OMB No. 4501074869786

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

How Cyberwarfare Actually Works Cyber War Explained In 6 Minutes | What Is Cyber War? | Cyber Security For Beginners | Simplilearn Offensive Cyber Operations - A Book Discussion with Daniel Moore Why Cyber Warfare Is The New World War | Future Warfare | Spark Cyber Warfare - Truth, Tactics, and Strategies:... by Dr. Chase Cunningham · Audiobook preview Why Hacking is the Future of War The United States' Most Protected Armies (S3, E5) | America's Book Of Secrets | Full Episode The Age of Cyber Warfare: The Digital Battlefield | Future Warfare Tailored Access Operations: Top-Secret NSA Cyber Warfare Unit Exploring Cyber Security Tools: From Cheap DIY to High-Tech \u0026 The Future of AI in Cyber Security 3 Things I Wish I Knew. DO NOT Go Into Cyber Security Without Knowing! Cyber Warfare: Fighting The Crimes Of The Future (Full Documentary) | Real Crime The Cybersecurity Salary Myth Cyber Attacks | 60 Minutes Full Episodes The Digital Threat To Nations | Secret Wars | Episode 1/2 Mossad: Israel's Secret Warriors | Ep 4 | Full Documentary Why We Shouldn't Underestimate This Spy Network Top 10: Best Books For Hackers Vigilante Hacker Outsmarts Cyber Mafia [4K] | Web Warriors | Spark The Cybersecurity Canon: Must-Reads What Makes Israel So Good at Hacking? Cyber Warfare Engineer – CWE | Prevent Cyber Attacks in the U.S. Navy Timothy Thomas. Understanding Chinese Information Operations. Offensive Cyber Operations: Understanding Intangible Warfare, with Daniel Moore Cyber-Influence: Cyberwar and Psychological Operations Analyzing Chinese Information Operations with Threat Intelligence How to fight back against information warfare | David Troy | TEDxBoston PSYOP Explained – What are Psychological Operations / Military Information Support Operations? CIA Spy EXPLAINS Mossad’s Ruthless Tactics | #shorts Black Hat Asia 2018 Keynote: A Short Course in Cyber Warfare by The Grugq

Information Operations Matters
Information Warfare
Inside Cyber Warfare
21st Century Chinese Cyberwarfare
Cyberwarfare: Information Operations in a Connected World
An Introduction to Information-age Conflict
Cyberwarfare
Bitskrieg
A Multidisciplinary Approach
Cyberwar 3.0
Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare
Bytes, Bombs, and Spies
The Oxford Handbook of Cyber Security
Information Warfare in the Age of Cyber Conflict
The Strategic Dimensions of Offensive Cyber Operations
Strategic Information Warfare
Inside China's Information Warfare and Cyber Operations
Mapping the Cyber Underworld
The Quest for Responsible Security in the Age of Digital Warfare
Cyber Dragon: Inside China's Information Warfare and Cyber Operations
Politics, Policy and Strategy
Human Factors in Information Operations and Future Conflict

Cyberwarfare Information Operations In A Connected World
Jones Bartlett Learning Information Systems Security Assurance Series
OMB No. 4501074869786 edited by

