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

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.

Cyber weapons and cyber warfare have become one of the most dangerous innovations of recent years, and a significant threat to national security. Cyber weapons can imperil economic, political, and military systems by a single act, or by multifaceted orders of effect, with wide-ranging potential consequences. Unlike past forms of warfare circumscribed by centuries of just war tradition and Law of Armed Conflict prohibitions, cyber warfare occupies a particularly ambiguous status in the conventions of the laws of war. Furthermore, cyber attacks put immense pressure on conventional notions of sovereignty, and the moral and legal doctrines that were developed to regulate them. This book, written by an unrivalled set of experts, assists in proactively addressing the ethical and legal issues that surround cyber warfare by considering, first, whether the Laws of Armed Conflict apply to cyberspace just as they do to traditional warfare, and second, the ethical position of cyber warfare against the background of our generally recognized moral traditions in armed conflict. The book explores these moral and legal issues in three categories. First, it addresses foundational questions regarding cyber attacks. What are they and what does it mean to talk about a cyber war? The book presents alternative views concerning whether the laws of war should apply, or whether transnational criminal law or some other peacetime framework is more appropriate, or if there is a tipping point that enables the laws of war to be used. Secondly, it examines the key principles of jus in bello to determine how they might be applied to cyber-conflicts, in particular those of proportionality and necessity. It also investigates the distinction between civilian and combatant in this context, and studies the level of causation necessary to elicit a response, looking at the notion of a 'proximate cause'. Finally, it analyzes the specific operational realities implicated by particular regulatory regimes. This book is unmissable reading for anyone interested in the impact of cyber warfare on international law and the laws of war.

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 to cyber-warfare, analyzing the information technology, military, policy, social, and scientific issues that are in play Presents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents within a state (Russia, Iran) Explores cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and LulzSec Covers cyber-attacks directed against infrastructure, such as water treatment plants and power-grids, with a detailed account of Stuxent

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.

Competing National Perspectives

Cyber Conflict

Strategic Information Warfare

Doctrine and Practice : a Reference Handbook

Mapping the Cyber Underworld

Developments in Information Security and Cybernetic Wars

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.

As internet technologies continue to advance, new types and methods of data and security breaches threaten national security. These potential breaches allow for information theft and can provide footholds for terrorist and criminal organizations. Developments in Information Security and Cybernetic Wars is an essential research publication that covers cyberwarfare and terrorism globally through a wide range of security-related areas. Featuring topics such as crisis management, information security, and governance, this book is geared toward practitioners, academicians, government officials, military professionals, and industry professionals.

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

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.

Cyber-Security and Information Warfare

Cyber Warfare

Inside China's Information Warfare and Cyber Operations

Information Warfare

The New Challenge of Cyberwarfare

The Basics of Cyber Warfare

“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.

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.

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

Today, cyber security, cyber defense, information warfare andcyber warfare issues are among the most relevant topics both at thenational and international level. All the major states of the worldare facing cyber threats and trying to understand how cyberspacecould be used to increase power. Through an empirical, conceptual and theoretical approach, CyberConflict has been written by researchers and experts in the fieldsof cyber security, cyber defense and information warfare. It aimsto analyze the processes of information warfare and cyber warfarethrough historical, operational and strategic perspectives of cyberattack. It is original in its delivery because of itsmultidisciplinary approach within an international framework, withstudies dedicated to different states – Canada, Cuba, France,Greece, Italy, Japan, Singapore, Slovenia and South Africa –describing the state’s application of information warfareprinciples both in terms of global development and“local” usage and examples. Contents 1. Canada’s Cyber Security Policy: a Tortuous Path Towarda Cyber Security Strategy, Hugo Loiseau and Lina Lemay. 2. Cuba: Towards an Active Cyber-defense, Daniel Ventre. 3. French Perspectives on Cyber-conflict, Daniel Ventre. 4. Digital Sparta: Information Operations and Cyber-warfare inGreece, Joseph Fitsanakis. 5. Moving Toward an Italian Cyber Defense and Security Strategy,Stefania Ducci. 6. Cyberspace in Japan’s New Defense Strategy, DanielVentre. 7. Singapore’s Encounter with Information Warfare: FilteringElectronic Globalization and Military Enhancements, AlanChong. 8. A Slovenian Perspective on Cyber Warfare, Gorazd Praprotnik,Iztok Podbregar, Igor Bernik and Bojan Ticar. 9. A South African Perspective on Information Warfare and CyberWarfare, Brett van Niekerk and Manoj Maharaj. 10. Conclusion, Daniel Ventre

