1. Record Nr. UNINA9910815299503321

Autore	Winterfeld Steve
Titolo	The basics of cyber warfare : understanding the fundamentals of cyber warfare in theory and practice / / Steve Winterfield, Jason Andress
Pubbl/distr/stampa	Boston, : Syngress, c2013
ISBN	9781283810845 1283810840 9780124051812 0124051812
Edizione	[1st edition]
Descrizione fisica	1 online resource (169 p.)
Collana	Syngress basics series The basics of cyber warfare
Altri autori (Persone)	AndressJason
Disciplina	005.8 355.343
Soggetti	Internet - Security measures Computer networks - Security measures Information warfare
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	Half Title; Title page; Copyright; Dedication; Contents; Author Biography; Introduction; 1 Cyber Threatscape; How Did We Get Here?; Attack Methodology Plus Tools/Techniques Used; Attackers (The Types of Threats); How Most Organizations Defend Today (Defensive Mountain Range)?; Targeted Capabilities (What We Should be Defending); Summary; References; 2 Cyberspace Battlefield Operations; What is Cyber Warfare?; Definition for Cyber Warfare; Tactical and Operational Reasons for Cyber War; Cyber Strategy and Power; Cyber Arms Control; Cyber War-Hype or Reality; Boundaries in Cyber Warfare Defense in DepthComputer Controlled Infrastructure; Organizational View; Where Cyber Fits in the War-Fighting Domains; Land; Sea; Air; Space; Cyber Domain; Summary; References; 3 Cyber Doctrine; Current US Doctrine; US Forces; US Air Force; US Navy; US Army; DoD INFOCONs; Sample Doctrine / Strategy From Around the World; Chinese Doctrine; Other Asian countries; European Countries; Private or Mercenary Armies; Some Key Military Principles that Must be Adapted to Cyber Warfare; Intelligence Preparation of the Operational

Environment (IPOE); Joint Munitions Effectiveness Manual (JMEM)
Measures of Effectiveness (MOE)Battle Damage Assessment (BDA); Close Air Support (CAS); Counterinsurgency (COIN); Summary; References; 4 Tools and Techniques; Logical Weapons; Reconnaissance Tools; Scanning Tools; Access and Escalation Tools; Exfiltration Tools; Sustainment Tools; Assault Tools; Obfuscation Tools; Physical Weapons; How the Logical and Physical Realms are Connected; Logical Systems Run on Physical Hardware; Logical Attacks Can Have Physical Effects; Infrastructure Concerns; What is SCADA?; What Security Issues are Present in the World of SCADA?
What are the Consequences of SCADA Failures?Supply Chain Concerns; Compromised Hardware; Deliberately Corrupted Components; Non-Technical Issues; Tools for Physical Attack and Defense; Electromagnetic Attacks; Electromagnetic Pulse (EMP) Weapons; Jamming; Defense Against Conventional Attacks; Summary; References; 5 Offensive Tactics and Procedures; Computer Network Exploitation; Intelligence and Counter-Intelligence; Reconnaissance; Open Source Intelligence; Passive Reconnaissance; Surveillance; Voice Surveillance; Data Surveillance; Large Scale Surveillance Programs
Uses of Surveillance DataComputer Network Attack; Waging War in the Cyber Era; Physical Warfare; Electronic Warfare; Logical Warfare; Reactive vs Proactive Attacks; The Attack Process; Recon; Scan; Access; Escalate; Exfiltrate; Assault; Sustain; Obfuscate; Summary; References; 6 Psychological Weapons; Social Engineering Explained; Is Social Engineering science?; SE Tactics Techniques and Procedures (TTPs); Types of SE approaches; Types of SE methodologies; How the Military Approaches Social Engineering; Army Doctrine; How the Military Defends against Social Engineering; How the Army Does CI
An Air Force Approach

Sommario/riassunto

The Basics of Cyber Warfare provides readers with fundamental knowledge of cyber war in both theoretical and practical aspects. This book explores the principles of cyber warfare, including military and cyber doctrine, social engineering, and offensive and defensive tools, tactics and procedures, including computer network exploitation (CNE), attack (CNA) and defense (CND). Readers learn the basics of how to defend against espionage, hacking, insider threats, state-sponsored attacks, and non-state actors (such as organized criminals and terrorists). Finally, the book looks ahe