AMIYA HOWE

Information Operations Matters Oxford University Press
A comprehensive analysis of the international law applicable to cyber operations, including a systematic study of attribution, lawfulness and remedies.
Information Warfare Newnes
This book examines the shape, sources and dangers of information warfare (IW) as it pertains to military, diplomatic and civilian stakeholders. Cyber warfare and information warfare are different beasts. Both concern information, but where the former does so exclusively in its digitized and operationalized form, the latter does so in a much broader sense: with IW, information itself is the weapon. The present work aims to help scholars, analysts and policymakers understand IW within the context of cyber conflict. Specifically, the chapters in the volume address the shape of influence campaigns waged across digital infrastructure and in the psychology of democratic populations in recent years by belligerent state actors, from the Russian Federation to the Islamic Republic of Iran. In marshalling evidence on the shape and evolution of IW as a broad-scoped phenomenon aimed at societies writ large, the authors in this book present timely empirical investigations into the global landscape of influence operations, legal and strategic analyses of their role in international politics, and insightful examinations of the potential for democratic process to overcome pervasive foreign manipulation. This book will be of much interest to students of cybersecurity, national security, strategic studies, defence studies and International Relations in general.
Inside Cyber Warfare ABC-CLIO
What people are saying about Inside Cyber Warfare "The necessary handbook for the 21st century." --Lewis Shepherd, Chief Tech Officer and Senior Fellow, Microsoft Institute for Advanced Technology in Governments "A must-read for policy makers and leaders who need to understand the big-picture landscape of cyber war." --Jim Stogdill, CTO, Mission Services Accenture You may have heard about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations Read about China's commitment to penetrate the networks of its technologically superior adversaries as a matter of national survival Find out why many attacks originate from servers in the United States, and who's responsible Learn how hackers are "weaponizing" malware to attack vulnerabilities at the application level
21st Century Chinese Cyberwarfare Rand Corporation
New information technologies have contributed to the emergence of new lifestyles and modern strategic developments, but they have also provided new forms of weapons for all kinds of belligerents. This book introduces the concept of “information warfare”, covering its evolution over the last decade and its developments among several economic and political giants: China, Russia, Japan, India and Singapore. Discussion is then given to the national particularities of these countries, such as how they imagine the concept of information warfare to be, what it comprises and how it interacts with their military doctrine and employment, as well as their specific political, diplomatic and economic contexts. The use of information warfare as a form of attack is also covered, with particular emphasis given to cyberspace, which has become the space for a new war as the tool not only of nations but also terrorists, activists, insurgents, etc. The challenges faced by countries who usually fail in securing their cyberspace (Japan, Singapore, USA, etc.) in terms of national and defence security, and economic and power losses are also covered. The book also introduces several analyses of recent events in terms of cyber attacks and tries to propose interpretations and tools to better understand cyber conflicts: what is merely cyber crime and what is warfare in cyberspace.
Cyberwarfare: Information Operations in a Connected World Cambridge University Press
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. The ultimate objective of the book is to provide a concise text book for university students on science and engineering courses as well as for professional practitioners. principles and physical systems used for harvesting and harnessing of renewable resources and makes comprehensive use of worked examples and problems. Readers will also learn how to effectively calculate the cost and payback time for a given renewable energy plant by understanding the factors affecting the cost of generating electricity from a renewable energy system. The book uses a simplified mathematical approach and provides appropriate background material.
An Introduction to Information-age Conflict Jones & Bartlett Learning
Each era brings with it new techniques and methods of waging a war. While military scholars and experts have mastered land, sea, air and space warfare, time has come that they studied the art of cyberwar too. Our neighbours have acquired the capabilities to undertake this new form of

asymmetric form of warfare. India too therefore needs to acquire the capabilities to counter their threat. Cyber space seems to have invaded every aspect of our life. More and more systems whether public or private are getting automated and networked. This high dependence of our critical infrastructure on Information and Communication Technology exposes it to the vulnerabilities of cyberspace. Enemy now can target such infrastructure through the cyberspace and degrade/ destroy them. This implies that the critical information infrastructure of the country and military networks today are both equally vulnerable to enemy’s cyberattacks. India therefore must protect its critical information infrastructure as she would protect the military infrastructure in the battlefield. Public – Private Partnership model is the only model which would succeed in doing so. While the Government needs to lay down the policies and frame the right laws, private sector needs to invest into cyber security. Organisations at national level and at the level of armed forces need to be raised which can protect our assets and are also capable of undertaking offensive cyber operations. This book is an attempt to understand various nuances of cyber warfare and how it affects our national security. Based on the cyber threat environment, the books recommends a framework of cyber doctrine and cyber strategies as well as organisational structure of various organisations which a nation needs to invest in.

