Cyberwar And Information Warfare

Cyberwarfare, like the seismic shift of policy with nuclear warfare, is modifying warfare into non-war warfare. A few distinctive characteristics of cyberwar emerge. Cyberwarfare has blurred the distinction between adversary and ally. Cyber probes continuously occur between allies and enemies alike, causing cyberespionage to merge with warfare. Espionage, as old as war itself, has technologically merged with acts of cyberwar as states

threaten each other with prepositioned malware in each other's cyberespionage probed infrastructure. These two cyber shifts to warfare are agreed upon and followed by the US, Russia and China. What is not agreed upon in this shifting era of warfare are the policies upon which cyberwarfare is based. This book charts the policies in three key actors and navigates the futures of policy on an international stage. Essential reading for students of war studies and security professionals alike.

Cyberspace, where information--and hence serious value--is stored and

manipulated, is a tempting target. An attacker could be a person, group, or state and may disrupt or corrupt the systems from which cyberspace is built. When states are involved, it is tempting to compare fights to warfare, but there are important differences. The author addresses these differences and ways the United States protect itself in the face of attack.

This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning interstate cyber

aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare – given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt down – has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120

states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary engagement. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks

are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks, both as international uses of force and as part of an on-going armed conflict, and the ethical implications of cyber warfare. This book will be of great interest to students of cyber warfare, cyber security, military ethics, international law, security studies and IR in general.

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.
As virtually every aspect of society becomes increasingly dependent on information and communications technology, so our vulnerability to attacks on this technology increases. This is a major theme of this collection of leading edge research papers. At the same time there is another side to this issue, which is if the technology can be used against society by the purveyors of malware etc.,

then technology may also be used positively in the pursuit of society's objectives. Specific topics in the collection include Cryptography and Steganography, Cyber Antagonism, Information Sharing Between Government and Industry as a Weapon, Terrorist Use of the Internet, War and Ethics in Cyberspace to name just a few. The papers in this book take a wide ranging look at the more important issues surrounding the use of information and communication technology as it applies to the security of vital systems that can have a major impact on the

functionality of our society. This book includes leading contributions to research in this field from 9 different countries and an introduction to the subject by Professor Julie Ryan from George Washington University in the USA.

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.

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. 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

The Quest for Responsible Security in the Age of Digital Warfare

Understanding the Fundamentals of Cyber

Warfare in Theory and Practice
Cyber Conflict in the International System
Cybercrime and Cyber Warfare
Cyber Warfare and Cyber Terrorism
The Next Threat to National Security and What to Do About It
The Anatomy of the Global Security Threat
Cyberdeterrence and Cyberwar
The Basics of Cyber Warfare
Law and Ethics for Virtual Conflicts
Techniques, Tactics and Tools for Security Practitioners
Cyber War

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

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 Features Define and determine a cyber-defence strategy based on current and past real-life examples Understand how future technologies will impact cyber warfare campaigns and society Future-ready yourself and your

business against any cyber threat Book 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 learn Hacking at scale – how machine learning (ML) and artificial intelligence (AI) skew the battlefield Defending a boundaryless enterprise Using video and audio as weapons of influence Uncovering DeepFakes and their associated attack vectors Using voice augmentation for exploitation Defending when there is no perimeter Responding tactically to counter-campaign-based attacks Who 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.
Provides information on the ways individuals, nations, and groups are using the Internet as an attack platform.
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

This book features a wide spectrum of the latest computer science research relating to cyber warfare, including military and policy dimensions. It is the first book to explore the scientific foundation of cyber warfare and features research from the areas of artificial intelligence, game theory, programming languages, graph theory and more. The high-level approach and emphasis on

scientific rigor provides insights on ways to improve cyber warfare defense worldwide. Cyber Warfare: Building the Scientific Foundation targets researchers and practitioners working in cyber security, especially government employees or contractors. Advanced-level students in computer science and electrical engineering with an interest in security will also find this content valuable as a secondary textbook or reference. Reviews of the First Edition: "The book raises important points and makes a strong case for more coordinated government and private sector efforts to address the information war problem effectively. Recommended"--Choice "A strong

addition to current events and international issues collections, recommended"--Midwest Book Review "Extensive factual research...provides ample references in this detailed research...an eye opening expose that details the working of the Chinese government...fascinating "--Slashdot China's information war against the United States is clever technically, broadly applied and successful. The intelligence community in the U.S. has publicly stated this is a kind of war we do not know how to fight--yet it is the U.S. military that developed and expanded the doctrine of information war. In fact, the U.S. military is at a disadvantage because it is part of a democratic, decentralized

system of government that separates the state from commercial business. China's political systems are more easily adapted to this form of warfare, as their recent land seizures in the South China Sea demonstrate. We call this annexation, when it is a new form of conquest.

