Cyberwarfare Information Operations In A Connected World Jones Bartlett Learning Information Systems Security Assurance Series

Cyber-Security and Information Warfare
Cyber Warfare and Cyber Terrorism
Information Warfare and Security
Cyber Warfare
Offensive Cyber Operations
Information Warfare and Electronic Warfare Systems
The Art of Cyberwarfare
Redefining Information Warfare Boundaries for an Army in a Wireless World
Cybersecurity
Information Warfare
Inside Cyber Warfare
Strategic Warfare in Cyberspace
Cyber Operations
Cyberwar and Information Warfare
Understanding Cyber Warfare
Cyber Warfare – Truth, Tactics, and Strategies
Cyberwarfare: Information Operations in a Connected World
Offensive Cyber Operations
Russian Cyber Operations
Bytes, Bombs, and Spies
Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications
Cyber Warfare and the Laws of War
Cybercrime and Cyber Warfare
Introduction to Cyber-Warfare
Cyber Operations and International Law
21st Century Chinese Cyberwarfare
Cyber War Will Not Take Place
The Basics of Cyber Warfare
Cyber Dragon
Tallinn Manual on the International Law Applicable to Cyber Warfare
The Oxford Handbook of Cyber Security
Hacker Techniques, Tools, and Incident Handling
Cyberwarfare: An Introduction to Information-Age Conflict
Cyberwar 3.0
Information Warfare in the Age of Cyber Conflict

Dark Territory
Evolution of Cyber Technologies and Operations to 2035
Cyberwarfare: Information Operations in a Connected World
Cyberwarfare

LIZETH ANGELICA

Cyber-Security and Information Warfare Cambridge University Press
Cyberspace is one of the major bases of the economic development of industrialized societies and developing. The dependence of modern society in this technological area is also one of its vulnerabilities. Cyberspace allows new power policy and strategy, broadens the scope of the actors of the conflict by offering to both state and non-state new weapons, new ways of offensive and defensive operations. This book deals with the concept of "information war", covering its development over the last two decades and seeks to answer the following questions: is the control of the information space really possible remains or she a utopia? What power would confer such control, what are the benefits?
Cyber Warfare and Cyber Terrorism John Wiley & Sons
The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.
Information Warfare and Security IGI Global
Cyber Warfare Techniques, Tactics and Tools for Security Practitioners provides a comprehensive look at how and why digital warfare is waged. This book explores the participants, battlefields, and the tools and techniques used during today's digital conflicts. The concepts discussed will give students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. Every one of our systems is under attack from multiple vectors - our defenses must be ready all the time and our alert systems must detect the threats every time. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It considers relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Starting with a definition of cyber warfare, the book's 15 chapters discuss the following topics: the cyberspace battlefield; cyber doctrine; cyber warriors; logical, physical, and psychological weapons; computer network exploitation; computer network attack and defense; non-state actors in computer network operations; legal system impacts; ethics in cyber warfare; cyberspace challenges; and the future of cyber war. This book is a valuable resource to those involved in cyber warfare activities, including policymakers, penetration testers, security professionals, network and systems administrators, and college instructors. The information provided on cyber tactics and attacks can also be

used to assist in developing improved and more efficient procedures and technical defenses. Managers will find the text useful in improving the overall risk management strategies for their organizations. - Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks - Dives deeply into relevant technical and factual information from an insider's point of view - Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

Cyber Warfare Oxford University Press
What individuals, corporations, and governments need to know about information-related attacks and defenses! Every day, we hear reports of hackers who have penetrated computer networks, vandalized Web pages, and accessed sensitive information. We hear how they have tampered with medical records, disrupted emergency 911 systems, and siphoned money from bank accounts. Could information terrorists, using nothing more than a personal computer, cause planes to crash, widespread power blackouts, or financial chaos? Such real and imaginary scenarios, and our defense against them, are the stuff of information warfare-operations that target or exploit information media to win some objective over an adversary. Dorothy E. Denning, a pioneer in computer security, provides in this book a framework for understanding and dealing with information-based threats: computer break-ins, fraud, sabotage, espionage, piracy, identity theft, invasions of privacy, and electronic warfare. She describes these attacks with astonishing, real examples, as in her analysis of information warfare operations during the Gulf War. Then, offering sound advice for security practices and policies, she explains countermeasures that are both possible and necessary. You will find in this book: A comprehensive and coherent treatment of offensive and defensive information warfare, identifying the key actors, targets, methods, technologies, outcomes, policies, and laws; A theory of information warfare that explains and integrates within a single framework operations involving diverse actors and media; An accurate picture of the threats, illuminated by actual incidents; A description of information warfare technologies and their limitations, particularly the limitations of defensive technologies. Whatever your interest or role in the emerging field of information warfare, this book will give you the background you need to make informed judgments about potential threats and our defenses against them. 0201433036B04062001