Cyberwarfare

Praeger
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.
Bitskrieg "O'Reilly Media, Inc."
Threatcasting uses input from social science, technical research, cultural history, economics, trends, expert interviews, and even a little science fiction to recognize future threats and design potential futures. During this human-centric process, participants brainstorm what actions can be taken to identify, track, disrupt, mitigate, and recover from the possible threats. Specifically, groups explore how to transform the future they desire into reality while avoiding an undesired future. The Threatcasting method also exposes what events could happen that indicate the progression toward an increasingly possible threat landscape. This book begins with an overview of the Threatcasting method with examples and case studies to enhance the academic foundation. Along with end-of-chapter exercises to enhance the reader's understanding of the concepts, there is also a full project where the reader can conduct a mock Threatcasting on the topic of "the next biological public health crisis." The second half of the book is designed as a practitioner's handbook. It has three separate chapters (based on the general size of the Threatcasting group) that walk the reader through how to apply the knowledge from Part I to conduct an actual Threatcasting activity. This book will be useful for a wide audience (from student to practitioner) and will hopefully promote new dialogues across communities and novel developments in the area. Impending technological advances will widen an adversary's attack plane over the next decade. Visualizing what the future will hold, and what new threat vectors could emerge, is a task that traditional planning mechanisms struggle to accomplish given the wide range of potential issues. Understanding and preparing for the future operating environment is the basis of an analytical method known as Threatcasting. It is a method that gives researchers a structured way to envision and plan for risks ten years in the future.
A Multidisciplinary Approach Cyberwarfare
CyberwarfareJones & Bartlett Publishers

Cyberwar 3.0

IT Governance Ltd
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.

Strategic Concepts and Truths to Help You and Your Organization Survive on the Battleground of Cyber Warfare

Elsevier
From North Korea's recent attacks on Sony to perpetual news reports of successful hackings and criminal theft, cyber conflict has emerged as a major topic of public concern. Yet even as attacks on military, civilian, and commercial targets have escalated, there is not yet a clear set of ethical guidelines that apply to cyber warfare. Indeed, like terrorism, cyber warfare is commonly believed to be a war without rules. Given the prevalence cyber warfare, developing a practical moral code for this new form of conflict is more important than ever. In Ethics and Cyber Warfare, internationally-respected ethicist George Lucas delves into the confounding realm of cyber conflict. Comparing "state-sponsored hacktivism" to the transformative impact of "irregular warfare" in conventional armed conflict, Lucas offers a critique of legal approaches to governance, and outlines a new approach to ethics and "just war" reasoning. Lucas draws upon the political philosophies of Alasdair

MacIntyre, John Rawls, and Jürgen Habermas to provide a framework for understanding these newly-emerging standards for cyber conflict, and ultimately presents a professional code of ethics for a new generation of "cyber warriors." Lucas concludes with a discussion of whether preemptive self-defense efforts - such as the massive government surveillance programs revealed by Edward Snowden - can ever be justified, addressing controversial topics such as privacy, anonymity, and public trust. Well-reasoned and timely, Ethics and Cyber Warfare is a must-read for anyone with an interest in philosophy, ethics, or cybercrime.

Bytes, Bombs, and Spies Jones & Bartlett Learning

“We are dropping cyber bombs. We have never done that before.”—U.S. Defense Department official A new era of war fighting is emerging for the U.S. military. Hi-tech weapons have given way to hi tech in a number of instances recently: A computer virus is unleashed that destroys centrifuges in Iran, slowing that country’s attempt to build a nuclear weapon. ISIS, which has made the internet the backbone of its terror operations, finds its network-based command and control systems are overwhelmed in a cyber attack. A number of North Korean ballistic missiles fail on launch, reportedly because their systems were compromised by a cyber campaign. Offensive cyber operations like these have become important components of U.S. defense strategy and their role will grow larger. But just what offensive cyber weapons are and how they could be used remains clouded by secrecy. This new volume by Amy Zegart and Herb Lin is a groundbreaking discussion and exploration of cyber weapons with a focus on their strategic dimensions. It brings together many of the leading specialists in the field to provide new and incisive analysis of what former CIA director Michael Hayden has called “digital combat power” and how the United States should incorporate that power into its national security strategy.