"All political and military conflicts now have a cyber dimension, the size and impact of which are difficult to predict. Internet-enabled propaganda, espionage, and attacks on critical infrastructure can target decision makers, weapons systems, and citizens in general, during times of peace or war. Traditional threats to national security now have a digital delivery

mechanism which would increase the speed, diffusion, and power of an attack. There have been no true cyber wars to date, but cyber battles of great consequence are easy to find. This book is divided into two sections--Strategic viewpoints and Technical challenges & solutions--and highlights the growing connection between computer security and national security"--P. 4 of cover.

"In January 2014 Pope Francis called the Internet a "gift from God." Months later former Secretary of Defense, Leon Panetta, described cyber warfare as "the most serious threat in the 21st century," capable of destroying our entire infrastructure and crippling the

nation. Already, cyber warfare has impacted countries around the world: Estonia in 2007, Georgia in 2008, and Iran in 2010; and, as with other methods of war, cyber technology has the ability to be used not only on military forces and facilities, but on civilian targets.Our computers have become spies and tools for terrorism, and a have allowed for a new, unchecked method of war.And yet, cyber warfare is still in its infancy, with inumerable possibilities and contingencies for how such a war may play out in the coming decades. Cyber War Taboo?: The Evolution of Norms for Emerging-Technology Weapons, from Chemical Weapons to Cyber Warfare examines the international

development of constraining norms for cyber warfare and and predicts how those norms will unfold in the future. Using case studies for other emerging-technology weapons--chemical and biological weapons, strategic bombing, and nuclear weapons--author Brian Mazanec expands previous definitions of norm evolution theory and offers recommendations for citizens and U.S. policymakers and as they grapple with the impending reality of cyber war"--

Information Warfare in the Age of Cyber Conflict

Introduction to Cyber-Warfare A Multidisciplinary Approach

Tallinn Manual on the International Law Applicable to Cyber Warfare

The move on the part of the US military, which began in 1996, to Network-Centric Warfare (NCW), meant the combination of sensor grids, C&C grids, and precision targeting to increase speed to command, and represented a military

offset. Along with networking comes exposure to cyber attacks, attacks that will be used in future wars.

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

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.

"Published in the United Kingdom in 2013 by C. Hurst & Co. (Publishers) Ltd"--Title page verso.

This book offers an overview of the ethical problems posed by Information Warfare, and of the different approaches and methods

used to solve them, in order to provide the reader with a better grasp of the ethical conundrums posed by this new form of warfare. The volume is divided into three parts, each comprising four chapters. The first part focuses on issues pertaining to the concept of Information Warfare and the clarifications that need to be made in order to address its ethical implications. The second part collects contributions focusing on Just War Theory and its application to the case of Information Warfare. The third part adopts alternative approaches to Just War Theory for analysing the ethical implications of this phenomenon. Finally, an afterword by Neelie Kroes - Vice President of

the European Commission and European Digital Agenda Commissioner - concludes the volume. Her contribution describes the interests and commitments of the European Digital Agenda with respect to research for the development and deployment of robots in various circumstances, including warfare. 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.

Cyber warfare has become more pervasive and more complex in recent years. It is difficult to regulate, as it holds an ambiguous position within the laws of war. This book investigates the legal and ethical ramifications of cyber war, considering which sets of laws apply to it, and how it fits into traditional ideas of armed conflict.

"What Valeriano and Maness provide in this book is an empirically-grounded discussion of the reality of cyber conflict, based on an analysis of cyber incidents and disputes experienced by international states since 2001. They delineate patterns of cyber conflict to develop a larger theory of cyber war that gets at the processes leading to cyber conflict.

They find that, in addition to being a little-used tactic, cyber incidents thus far have been of a rather low-level intensity and with few to no long-term effects. Interestingly, they also find that many cyber incidents are motivated by regional conflict. They argue that restraint is the norm in cyberspace and suggest there is evidence this norm can influence how the tactic is used in the future. In conclusion, the authors lay out a set of policy recommendations for proper defense against cyber threats that is built on restraint and regionalism"--

Cyberwar Policy in the United States, Russia and China

The Secret History of Cyber War

The Strategic Dimensions of

An analysis of the status of computer network attacks in international law.

This unique project takes a socio-

political approach to the widely debated issue of cyber-war, considering changing patterns of conflict, international diplomacy and governmental thinking in the face of the emerging threat. In examining whether an example of cyber war has yet been seen, a number of case studies are explored, from the explosion of a Soviet pipeline in the latter stages of the Cold War; to the 2007 attacks on Estonia; and the recent discovery of the Stuxnet worm in an Iranian nuclear plant. This highly accessible study attempts to demystify technical concepts, and will appeal to scholars, practitioners and interested observers involved in the study of this most contemporary of security threats.