Offensive Cyber Operations Routledge
Conflict in cyberspace is becoming more prevalent in all public and private sectors and is of concern on many levels. As a result, knowledge of the topic is becoming essential across most disciplines. This book reviews and explains the technologies that underlie offensive and defensive cyber operations, which are practiced by a range of cyber actors including state actors, criminal enterprises, activists, and individuals. It explains the processes and technologies that enable the full spectrum of cyber operations. Readers will learn how to use basic tools for cyber security and pen-testing, and also be able to quantitatively assess cyber risk to systems and environments and discern and categorize malicious

activity. The book provides key concepts of information age conflict technical basics/fundamentals needed to understand more specific remedies and activities associated with all aspects of cyber operations. It explains techniques associated with offensive cyber operations, with careful distinctions made between cyber ISR, cyber exploitation, and cyber attack. It explores defensive cyber operations and includes case studies that provide practical information, making this book useful for both novice and advanced information warfare practitioners.

Information Warfare and Electronic Warfare Systems Oxford University Press, USA

This book provides a framework for assessing China's extensive cyber espionage efforts and multi-decade modernization of its military, not only identifying the "what" but also addressing the "why" behind China's focus on establishing information dominance as a key component of its military efforts. China combines financial firepower—currently the world's second largest economy—with a clear intent of fielding a modern military capable of competing not only in the physical environments of land, sea, air, and outer space, but especially in the electromagnetic and cyber domains. This book makes extensive use of Chinese-language sources to provide policy-relevant insight into how the Chinese view the evolving relationship between information and future warfare as well as issues such as computer network warfare and electronic warfare. Written by an expert on Chinese military and security developments, this work taps materials the Chinese military uses to educate its own officers to explain the bigger-picture thinking that motivates Chinese cyber warfare. Readers will be able to place the key role of Chinese cyber operations in the overall context of how the Chinese military thinks future wars will be fought and grasp how Chinese computer network operations, including various hacking incidents, are part of a larger, different approach to warfare. The book's explanations of how the Chinese view information's growing role in warfare will benefit U.S. policymakers, while students in cyber security and Chinese studies will better understand how cyber and information threats work and the seriousness of the threat posed by China specifically.

The Art of Cyberwarfare Newnes

Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

Redefining Information Warfare Boundaries for an Army in a Wireless World Packt Publishing Ltd

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and

logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Cybersecurity Routledge

A practical guide to understanding and analyzing cyber attacks by advanced attackers, such as nation states. Cyber attacks are no longer the domain of petty criminals. Today, companies find themselves targeted by sophisticated nation state attackers armed with the resources to craft scarily effective campaigns. This book is a detailed guide to understanding the major players in these cyber wars, the techniques they use, and the process of analyzing their advanced attacks. Whether you're an individual researcher or part of a team within a Security Operations Center (SoC), you'll learn to approach, track, and attribute attacks to these advanced actors. The first part of the book is an overview of actual cyber attacks conducted by nation-state actors and other advanced organizations. It explores the geopolitical context in which the attacks took place, the patterns found in the attackers' techniques, and the supporting evidence analysts used to attribute such attacks. Dive into the mechanisms of: North Korea's series of cyber attacks against financial institutions, which resulted in billions of dollars stolen The world of targeted ransomware attacks, which have leveraged nation state tactics to cripple entire corporate enterprises with ransomware Recent cyber attacks aimed at disrupting or influencing national elections globally The book's second part walks through how defenders can track and attribute future attacks. You'll be provided with the tools, methods, and analytical guidance required to dissect and research each stage of an attack campaign. Here, Jon DiMaggio demonstrates some of the real techniques he has employed to uncover crucial information about the 2021 Colonial Pipeline attacks, among many other advanced threats. He now offers his experience to train the next generation of expert analysts.

Information Warfare "O'Reilly Media, Inc."

