Information Systems Protection, Version One -- GAO Comments on the National Plan for Information Systems Protection -- Oplan 3600 -- THE SUCCESS OF THE FEDERAL GOVERNMENT EFFORT TO DATE -- Chapter 4 Analyzing Federal Critical Infrastructure Programs by Department and Agency -- THE NATIONAL PLAN FOR INFORMATION SYSTEMS ESTIMATE -- THE OMB ANALYSIS -- ANNUAL REPORT TO CONGRESS ON COMBATING TERRORISM -- Government-wide Spending on CIP -- EFFORTS BY FEDERAL AGENCIES -- Department of Agriculture -- Department of Commerce -- Critical Infrastructure Assurance Office -- Department of Energy -- Environmental Protection Agency and GAO Audits -- Health and Human Services -- Department of Interior -- Department of Justice -- NASA -- GAO Assessments of NASA Information Security -- NATIONAL SCIENCE FOUNDATION -- NATIONAL SECURITY COMMUNITY -- The Role of the Department of Defense -- Patterns of Attack and Response -- Major DoD Cyber-defense Programs -- GAO Critiques of DoD Efforts: The 1996 Study -- The GAO's 1999 Recommendations -- DoD Progress in Addressing Security Weaknesses -- Cyber and Information Warfare and the Role of the Intelligence Community -- Total Spending on National Security Activity -- Department of State -- Department of Transportation -- Department of Treasury -- Department of Veterans Affairs -- Chapter 5 Assessments of Effectiveness -- INDEPENDENT U.S. GOVERNMENT EFFORTS TO ASSESS RISK, COST, AND BENEFITS: GAO TESTIMONY OF OCTOBER 6, 1999 -- Management Recommendations Within Brock's Testimony.
INDEPENDENT U.S. GOVERNMENT EFFORTS TO ASSESS RISK, COST, AND BENEFITS: GAO TESTIMONY OF MARCH 29, 2000 -- Weaknesses in Controls -- Raise Awareness -- Implement Software Patches -- Routinely Use Automated Tools to Monitor Security -- Identify and Propagate Pockets of Excellence -- Focus on the Most Common Vulnerabilities First -- Enforce a Strong Management Approach -- PRELIMINARY ANALYSIS OF GAO FINDINGS -- OTHER EFFORTS TO ASSESS RISK, COST, AND BENEFITS -- TECHNICAL RISKS, TESTS, AND EVALUATIONS OF IW PROGRAMS -- Chapter 6 Role of State and Local Governments -- Chapter 7 Role of Private Industry -- Chapter 8 Lessons from Other Nations: International Vulnerability -- Chapter 9

Conclusions and Recommendations -- Notes -- About the Authors.

Sommario/riassunto

During the last two decades, the infrastructure of the U.S. economy has undergone a fundamental set of changes. It has steadily increased its reliance on its service sector and high-technology economy. The U.S. has come to depend on computers, electronic data storage and transfers, and highly integrated communications networks. The result is the rapid development of a new form of critical infrastructure--and one that is exceedingly vulnerable to a new family of threats, loosely grouped together as information warfare. This detailed volume examines these threats and the evolving U.S. policy response. After examining the dangers posed by information warfare and efforts at threat assessment, Cordesman considers the growing policy response on the part of various federal agencies, state and local governments, and the private sector. The changing nature of the threats is leading these actors to reassess the role they must play in critical infrastructure protection. Government at all levels, industry, and even friendly and neutral foreign governments are learning that an effective response requires coordination in deterrence, defense, and counterattack.