# Cyber Wars A 21st Century Disease Bringing A New Bdo

**Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is little agreement about how they will be deployed, how effective they can be, and how they can be managed. Written by leading scholars, the fourteen case studies in this volume will help policymakers, scholars, and students make sense of contemporary cyber conflict through historical analogies to past military-technological problems. The chapters are divided into three groups. The first—What Are Cyber Weapons Like?—examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision striking compares with earlier technologies for such missions. The second section—What Might Cyber Wars Be Like?—explores how lessons from several wars since the early nineteenth century, including the World Wars, could apply—or not—to cyber conflict in the twenty-first century. The final section—What Is Preventing and/or Managing Cyber Conflict Like?—offers lessons from past cases of managing threatening actors and technologies.**

**This book examines the key dimensions of 21st century war, and shows that orthodox thinking about war, particularly what it is and how it is fought, needs to be updated. Accelerating societal, economic, political and technological change affects how we prepare, equip and organise for war, as well as how we conduct war – both in its low-tech and high-tech forms, and whether it is with high intensity or low intensity. The volume examines changes in warfare by investigating the key features of the conduct of war during the first decades of the 21st century. Conceptually centred around the terms 'kinetic', 'connected' and 'synthetic', the analysis delves into a wide range of topics. The contributions discuss hybrid warfare, cyber and influence activities, machine learning and artificial intelligence, the use of armed drones and air power, the implications of the counterinsurgency experiences in Iraq, Afghanistan and Syria, as well as the consequences for law(fare) and decision making. This work will be of much interest to students of military and strategic studies, security studies and International Relations. Chapters 1, 2, 5, and 19 of this book are freely available as a downloadable Open Access PDF under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 license available at https://www.routledge.com/The-Conduct-of-War-in-the-21st-Century-Kinetic-Connected-and-Synthetic/Johnson-Kitzen-Sweijs/p/book/9780367515249**

**Choice to wage war is a political matter. This choice translates into the prosecution of war which is an operational matter. Use of force will continue to be a driver of state power. There is a need for an ongoing and sustained professional study of inter-state wars from the operational and military dimension. From a study of the operational dimensions of war, relevant lessons and insights can be discerned. The study of lessons also depends on how a country and its society see war and its future. In a welcome trend of reduction of wars, it is incumbent to record and analyse in order to observe the change in the character of war. Military capabilities matter. Countries and regions where wars have taken place have one important attribute- battle and operational experience. The monograph examines 21st century wars in Afghanistan, Iraq, Lebanon, Georgia and Libya. New trend of cyber war is also included. Key highlights have been extracted and distilled into lessons to be learnt.**

**This reference work examines how sophisticated cyber-attacks and innovative use of social media have changed conflict in the digital realm, while new military technologies such as drones and robotic weaponry continue to have an impact on modern warfare. • Provides fascinating information about cyber weapons that effectively strike through cyberspace to weaken and even cripple its target • Demonstrates how social media is employed in conflicts in innovative ways, including communication, propaganda, and psychological warfare • Explores potential technology avenues related to ensuring the continued military advantages of the United States • Identifies and describes nuclear, precision, and other technological capabilities that have historically been the preserve of superpowers but have been newly acquired by various states**

**ECCWS 2015**

**How Conflicts in Cyberspace are Challenging America and Changing the World**

**Cyber Warfare and Cyber Terrorism**

**21st European Conference on Cyber Warfare and Security**

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

**Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities**

An exhaustive and comprehensive probing into the vast universe of cyber terrorism and the havoc it can wreak. With many pages of references and data, these insights into the reach of cyberspace from the private sector to world governments will open your eyes to the evolving landscape of internet security.

Hackers reported as working on behalf of the Russian Government have attacked a wide variety of American citizens and institutions. They include political organizations of both parties, the Republican National Committee and the Democratic National Committee, as well as prominent Democrat and Republican leaders, as well as civil society groups like various American universities and academic research programs. These attacks started years back, but it continued after the 2016 election. They have been reported as hitting government sites, like the Pentagon's email system, as well as private networks, like U.S. banks. They have also been reported as targeting a wide variety of American allies ranging from government, military, and civilian targets, and states that range from Norway to the United Kingdom, as well as now trying to influence upcoming elections in Germany, France, and the Netherlands. In cyberspace, the malevolent actors presently engaged in attacks on U.S. persons and institutions range from criminals who are stealing personal information or holding ransom valuable corporate data to governments, like China, which have been accused of large-scale intellectual property theft, as well as breaking into government databases like the OPM [Office of Personnel Management] in the cyber version of traditional espionage. What can be done to defend America in this challenging realm? As long as we use the internet, adversaries like Putin's Russia and many others will seek to exploit this technology and our dependence on it in realms that range from politics to business to warfare itself. In response, the United States can build a new set of approaches to deliver true cybersecurity, aiming to better protect ourselves while reshaping adversary attitudes and options, or we can continue to be a victim.

