1. Record Nr. UNINA9910520070203321

Autore	Pavlidis George
Titolo	A brief history of colour theory : foundations of colour science / / George Pavlidis
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	9783030877712 9783030877705
Descrizione fisica	1 online resource (151 pages)
Disciplina	535.6
Soggetti	Color Color (Philosophy)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910713505503321

Titolo	Loudness balance study of selected audiometer earphones : determination of the characteristics of three configurations of TDH-39 earphones used in the first three cycles of the Health Examination Survey and the newer TDH-49 earphone, by the method of loudness balance on human subjects / / Kenneth C. Stewart and Ernest J. Burgi
Pubbl/distr/stampa	Rockville, Maryland : , : U.S. Dept. of Health, Education, and Welfare, Public Health Service, Health Services and Mental Health Administration, , 1970
Descrizione fisica	1 online resource (vi, 37 pages) : illustrations
Collana	Vital and health statistics. Series 2: Data evaluation and methods research ; ; number 40 Public Health Service publication ; ; no. 1000-series 2-no. 40
Soggetti	Audiometry Headphones - United States Hearing levels - United States Hearing levels United States
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"December 1970."
Nota di bibliografia	Includes bibliographical references (page 12).

3.	Record Nr.	UNISA996464400503316
	Titolo	Adversary-aware learning techniques and trends in cybersecurity / / Prithviraj Dasgupta; Joseph B Collins; Ranjeev Mittu
	Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
	ISBN	9783030556921 3-030-55692-1
	Edizione	[1st ed. 2021.]
	Descrizione fisica	1 online resource (X, 227 p. 68 illus., 50 illus. in color.)
	Disciplina	016.391
	Soggetti	Intelligent agents (Computer software) - Security measures Artificial intelligence Computer security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Part I: Game-Playing AI and Game Theory-based Techniques for Cyber Defenses -- 1. Rethinking Intelligent Behavior as Competitive Games for Handling Adversarial Challenges to Machine Learning -- 2. Security of Distributed Machine Learning:A Game-Theoretic Approach to Design Secure DSVM -- 3. Be Careful When Learning Against Adversaries: Imitative Attacker Deception in Stackelberg Security Games -- Part II: Data Modalities and Distributed Architectures for Countering Adversarial Cyber Attacks -- 4. Adversarial Machine Learning in Text: A Case Study of Phishing Email Detection with RCNN model -- 5. Overview of GANs for Image Synthesis and Detection Methods -- 6. Robust Machine Learning using Diversity and Blockchain -- Part III: Human Machine Interactions and Roles in Automated Cyber Defenses -- 7. Automating the Investigation of Sophisticated Cyber Threats with Cognitive Agents -- 8. Integrating Human Reasoning and Machine Learning to Classify Cyber Attacks -- 9. Homology as an Adversarial Attack Indicator -- Cyber-(in)security, revisited: Proactive Cyber-defenses, Interdependence and Autonomous Human Machine Teams (A-HMTs).
	Sommario/riassunto	This book is intended to give researchers and practitioners in the

cross-cutting fields of artificial intelligence, machine learning (AI/ML) and cyber security up-to-date and in-depth knowledge of recent techniques for improving the vulnerabilities of AI/ML systems against attacks from malicious adversaries. The ten chapters in this book, written by eminent researchers in AI/ML and cyber-security, span diverse, yet inter-related topics including game playing AI and game theory as defenses against attacks on AI/ML systems, methods for effectively addressing vulnerabilities of AI/ML operating in large, distributed environments like Internet of Things (IoT) with diverse data modalities, and, techniques to enable AI/ML systems to intelligently interact with humans that could be malicious adversaries and/or benign teammates. Readers of this book will be equipped with definitive information on recent developments suitable for countering adversarial threats in AI/ML systems towards making them operate in a safe, reliable and seamless manner.