Print Bundle

Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare

Myths and Realities of Cyber Warfare: Conflict in the Digital Realm

Human Factors in Information Operations and Future Conflict

Cyberwarfare: Information Operations in a Connected World

Redefining Information Warfare Boundaries for an Army in a Wireless World

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. • Provides a detailed overview and thorough analysis of Chinese cyber activities • Makes extensive use of Chinese-language materials, much of which has not been utilized in the existing Western literature on the subject • Enables a better understanding of Chinese computer espionage by placing it in the context of broader Chinese information warfare activities • Analyzes Chinese military modernization efforts, providing a context for the ongoing expansion in China's military spending and reorganization • Offers readers policy-relevant insight into Chinese military thinking while maintaining academic-level rigor in analysis and source selection

"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.

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

The modern means of communication have turned the world into an information fishbowl and, in terms of foreign policy and national security in post-Cold War power politics, helped transform international power politics. Information operations (IO), in which time zones are as important as national boundaries, is the use of modern technology to deliver critical information and influential content in an effort to shape perceptions, manage opinions, and control behavior. Contemporary IO differs from traditional psychological operations practiced by nation-states, because the availability of low-cost high technology permits nongovernmental organizations and rogue elements, such as terrorist groups, to deliver influential content of their own as well as facilitates damaging cyber-attacks ("hactivism") on computer networks and infrastructure. As current vice president Dick Cheney once said, such technology has turned third-class powers into first-class threats. Conceived as a textbook by instructors at the Joint Command, Control, and Information Warfare School of the U.S. Joint Forces Staff College and involving IO experts from several countries, this book fills an important gap in the literature by analyzing under one cover the military, technological, and psychological aspects of information operations. The general reader will appreciate the examples taken from recent history that reflect the impact of IO on U.S. foreign policy, military operations, and government organization.

Introduction to Cyber-Warfare

Hacker Techniques, Tools, and Incident Handling

Information Warfare in the Age of Cyber Conflict

Inside Cyber Warfare

Bytes, Bombs, and Spies

Espionage, Strategy, and Politics in the Digital Domain

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.

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.

New technologies are changing how we protect our citizens and wage our wars. Among militaries, everything taken for granted about the ability to maneuver and fight is now undermined by vulnerability to “weapons of mass disruption”: cutting-edge computer worms, viruses,

and invasive robot networks. At home, billions of household appliances and other “smart” items that form the Internet of Things risk being overtaken, then added to the ranks of massive, malicious “zombie” armies. The age of Bitskrieg is here, bringing vexing threats that range from the business sector to the battlefield. In this new book, world-renowned cyber security expert John Arquilla looks unflinchingly at the challenges posed by cyberwarfare – which he argues have neither been met nor mastered. He offers fresh solutions for protecting against enemies that are often anonymous, unpredictable and capable of projecting force and influence vastly disproportionate to their size, strength or wealth. The changes called for require radical rethinking of military and security affairs, diplomacy, even the routines of our daily lives.