An authoritative, single-volume introduction to cybersecurity addresses topics ranging from phishing and electrical-grid takedowns to cybercrime and online freedom, sharing illustrative anecdotes to explain how cyberspace security works and what everyday people can do to protect themselves. Simultaneous.

This book examines cyberspace superiority in nation-state conflict from both a theoretical and a practical perspective. This volume analyses superiority concepts from the domains of land, maritime, and air to build a model that can be applied to cyberspace. Eight different cyberspace conflicts between nation states are examined and the resulting analysis is combined with theoretical concepts to present the reader with a conclusion. Case studies include the conflict between Russia and Estonia (2007), North Korea and the US and South Korea (2009) and Saudi Arabia and Iran in the Aramco attack (2012). The book uses these case studies to examine cyberspace superiority as an analytical framework to understand conflict in this domain between nation-states. Furthermore, the book makes the important distinction between local and universal domain superiority, and presents a unique model to relate this superiority in all domains, as well as a more detailed model of local superiority in cyberspace. Through examining the eight case studies, the book develops a rigorous system to measure the amount of cyberspace superiority achieved by a combatant in a conflict, and seeks to reveal if cyberspace superiority proves to be a significant advantage for military operations at the tactical, operational, and strategic levels. This book will be of much interest to students of cyber-conflict, strategic studies, national security, foreign policy and IR in general.

Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century

International Conflict and Cyberspace Superiority

Cyber Warfare and the Laws of War

A Multidisciplinary Analysis

Theory and Practice

21st Century Chinese Cyberwarfare

Cyberwars in the Middle East argues that hacking is a form of online political disruption whose influence flows vertically in two directions (top-bottom or bottom-up) or horizontally. These hacking activities are performed along three political dimensions: international, regional, and local. Author Ahmed Al-Rawi argues that political hacking is an aggressive and militant form of public communication employed by tech-savvy individuals, regardless of their affiliations, in order to influence politics and policies. Kenneth Waltz's structural realism theory is linked to this argument as it provides a relevant framework to explain why nation-states employ cyber tools against each other. On the one hand, nation-states as well as their affiliated hacking groups like cyber warriors employ hacking as offensive and defensive tools in connection to the cyber activity or inactivity of other nation-states, such as the role of Russian Trolls disseminating disinformation on social media during the US 2016 presidential election. This is regarded as a horizontal flow of political disruption. Sometimes, nation-states, like the UAE, Saudi Arabia, and Bahrain, use hacking and surveillance tactics as a vertical flow (top-bottom) form of online political disruption by targeting their own citizens due to their oppositional or activists' political views. On the other hand, regular hackers who are often politically independent practice a form of bottom-top political disruption to address issues related to the internal politics of their respective nation-states such as the case of a number of Iraqi, Saudi, and Algerian hackers. In some cases, other hackers target ordinary citizens to express opposition to their political or ideological views which is regarded as a horizontal form of online political disruption. This book is the first of its kind to shine a light on many ways that governments and hackers are perpetrating cyber attacks in the Middle East and beyond, and to show the ripple effect of these attacks.

Former secretary of defense Leon Panetta once described cyber warfare as "the most serious threat in the twenty-first century," capable of destroying our entire infrastructure and crippling the nation. Already, major cyber attacks have affected countries around the world: Estonia in 2007, Georgia in 2008, Iran in 2010, and most recently the United States. As with other methods of war, cyber technology can be used not only against military forces and facilities but also against civilian targets. Information technology has enabled a new method of warfare that is proving extremely difficult to combat, let alone defeat. And yet cyber warfare is still in its infancy, with innumerable possibilities and contingencies for how such conflicts may play out in the coming decades. Brian M. Mazanec examines the worldwide development of constraining norms for cyber war and predicts how those norms will unfold in the future. Employing case studies of other emerging-technology weapons--chemical and biological, strategic bombing, and nuclear weaponry--Mazanec expands previous understandings of norm-evolution theory, offering recommendations for U.S. policymakers and citizens alike as they grapple with the reality of cyber terrorism in our own backyard.