The Oxford Handbook of Cyber Security

Cambridge University 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.

Information Warfare in the Age of Cyber Conflict ANU E Press

In 2011, Nasser Al-Awlaki, a terrorist on the US 'kill list' in Yemen, was targeted by the CIA. A week later, a military strike killed his son. The following year, the US Ambassador to Pakistan resigned, undermined by CIA-conducted drone strikes of which he had no knowledge or control. The demands of the new, borderless 'gray area' conflict have cast civilians and military into unaccustomed roles with inadequate legal underpinning. As the Department of Homeland Security defends against cyber threats and civilian contractors work in paramilitary roles abroad, the legal boundaries of war demand to be outlined. In this book, former Under Secretary of the Air Force Antonia Chayes examines these new 'gray areas' in counterinsurgency, counter-terrorism and cyber warfare. Her innovative solutions for role definition and transparency will establish new guidelines in a rapidly evolving military-legal environment.

The Strategic Dimensions of Offensive Cyber Operations

John Wiley & Sons

This book explores Australia's prospective cyber-warfare requirements and challenges. It describes the current state of planning and thinking within the Australian Defence Force with respect to Network Centric Warfare, and discusses the vulnerabilities that accompany the use by Defence of the National Information Infrastructure (NII), as well as Defence's responsibility for the protection of the NII. It notes the multitude of agencies concerned in various ways with information security, and argues that mechanisms are required to enhance coordination between them. It also argues that Australia has been laggard with respect to the development of offensive cyber-warfare plans and capabilities. Finally, it proposes the establishment of an Australian Cyber-warfare Centre responsible for the planning and conduct of both the defensive and offensive dimensions of cyber-warfare, for developing doctrine and operational concepts, and for identifying new capability requirements. It argues that the matter is urgent in order to ensure that Australia will have the necessary capabilities for conducting technically and strategically sophisticated cyber-warfare activities by the 2020s. The Foreword has been contributed by Professor Kim C. Beazley, former Minister for Defence (1984--90), who describes it as 'a timely book which transcends old debates on priorities for the defence of Australia or forward commitments, (and) debates about globalism and regionalism', and as 'an invaluable compendium' to the current process of refining the strategic guidance for Australia's future defence policies and capabilities.

Strategic Information Warfare Polity

Print Textbook & Online Course Access: 180-day subscription. Please confirm the ISBNs used in your course with your instructor before placing your order; your institution may use a custom integration or an access portal that requires a different access code. Cyberwarfare: Information Operations in a Connected World puts students on the real-world battlefield of cyberspace! It reviews the role that cyberwarfare plays in modern military operations -- operations in which it has become almost impossible to separate cyberwarfare from traditional warfare. Part 1 discusses the history of cyberwarfare and the variety of new concerns its emergence has fostered--from tactical considerations to the law of armed conflict and protection of civilians. Part 2 discusses how offensive cyberwarfare has become an important part of the modern military arsenal. The rise of the advanced persistent threat has changed the face of cyberwarfare, and military planners must now be conscious of a series of cyberwarfare actions. In response, the defensive strategies that militaries use have evolved to protect themselves against cyber attacks. The concept of defense-in-depth is critical to building a well-rounded defense that will stand up to cyberwarfare events. Part 3 explores the future of cyberwarfare; its interaction with military doctrine; and the Pandora's box opened by recent events, which have set the stage for future cyber attacks.

