1. Record Nr. UNISA996499855403316

Autore	Stoddart Kristan
Titolo	Cyberwarfare : threats to critical infrastructure / / Kristan Stoddart
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	9783030972998 9783030972981
Descrizione fisica	1 online resource (550 pages)
Collana	Palgrave studies in cybercrime and cybersecurity
Disciplina	364.168
Soggetti	Computer crimes - Prevention Computer networks - Security measures Cyberspace operations (Military science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Acknowledgments -- Contents -- Abbreviations and Concepts -- List of Figures -- 1 Introduction -- Cyberwar and Critical Infrastructure -- The Threat Actors -- The Cyber Context: States as Targets and Attackers -- Cybercriminals and Their Usefulness as 'Proxies' and 'Privateers' -- The Threat Landscape -- Machine Learning, Artificial Intelligence, and High Performance (Quantum) Computing -- Critical Infrastructure: ICS and SCADA -- Subdue the Enemy Without Fighting -- Cyber: The Fifth Domain of Warfare -- A Short Guide to Terminology -- Malware -- Cyber Forensics -- Overview -- Notes -- 2 On Cyberwar: Theorizing Cyberwarfare Through Attacks on Critical Infrastructure-Reality, Potential, and Debates -- Introduction -- The Fog of Cyberwar -- What Is Cyberwar(fare)? -- Cyberwar Deconstructed -- Hybrid Warfare -- International Law: JWT and the LOAC -- Rules of Engagement -- The Tallinn Manuals and the Cyberwarfare Debate -- Cyberwar Against Critical Infrastructure as a War Winner -- The Failure of Cyber Deterrence and the Attribution Problem -- Iran -- North Korea -- Policy and Debates in the United States -- The 2018 U.S. National Cyber Strategy: CISA and the Biden Administration -- The U.S. Military and 'Forward Defense' -- Conclusion -- Notes -- 3 Cyberwar:

Attacking Critical Infrastructure -- Introduction -- SCADA Systems and Critical Infrastructure -- Proof-of-Concept: Aurora and Stuxnet -- The Implications of Aurora and Stuxnet -- Real-World Cases -- Electricity Generation and Distribution -- Electricity Producing Sites Include Nuclear Power Stations -- Water Treatment and Sanitation -- Dams and Reservoirs -- The Oil and Gas Industry: Rigs, Refineries, and Pipelines -- Chemical Plants -- Ports and Logistics -- Merchant Shipping -- Road and Rail -- Civil Aviation -- The Good News -- The Bad News -- Ukraine and Russia's 2022 Invasion.
Conclusion -- Notes -- 4 Gaining Access: Attack and Defense Methods and Legacy Systems -- Introduction -- Common Technical Attack Methods -- Drive-by Downloads -- Watering Hole Attacks -- Man-in-the-Middle/Session HIJACKING -- Zero-Days -- Rootkits -- Remote Access Trojans (RATs) -- The Use of Mobile/Cellular Devices and Remote Access -- Script Kiddies or Nation-States? -- Common TTPs -- Counters and Defenses -- Firewalls -- Demilitarized Zones (DMZs) -- Intrusion Detection Systems (IDS): HIDS/SIDS/HIPS -- Honeypots and Honeytraps -- Signature and Behavior-Based Malware Detection -- Sandboxing -- Packet Sniffers -- Application Whitelisting -- Security Information and Event Management -- Blockchain -- Pressing the Reset -- The Zero Trust Security Model -- Legacy Systems: In-Built Vulnerabilities in Critical Infrastructure -- Legacy Systems of the U.S. Government -- Industry and the Costs of 'Keeping the Lights On' -- Patching -- Targeting Supply Chains -- Conclusion -- Notes -- 5 Hacking the Human -- Introduction -- Social Engineering -- Examples of Social Engineering -- Exploiting Cognitive and Behavioral Psychology -- Hacking the Human -- Spear Phishing -- Mitigating Spear Phishing -- Spear Phishing Attack Tools and Websites -- State Intelligence: HUMINT Beyond Social Engineering -- The 'Birds Eye' Macro View and the Micro Level of HUMINT -- Human Sources and Human Agency -- Cyber Defense and Offense -- Defending Insider Threats -- Mitigation and the Insider Threat -- Physical Security I -- Physical Security II: The CIA Triad and 'Full Disclosure' -- The Cybersecurity Workforce Deficit -- Computer Emergency Response Teams -- Cyber Threat Intelligence and the Cybersecurity Community -- Industry and Government Backed Self-Help Groups -- Conclusion -- Notes -- 6 Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers -- Introduction.
Outsider Threats, Insider Threats, and Target Spotting -- Hackers, Hacking Groups, and Social Engineering -- Social Network Analysis -- SNA as a Law Enforcement and Intelligence Tool -- Terrorism -- Encryption and the Risk of 'Going Dark' -- State-Backed/State-Sanctioned Cybercrime -- Cybercriminals and States -- 'Dark Net' Markets -- Organized Crime, Ransomware, and the 'Dark Net' -- WannaCry and Petya/NotPetya -- The Cloak of Attribution: The Use of Proxy Actors by States -- Conclusion -- Notes -- 7 Conclusion -- On Cyberwarfare -- Attacking Critical Infrastructure -- Pinprick Attacks and First Strike -- Cybersecurity Defenses: Risk Management and Legacy Systems -- Hacking the Human -- Reducing Risk -- Risk Management and Resilience -- States as Advanced Persistent Threats -- The U.S. Intelligence Community and a 'Whole of Nation' Effort -- Zugzwang -- Notes -- Bibliography -- Index.