Conflict in cyberspace is not a new phenomenon, but the legality of hostile cyber activity at a state level remains imperfectly defined. While the United States and its allies are in general agreement on the legal status of conflict in cyberspace, China, Russia, and a number of like-minded nations have an entirely different concept of the applicability of international law to cyberspace. This e-book presents the opposed views of USA and Russia on cyber security. Ultimately, you can find out from the official report how cyber-attack can jeopardize national security in the latest attack performed by the Russian hackers in order to interfere with the 2016 U.S. elections.

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

The Evolution of Cyber War

War, Sabotage, and Fear in the Cyber Age

ECCWS 2018 17th European Conference on Cyber Warfare and Security V2

Cybersecurity

The Perfect Weapon

Weapons and Warfare: From Ancient and Medieval Times to the 21st Century [2 volumes]

**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**

**This book consists of the testimony before the House Armed Services Committee on March 1, 2017 and provides insight into the extent of the cyber threat facing our nation. The witnesses discuss the policies that got us to where we are today and possible changes that could bolster our defenses against cyber-attacks. The book includes the full written statements submitted as well as the responses to questions submitted by House Committee members post-hearing.**

**Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited**

**Cyber warfare in the 21st century : threats, challenges, and opportunities : Committee on Armed Services, House of Representatives, One Hundred Fifteenth Congress, first session, hearing held March 1, 2017.**

**Threats, Challenges, and Opportunities : Committee on Armed Services, House of Representatives, One Hundred Fifteenth Congress, First Session, Hearing Held March 1, 2017**

**To Whom does the 21st Century Belong?**

**A History**

**Threats, Challenges, and Opportunities**

**ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015**

**Cyber Conflicts and Small States**

*Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs*

*"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 innumerable 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 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"--*

*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.*

*This work covers major weapons throughout human history, beginning with clubs and maces; through crossbows, swords, and gunpowder; up to the hypersonic railgun, lasers, and robotic weapons under development today. Weapons and Warfare is designed to provide students with a comprehensive and highly informative overview of weapons and their impact on the course of human history. In addition to providing basic factual information, this encyclopedia will delve into the greater historical context and significance of each weapon. The chronological organization by time period will enable readers to fully understand the evolution of weapons throughout history. The work begins with a foreword by a top scholar and a detailed introductory essay by the editor that provides an illuminating historical overview of weapons. It then offers entries on more than 650 individual weapons systems. Each entry has sources for further reading. The weapons are presented alphabetically within six time periods, ranging from the prehistoric and ancient periods to the contemporary period. Each period has its own introduction that treats the major trends occurring in that era. In addition, 50 sidebars offer fascinating facts on various weapons. Numerous illustrations throughout the text are also included. Includes an informative foreword on the impact of weapons on tactics by distinguished historian British Army Major General Mungo Melvin (Retired) Offers individual introductory essays to each of the six chronological sections of the book Provides concise studies, written distinguished military historians, of more than 650 important weapons systems Features 50 sidebars that supply interesting insights related to the employment of various weapons*

*Should There Be Rules Regarding the Rise of Cyber-Warfare Techniques by Rival Nations*

*21st Century Cyber Warfare*

*Inside Cyber Warfare*

*International Norms for Emerging-Technology Weapons*

*Cyber Warfare in the 21st Century*

*Operational Lessons of the Wars of 21st Century*

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.