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

"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 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.

This text introduces the concepts of information warfare from a non-military, organizational perspective. It is designed to stimulate managers to develop policies, strategies, and tactics for the aggressive use and defence of their data and knowledge base. The book covers the full gambit of information warfare subjects from the direct attack on computer systems to

the more subtle psychological technique of perception management. It provides the framework needed to build management strategies in this area. The topics covered include the basics of information warfare, corporate intelligence systems, the use of deception, security of systems, modes of attack, a methodology to develop defensive measures, plus specific issues associated with information warfare. This book will be of interest to executives and managers in any public or private organization. Specifically, managers or staff in the areas of information technology, security, knowledge management, public relations, or marketing should find it directly useful. Its main

purpose is to make readers aware of the new world of information saturation; thus decreasing the chance that they will become victims of those abusing the information age, whilst at the same time increasing their chances of benefiting from the new opportunities produced. Addresses the issues and implications of cyber warfare and how it directly impacts on companies

A Multidisciplinary Analysis
The Chinese Information War
Shadow Warfare
International Norms for Emerging-Technology Weapons
Cyberwarfare
What Everyone Needs to Know
Building the Scientific

Foundation
Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare
Information Warfare
Inside Cyber Warfare
Cyber War Will Not Take Place
Bytes, Bombs, and Spies

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.

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

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.

An essential, eye-opening book about cyberterrorism, cyber war, and the next great threat to our national security. "Cyber War may be the most important book about national security policy in the last several years." –Slate Former presidential advisor and counter-terrorism expert Richard A. Clarke sounds a timely and chilling warning about America's vulnerability in a terrifying new international conflict.

Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. It explains clearly and convincingly what cyber war is, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. Every concerned American should read this startling and explosive book that offers an insider's view of White House 'Situation Room' operations and carries the reader to the frontlines of our cyber

defense. Cyber War exposes a virulent threat to our nation's security. Understand the challenges of implementing a cyber warfare strategy and conducting cyber warfare. This book addresses the knowledge gaps and misconceptions of what it takes to wage cyber warfare from the technical standpoint of those with their hands on the keyboard. You will quickly appreciate the difficulty and complexity of executing warfare within the cyber domain. Included is a

detailed illustration of cyber warfare against the backdrop of national and international policy, laws, and conventions relating to war. Waging Cyber War details technical resources and activities required by the cyber war fighter. Even non-technical readers will gain an understanding of how the obstacles encountered are not easily mitigated and the irreplaceable nature of many cyber resources. You will walk away more informed on how war is conducted from a cyber perspective, and

perhaps why it shouldn't be waged. And you will come to know how cyber warfare has been covered unrealistically, technically misrepresented, and misunderstood by many. What You'll Learn Understand the concept of warfare and how cyber fits into the war-fighting domain Be aware of what constitutes and is involved in defining war and warfare as well as how cyber fits in that paradigm and vice versa Discover how the policies being put in place to plan and conduct cyber warfare reflect a lack of

understanding regarding the technical means and resources necessary to perform such actions Know what it means to do cyber exploitation, attack, and intelligence gathering; when one is preferred over the other; and their specific values and impacts on each other Be familiar with the need for, and challenges of, enemy attribution Realize how to develop and scope a target in cyber warfare Grasp the concept of self-attribution: what it is, the need to avoid it, and its impact See what goes into

establishing the access from which you will conduct cyber warfare against an identified target Appreciate how association affects cyber warfare Recognize the need for resource resilience, control, and ownership Walk through the misconceptions and an illustrative analogy of why cyber warfare doesn't always work as it is prescribed Who This Book Is For Anyone curious about warfare in the era of cyber everything, those involved in cyber operations and cyber warfare, and security practitioners and policy or

decision makers. The book is also for anyone with a cell phone, smart fridge, or other computing device as you are a part of the attack surface.

Originally published in hardcover in 2016 by Simon & Schuster.

Integrating empirical, conceptual, and theoretical approaches, thisbook presents the thinking of researchers and experts in the fieldsof cybersecurity, cyberdefense, and information warfare. The aim of this book is to analyze the processes of

informationwarfare and cyberwarfare through the historical, operational andstrategic perspectives of cyberattacks. Cyberwar and Information Warfare is of extreme use to experts insecurity studies and intelligence studies, defense universities,ministries of defense and security, and anyone studying politicalsciences, international relations, geopolitics, informationtechnologies, etc.

Technical Challenges and Operational Constraints

Cybersecurity
Cyber Operations and International Law
Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World
Understanding Cyber Warfare
Cyber Warfare
Cyber Warfare – Truth, Tactics, and Strategies
Ethics and Cyber Warfare
Waging Cyber War
Cyber Warfare and the Laws of War