Inside China's Information Warfare and Cyber Operations Packt Publishing Ltd

This latest revision of the Information Operations Primer provides an overview of Department of Defense (DoD) Information Operations (IO) doctrine and organizations at the joint and individual service levels. It is primarily intended to serve students and staff of the U.S. Army War College as a ready reference for IO information extracted and summarized from a variety of sources. Wherever

possible, Internet websites have been given to provide access to additional and more up-to-date information. This booklet is intentionally UNCLASSIFIED so that the material can be easily referenced during course work, while engaged in exercises, and later in subsequent assignments.This booklet begins with an overview of Information Operations, Strategic Communication and Cyberspace Operations. At each level it describes strategies or doctrine, agencies, organizations, and educational institutions dedicated to the information element of national power. Finally, the document concludes with an IO specific glossary and hyperlinks to information operations, cyberspace operations and strategic communication related websites.CHAPTER I - CONCEPTS * Information Operations * Strategic Communication * Cyberspace and Cyberspace Operations * CHAPTER II - STRATEGIES, GUIDANCE & DOCTRINE * National Strategy and Guidance * U.S. International Strategy for Cyberspace * National Framework for Strategic Communication * Department of Defense Strategy and Guidance * DoD Strategy for Operating in Cyberspace * DoD Report on Strategic Communication * DoD Principles of Strategic Communication * Department of Defense Directive (DoDD) 3600.01 Information Operations * Joint Doctrine * Joint Information Operations Doctrine * Service Doctrine * Army Information Doctrine * Marine Corps Information Operations Doctrine * Navy Information Operations Doctrine * Air Force Information Operations Doctrine * CHAPTER III - ORGANIZATIONS * Department of State * Under Secretary of State for Public Diplomacy and Public Affairs * The Center for Strategic Counterterrorism Communications * National Agencies * National Security Agency (NSA) * Department of Defense * Under Secretary of Defense - Policy (USD(P)) * Assistant Secretary of Defense for Public Affairs - Communication Planning and Integration (CPI) * Department of Defense Chief Information Officer (DoD CIO) * Defense Information Systems Agency (DISA) * Information Assurance Technology Analysis Center (IATAC) * Joint Organizations and Educational Institutions * Joint Staff, Deputy Director for Global Operations (DDGO J39) * Joint Spectrum Center (JSC) * Joint Public Affairs Support Element (JPASE) * Joint Information Operations Warfare Center (JIOWC) * U.S. Strategic Command (USSTRATCOM) * U.S. Cyber Command (USCYBERCOM) * U.S. Special Operations Command (USSOCOM) * Joint Forces Staff College - Information Operations Program * Information Operations Center for Excellence Naval Postgraduate School * Service Organizations * Army Cyber Command/2nd Army * Army - 1st Information Operations Command (1st IO Cmd) * Army Reserve Information Operations Command (ARIOC) * United States Army Information Proponent Office (USAIPO) * Marine Corps Information Operations Center * Navy Information Operations Organizations * Air Force Intelligence, Surveillance and Reconnaissance Agency * Headquarters 24th Air Force * 624th Operations Center * 67th Network Warfare Wing * 688th Information Operations Wing * 689th Combat Communications Wing * Glossary * Information Operations, Cyberspace, and Strategic Communication Related Websites

Mapping the Cyber Underworld

Newnes

Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare. Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade

The Quest for Responsible Security in the Age of Digital Warfare ABC-CLIO

A no-nonsense treatment of information operations, this handbook makes clear what does and does not fall under information operations, how the military plans and executes such efforts, and what the role of IO ought to be in the war of ideas. Paul provides detailed accounts of the doctrine and practice of the five core information operations capabilities (psychological operations, military deception, operations security, electronic warfare, and computer network operations) and the three related capabilities (public affairs, civil-military operations, and military support to public diplomacy). The discussion of each capability includes historical examples, explanations of tools and forces available, and current challenges faced by that community. An appendix of selected excerpts from military doctrine ties the work firmly to the military theory behind information operations. Paul argues that contemporary IO's mixing of capabilities focused on information content with those focused on information systems conflates apples with the apple carts. This important study concludes that information operations would be better poised to contribute to the war of ideas if IO were reorganized, separating content capabilities from systems capabilities and separating the employment of black (deceptive or falsely attributed) information from white (wholly truthful and correctly attributed) information.

Cyber Dragon: Inside China's Information Warfare and Cyber Operations Potomac Books, Inc.

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