In order to enable general understanding and to foster the implementation of necessary support measures in organizations, this book describes the fundamental and conceptual aspects of cyberspace abuse. These aspects are logically and reasonably discussed in the fields related to cybercrime and

cyberwarfare. The book illustrates differences between the two fields, perpetrators' activities, as well as the methods of investigating and fighting against attacks committed by perpetrators operating in cyberspace. The first chapter focuses on the understanding of cybercrime, i.e. the perpetrators, their motives and their organizations. Tools for implementing attacks are also briefly mentioned, however this book is not technical and does not intend to instruct readers about the technical aspects of cybercrime, but rather focuses on managerial views of cybercrime. Other sections of this chapter deal with the protection against attacks, fear, investigation and the cost of cybercrime. Relevant legislation and legal bodies, which are used in cybercrime, are briefly described at the end of the chapter. The second chapter deals with cyberwarfare and explains the difference between classic cybercrime and operations taking place in the modern inter-connected world. It tackles the following questions: who is committing cyberwarfare; who are the victims and who are the perpetrators? Countries which have an important role in cyberwarfare around the world, and the significant efforts being made to combat cyberwarfare on national and international levels, are mentioned. The common points of cybercrime and cyberwarfare, the methods used to protect against them and the vision of the future of cybercrime and cyberwarfare are briefly described at the end of the book. Contents 1. Cybercrime. 2. Cyberwarfare. About the Authors Igor Bernik is Vice Dean for Academic Affairs and Head of the Information Security Lab at the University of Maribor, Slovenia. He has written and contributed towards over 150 scientific articles and conference papers, and co-authored 4 books. His current research interests concern information/cybersecurity, cybercrime, cyberwarfare and cyberterrorism.

Inside Cyber Warfare Hurst Publishers

A variety of modern research methods in a number of innovating cyber-security techniques and information management technologies are provided in this book along with new related mathematical developments and support applications from engineering. This allows for the exploration of new approaches, useful practices and related problems for further investigation.Distinguished researchers and scientists coming from different scientific origins present their research and views concerning cyber-security, information warfare and communications systems.Graduate students, scientists and engineers interested in a broad spectrum of current theories, methods, and applications in interdisciplinary fields will find this book invaluable.Topics covered include: Electronic crime and ethics in cyberspace, new technologies in security systems/systems interfaces, economic information warfare, digital security in the economy, human factor evaluation of military security systems, cyber warfare, military communications, operational analysis and information warfare, and engineering applications to security systems/detection theory.

Strategic Warfare in Cyberspace John Wiley & Sons

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been

profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.

Addison-Wesley Professional

Cyber-warfare is often discussed, but rarely truly seen. When does an intrusion turn into an attack, and what does that entail? How do nations fold offensive cyber operations into their strategies? Operations against networks mostly occur to collect intelligence, in peacetime. Understanding the lifecycle and complexity of targeting adversary networks is key to doing so effectively in conflict. Rather than discussing the spectre of cyber war, Daniel Moore seeks to observe the spectrum of cyber operations. By piecing together operational case studies, military strategy and technical analysis, he shows that modern cyber operations are neither altogether unique, nor entirely novel. Offensive cyber operations are the latest incarnation of intangible warfare--conflict waged through non-physical means, such as the information space or the electromagnetic spectrum. Not all offensive operations are created equal. Some are slow-paced, clandestine infiltrations requiring discipline and patience for a big payoff; others are short-lived attacks meant to create temporary tactical disruptions. This book first seeks to understand the possibilities, before turning to look at some of the most prolific actors: the United States, Russia, China and Iran. Each has their own unique take, advantages and challenges when attacking networks for effect.

Cyber Operations Jones & Bartlett Learning

Cyberwarfare: Information Operations in a Connected WorldJones & Bartlett Learning

Cyberwar and Information Warfare

Newnes

Insights into the true history of cyber warfare, and the strategies, tactics, and cybersecurity tools that can be used to better defend yourself and your organization against cyber threat. Key FeaturesDefine and determine a cyber-defence strategy based on current and past real-life examplesUnderstand how future technologies will impact cyber warfare campaigns and societyFuture-ready yourself and your business against

any cyber threatBook Description The era of cyber warfare is now upon us. What we do now and how we determine what we will do in the future is the difference between whether our businesses live or die and whether our digital self survives the digital battlefield. Cyber Warfare – Truth, Tactics, and Strategies takes you on a journey through the myriad of cyber attacks and threats that are present in a world powered by AI, big data, autonomous vehicles, drones video, and social media. Dr. Chase Cunningham uses his military background to provide you with a unique perspective on cyber security and warfare. Moving away from a reactive stance to one that is forward-looking, he aims to prepare people and organizations to better defend themselves in a world where there are no borders or perimeters. He demonstrates how the cyber landscape is growing infinitely more complex and is continuously evolving at the speed of light. The book not only covers cyber warfare, but it also looks at the political, cultural, and geographical influences that pertain to these attack methods and helps you understand the motivation and impacts that are likely in each scenario. Cyber Warfare – Truth, Tactics, and Strategies is as real-life and up-to-date as cyber can possibly be, with examples of actual attacks and defense techniques, tools. and strategies presented for you to learn how to think about defending your own systems and data. What you will learnHacking at scale – how machine learning (ML) and artificial intelligence (AI) skew the battlefieldDefending a boundaryless enterpriseUsing video and audio as weapons of influenceUncovering DeepFakes and their associated attack vectorsUsing voice augmentation for exploitationDefending when there is no perimeterResponding tactically to counter-campaign-based attacksWho this book is for This book is for any engineer, leader, or professional with either a responsibility for cyber security within their organizations, or an interest in working in this ever-growing field.