"Examines cyberspace threats and policies from the vantage points of China and the U.S"--

Cyber Warfare – Truth, Tactics, and Strategies

21st Century Chinese Cyberwarfare

A New Face of War

A Multidisciplinary Approach

Cyber Dragon: Inside China's Information Warfare and Cyber Operations

Bitskrieg

This ambitious work which took the better part of a decade to produce will be essential reading for all serious defence study students, and of absorbing interest to military professionals and lay people concerned with the future of warfare and all aspects of response to military attack. Its ultimate aim is to demonstrate that the advent of Cyberwarfare has pushed traditional legal thinking regarding the regulation of forcible action beyond traditional boundaries. It attempts to do so by critically analyzing specific characteristics which are inherent to Cyberwarfare such as stealth, speed, untraceability, the availability to State as well as Non-State sponsored agents, their defiance of traditional borders, and an unprecedented potential for destruction, all of which have played a major role in making obsolescent traditional legal norms relied upon for the effective regulation of the use of force. It follows from the above that no defence system can be effectively regulated, especially one as new and unconventional as Information Warfare, unless all its specific aspects are explored as deeply as possible.The best means to achieve such a purpose have been deemed to be through the inclusion as well as the careful analysis of as many real life examples of Information Warfare operations as possible in order to illustrate the special nature of Information Warfare and its various individual features. The examples compiled for inclusion have been selected not on the basis of being the most recent, but on the basis of their factual background being as fully known as possible. Consequently, this book has been constructed around the concept of legality, starting with a section outlining currently existing legal norms of individual self-defense, then applying those norms to Information Warfare Operations including a presentation of existing international legal instruments with provisions applicable to Information Warfare which could serve as additional essential guidelines for a future legal framework specifically crafted to regulate the use of force in cyberspace. Last but not least this book sets a paradigm with regard to Cyberwarfare as well as with other methods of warfare which escape the boundaries of the traditional State monopoly of the use of force.It ultimately shows the extent to which traditional legal thinking, which is shaped around the premise of regulating typical forms of State forcible action, when faced with such methods of warfare is totally obsolete.

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.

This textbook offers an accessible introduction to the historical, technical, and strategic context of cyber conflict. The international relations, policy, doctrine, strategy, and operational issues associated with computer network attack, computer network exploitation, and computer network defense are collectively referred to as cyber warfare. This new textbook provides students with a comprehensive perspective on the technical, strategic, and policy issues associated with cyber conflict as well as an introduction to key state and non-state actors. Specifically, the book provides a comprehensive overview of these key issue areas: the historical emergence and evolution of cyber warfare, including the basic characteristics and methods of computer network attack, exploitation, and defense; a theoretical set of perspectives on conflict in the digital age from the point of view of international relations (IR) and the security studies field; the current national perspectives, policies, doctrines, and strategies relevant to cyber warfare; and an examination of key challenges in international law, norm development, and the potential impact of cyber warfare on future international conflicts. This book will be of much interest to students of cyber conflict and other forms of digital warfare, security studies, strategic studies, defense policy, and, most broadly, international relations.

CyberwarfareJones & Bartlett Publishers

Information Operations in a Connected World, Wgu Custom Edition

Right to National Self-Defense

Information Operations

Understanding Cyber Warfare

Capabilities and Related Policy Issues

Politics, Policy and Strategy

This illuminating book examines and refines the commonplace "wisdom" about cyber conflict—its effects, character, and implications for national and individual security in the 21st century. "Cyber warfare" evokes different images to different people. This book deals with the technological aspects denoted by "cyber" and also with the information operations connected to social media's role in digital struggle. The author discusses numerous mythologies about cyber warfare, including its presumptively instantaneous speed, that it makes distance and location irrelevant, and that victims of cyber attacks deserve blame for not defending adequately against attacks. The author outlines why several widespread beliefs about cyber weapons need modification and suggests more nuanced and contextualized conclusions about how cyber domain hostility impacts conflict in the modern world. After distinguishing between the nature of warfare and the character of wars, chapters will probe the widespread assumptions about cyber weapons themselves. The second half of the book explores the role of social media and the consequences of the digital realm being a battlespace in 21st-century conflicts. The book also considers how trends in computing and cyber conflict impact security affairs as well as the practicality of people's relationships with institutions and trends, ranging from democracy to the Internet of Things. Provides an overview of the numerous myths and realities associated with all aspects of cyber warfare Explains how the leveraging of social media shapes political discourse and frays cultural norms Shows how advanced persistent threats engage in espionage against critical infrastructure Reveals how individuals and criminal groups conduct an array of nefarious cyber activities with wide-ranging levels of skill

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.

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.

