1. Record Nr. UNINA9910822035903321

Autore	Shakarian Paulo
Titolo	Introduction to cyber-warfare : a multidisciplinary approach / / Paulo Shakarian, Jana Shakarian, Andrew Ruef ; foreword by Sushil Jajodia
Pubbl/distr/stampa	Amsterdam [Netherlands], : Morgan Kaufmann Publishers, an imprint of Elsevier, 2013 Waltham, MA : , : Syngress, , 2013
ISBN	0-12-407926-1
Edizione	[1st edition]
Descrizione fisica	1 online resource (xvii, 318 pages) : illustrations (some color), map
Collana	Gale eBooks
Disciplina	355.4
Soggetti	Information warfare Cyberterrorism Cyberspace - Security measures Computer crimes Data protection
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front Cover; Introduction to Cyber-Warfare: A Multidisciplinary Approach; Copyright; Contents; Preface; Foreword; Introduction; References; Biography; Chapter 1: Cyber Warfare: Here and Now; What Is Cyber War?; Is Cyber War a Credible Threat?; Attribution, Deception, and Intelligence; Origin; Structure; Purpose; Information Assurance; References; Part: I Cyber Attack; Chapter 2: Political Cyber Attack Comes of Age in 2007; Reliance on Information as a Vulnerability; Rudimentary but Effective: Denial of Service; Leaving Unwanted Messages: Web Site Defacement; Tools for Denial of Service The Difficulty of Assigning Blame: Why Attribution Is Tough in a DDoS AttackEstonia Is Hit by Cyber Attacks; The Estonian Government s Response; The End of the Attacks; General Response to DDoS; Summary; Suggested Further Reading; References; Chapter 3: How Cyber Attacks Augmented Russian Military Operations; The 2008 Russian Cyber Campaign Against Georgia; What Is Interesting About the Russian Cyber Campaign; Objectives of the Attack; Coordination with Conventional Forces; Reconnaissance and Preparation; Attribution;

Preparing for a Cyber-Capable Adversary

Cyber as a Battlefield Operating SystemThe Cyber Aspect of the Area of Interest; Cyber Reconnaissance and Surveillance (R&S); Summary; Suggested Further Reading; References; Chapter 4: When Who Tells the Best Story Wins: Cyber and Information Operations in the Middle East; Hijacking Noncombatant Civilian IP Addresses to Help the War Effort: The Israel-Hezbollah ``July War of 2006; The Information Operations of Hezbollah; Hezbollah Hijacks IP Addresses; Civilians in the Cyber Melee: Operation Cast Lead; IO and Cyber Warfare in the 2008 Israel-Hamas War; Summary; Suggested Further Reading ReferencesChapter 5: Limiting Free Speech on the Internet: Cyber Attack Against Internal Dissidents in Iran and Russia; DDoS as a Censorship Tool: Why Dissident Groups Are Inherently Vulnerable to Cyber Attacks; Silencing Novaya Gazeta and Other Russian Dissidents; Moving to LiveJournal; Possible Motivation for the 2011 DDoS; The Optima/Darkness Botnet; The ``March(es) of Millions ; Iran-How the 2009 Elections Led to Aggressive Cyber Operations; The 2009 Elections; The Iranian Cyber Army (ICA); ICA: Beyond Domain Name Hijacking; Who Controls the ICA?; Alleged Iranian Botnet Strikes The Iranian Cyber PoliceSummary; References; Chapter 6: Cyber Attacks by Nonstate Hacking Groups: The Case of Anonymous and Its Affiliates; ``Chaotic Beginnings: The Chaos Computer Club, CCC; The Roots of the Anon-4chan, 7chan, and Other Message Boards; How We Are Influenced by 4chan: Memes; Anonymous-On Image, Structure, and Motivation; Anonymous-External Connections and Spin Offs; Your Security Is a Joke: LulzSec; Anonymous Modus Operandi; Targeting Governments, Corporations, and Individuals: Notable Hacks on Anonymous; Habbo Hotel Raids; Internet Vigilantism; Project Chanology Arab Spring

Sommario/riassunto

Introduction to Cyber-Warfare: A Multidisciplinary Approach, written by experts on the front lines, gives you an insider's look into the world of cyber-warfare through the use of recent case studies. The book examines the issues related to cyber warfare not only from a computer science perspective but from military, sociological, and scientific perspectives as well. You'll learn how cyber-warfare has been performed in the past as well as why various actors rely on this new means of warfare and what steps can be taken to prevent it.Provides a multi-disciplinary approach t