Understanding Cyber Warfare IGI Global

Cyber security is concerned with the identification, avoidance, management and mitigation of risk in, or from, cyber space. The risk concerns harm and damage that might occur as the result of everything from individual carelessness, to organised criminality, to industrial and national security espionage and, at the extreme end of the scale, to disabling attacks against a country's critical national infrastructure. However, there is much more to cyber space than vulnerability, risk, and threat. Cyber space security is an issue of strategy, both commercial and technological, and whose breadth spans the international, regional, national, and personal. It is a matter of hazard and vulnerability, as much as an opportunity for social, economic and cultural growth. Consistent with this outlook, The Oxford Handbook of Cyber Security takes a comprehensive and rounded approach to the still evolving topic of cyber security. The structure of the Handbook is intended to demonstrate how the scope of cyber security is beyond threat, vulnerability, and conflict and how it manifests on many levels of human interaction. An understanding of cyber security requires us to think not just in terms of policy and strategy, but also in terms of technology, economy, sociology, criminology, trade, and morality. Accordingly, contributors to the Handbook include experts in cyber

security from around the world, offering a wide range of perspectives: former government officials, private sector executives, technologists, political scientists, strategists, lawyers, criminologists, ethicists, security consultants, and policy analysts.
Cyber Warfare – Truth, Tactics, and Strategies John Wiley & Sons
This book explores the future of cyber technologies and cyber operations which will influence advances in social media, cyber security, cyber physical systems, ethics, law, media, economics, infrastructure, military operations and other elements of societal interaction in the upcoming decades. It provides a review of future disruptive technologies and innovations in cyber security. It also serves as a resource for wargame planning and provides a strategic vision of the future direction of cyber operations. It informs military strategist about the future of cyber warfare. Written by leading experts in the field, chapters explore how future technical innovations vastly increase the interconnectivity of our physical and social systems and the growing need for resiliency in this vast and dynamic cyber infrastructure. The future of social media, autonomy, stateless finance, quantum information systems, the internet of things, the dark web, space satellite operations, and global network connectivity is explored along with the transformation of the legal and ethical considerations which surround them. The international challenges of cyber alliances, capabilities, and interoperability is challenged with the growing need for new laws, international oversight, and regulation which informs cybersecurity studies. The authors have a multi-disciplinary scope arranged in a big-picture framework, allowing both deep exploration of important topics and high level understanding of the topic. Evolution of Cyber Technologies and Operations to 2035 is as an excellent reference for professionals and researchers working in the security field, or as government and military workers, economics, law and more. Students will also find this book useful as a reference guide or secondary text book.
Cyberwarfare: Information Operations in a Connected World Jones & Bartlett Learning
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 ahead to emerging aspects of cyber security technology and trends, including cloud computing, mobile devices, biometrics and nanotechnology. The Basics of Cyber Warfare gives readers a concise overview of these threats and outlines the ethics, laws and consequences of cyber warfare. It is a valuable resource for policy makers, CEOs and CIOs, penetration testers, security administrators, and students and instructors in information security. - Provides a sound understanding of the tools and tactics used in cyber warfare - Describes both offensive and defensive tactics from an insider's point of view - Presents doctrine and hands-on techniques to understand as cyber

warfare evolves with technology
Offensive Cyber Operations Afcea International Press
"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.
Russian Cyber Operations Georgetown University Press
A comprehensive analysis of strategic information warfare waged via digital means as a distinct concern for the United States and its allies. In the "information age," information systems may serve as both weapons and targets. Although the media has paid a good deal of attention to information warfare, most treatments so far are overly broad and without analytical foundations. In this book Gregory Rattray offers a comprehensive analysis of strategic information warfare waged via digital means as a distinct concern for the United States and its allies. Rattray begins by analyzing salient features of information infrastructures and distinguishing strategic information warfare from other types of information-based competition, such as financial crime and economic espionage. He then establishes a conceptual framework for the successful conduct of strategic warfare in general, and of strategic information warfare in particular. Taking a historical perspective, he examines U.S. efforts to develop air bombardment capabilities in the period between World Wars I and II and compares them to U.S. efforts in the 1990s to develop the capability to conduct strategic information warfare. He concludes with recommendations for strengthening U.S. strategic information warfare defenses.