21st Century Chinese Cyberwarfare draws from a combination of business, cultural, historical and linguistic sources, as well as the author's personal experience, to attempt to explain China to the uninitiated. The objective of the book is to present the salient information regarding the use of cyber warfare doctrine by the People's Republic of China to promote its own interests and enforce its political, military and economic will on other nation states. The threat of Chinese Cyberwarfare can no longer be ignored. It is a clear and present danger to the experienced and innocent alike and will be economically, societally and culturally changing and damaging for the nations that are targeted.

Its Implications on National Security

Cybercrime and Cyber Warfare

Information Operations, Electronic Warfare, and Cyberwar

Information Warfare and Security

Cyberwar 3.0

Cyberwarfare: An Introduction to Information-Age Conflict

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

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.

A comprehensive analysis of the international law applicable to cyber operations, including a systematic study of attribution, lawfulness and remedies.

This book provides an up-to-date, accessible guide to the growing threats in cyberspace that affects everyone from private individuals to businesses to national governments.

Techniques, Tactics and Tools for Security Practitioners

Warfare and the Hard Reality of Soft Power

Understanding the Fundamentals of Cyber Warfare in Theory and Practice

Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World

Cyberwarfare

Borderless Wars

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.

Future U.S. national security strategy is likely to be profoundly affected by the ongoing, rapid evolution of cyberspace--the global information infrastructure--and in particular by the growing dependence of the U.S. military and other national institutions and infrastructures on potentially vulnerable elements of the U.S. national information infrastructure. To examine these effects, the authors conducted a series of exercises employing a methodology known as the Day After ... in which participants are presented with an information warfare crisis scenario and asked to advise the president on possible responses. Participants included senior national security community members and representatives from security-related telecommunications and information-systems industries. The report synthesizes the exercise results and presents the instructions from the exercise materials in their entirety.

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.

"In the U.S. Army as elsewhere, transmission of digitized packets on Internet-protocol and space-based networks is rapidly supplanting the use of old technology (e.g., dedicated analog channels) when it comes to information sharing and media broadcasting. As the Army moves forward with these changes, it will be important to identify the implications and potential boundaries of cyberspace operations. An examination of network operations, information operations, and the more focused areas of electronic warfare, signals intelligence, electromagnetic spectrum operations, public affairs, and psychological operations in the U.S. military found significant overlap that could inform the development of future Army doctrine in these areas. In clarifying the prevailing boundaries between these areas of interest, it is possible to predict the progression of these boundaries in the near future. The investigation also entailed developing new definitions that better capture this overlap for such concepts as information warfare. This is important because the Army is now studying ways to apply its cyber power and is reconsidering doctrinally defined areas that are integral to operations in cyberspace. It will also be critical for the Army to approach information operations with a plan to organize and, if possible, consolidate its operations in two realms: the psychological, which is focused on message content and people, and the technological, which is focused on content delivery and machines."--Page 4 of cover.

China and Cybersecurity

Civil Military Disorder and Legal Uncertainty

In Information Warfare Operations

Law and Ethics for Virtual Conflicts

The Strategic Dimensions of Offensive Cyber Operations

U. S. Army War College Information Operations Primer - Fundamentals of Information Operations - Botnet, Stuxnet, Cyber Warfare, NSA, Service Organizations

Part of the Jones & Bartlett Learning Information Systems Security & Assurance Series Cyberwarfare puts students on the real-world battlefield of cyberspace! Students will learn the history of cyberwarfare, techniques used in both offensive and defensive information warfare, and how cyberwarfare is shaping military doctrine. Written by subject matter experts, this book combines accessible explanations with realistic experiences and case studies that make cyberwar evident and understandable. Key Features: - Incorporates hands-on activities, relevant examples, and realistic exercises to prepare readers for their future careers. - Includes detailed case studies drawn from actual cyberwarfare operations and tactics. - Provides fresh capabilities information drawn from the Snowden NSA leaks

Cyberwarfare with Navigate 2 Essentials

Cyber Warfare and Cyber Terrorism

Cyber Operations and International Law

Cyber War