Military doctrine of The People's Republic of China (PRC) envisages war being waged in five spheres: land, sea, air, outer space and cyberspace. The PRC believes that the early degradation, or destruction, of an enemy's command and control infrastructure will significantly improve its chances of ultimate victory. But the Chinese 21st century approach to cyberwarfare is both more sophisticated and comprehensive than that. This book examines the military background to today's doctrines, and explores how the teachings of Sun Tzu (The Art of War), the Thirty-Six Principles from the Warring States era and the hard-learnt lessons of Mao's Long March infuse and support the modern state's approach to engaging with enemies and rivals. Chinese cyberwarriors, operating from behind the Great Firewall of China, have substantial campaign experience, and this book reviews operations from Titan Rain - sustained multi-year cyberattacks against the US that started in 2003 - to the most recent, ShadyRAT.This book also reviews the contributions made to the overall Chinese cyberstrategy by civilian hackers and state-owned enterprises and looks at how Advanced Persistent Threats already undermine many of China's rival states and enterprises. China's rivals lack a coherent cyberstrategy of their own. They also do not understand the complex cultural, political and historical routes of the modern Chinese state and this is a significant weakness. This book helps everyone with an interest in cybersecurity to 'know their enemy'. William Hagestad II is an internationally-recognized expert on the Chinese People's Liberation Army & Government information warfare. He advises international intelligence organizations, military flag officers and multi-national commercial enterprises with regard to their internal IT security governance and external security policies. The linguistic, historical, cultural, economic and military aspects of Chinese cyberwarfare are his forte.

The probability of a world-wide cyber conflict is small. Yet the probability of forms of cyber conflict, regional or even global, could be argued as being very high. Small countries are usually signatories to military and economic alliances with major world powers but rely heavily on the technical ability of these powers in protecting their own national interests. They may be considered to be IT 'technology colonies'. Their cyber infrastructure is usually fully imported and their ability to assess it is limited. This book poses the question: to what extent should, or can, a small country prepare itself for handling the broad range of cyber threats? Looking at cyber-warfare, cyber-terrorism, cyber-crime and associated concerns, national experts from New Zealand, Australia, The Netherlands, and Poland present analyses of cyber-defence realities, priorities and options for smaller countries. They show that what is needed is the ability of small nations to be able to define and prepare appropriate responses such as the role of military/law enforcement/business entities, continuity and resilience strategies, incident response and business continuity plans and more for handing nationally-aimed cyber-attacks particularly where these address national critical infrastructures.

Originally published: New York: Crown Publishers, 2018. Updated with a new chapter.

Its Implications on National Security

International Conflicts in Cyberspace - Battlefield of the 21st Century

Cyber Attacks at State Level, Legislation of Cyber Conflicts, Opposite Views by Different Countries on Cyber Security Control & Report on the Latest Case of Russian Hacking of Government Sectors

Testimony Before the House Committee on Armed Services

The Conduct of War in the 21st Century

This paper will try to answer this question, posed by the title. But, we want to start with the idea that cyber-warfare may be construed to be more than it is. The psychological effects of cyber-warfare may be greater than the real issue, particularly as its interpreted by the media. Another question that comes up is how do we begin to examine a question of law, where little information exists? Now that we're in the 21st century, it's long overdue to fully examine this issue. Although, more than a decade has passed since discussion of this issue began, there are still many questions. What if this thought, this idea, is being "psychologically built" into the minds of people; manipulation? What happens when it becomes a self-fulfilling prophecy? I think it's important to begin any discussion of this type with a "what do you mean by attitude". In other words, for us to provide a positive communication environment it's important that we begin by defining certain terms. Let's begin with cyberspace. What is cyberspace? What is, in fact, the meaning of this space? And if cyberspace can really be understood as space, what its resultant role of architecture in this still largely unknown realm? Is all reality then necessarily becoming virtual reality? Who are the architects of cyberspace, and which designing principles should they follow? And if there are really architects involved, why are the contemporary examples of virtual reality environments nowadays then still characterized as banal? Moreover, what does it actually mean to design cyberspace? Which urban metaphors are implemented in the virtual realm, so that in some way familiar notions become apparent in this abstract and technological world? Is cyberspace a novel departure or an extension – perhaps the final extension – of the trajectory of abstraction and dematerialization that has characterized so much modern art, architecture and human experience?

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

These essays of Mansoor Palloor aim at the sharp and flagrant disclosure of the brutal atrocities committed by imperialistic forces on the human race and the blatant violation of basic human rights. Those who derive boundless sadistic pleasure in the unbearable stench of burnt human flesh and blood and who consider the woeful cries of pain and misery of children with dismembered bodies and their mentally ailing mothers, as sweet music to their ears, are definitely at full liberty to disagree with his views. The articles in this book, which throw light on international trends since the year 2001, impeccably forecast and predict global events like the Middle East conflicts and wars, the rise of the Internet community and its far-reaching impact in shaping the future, the economic collapse of America, the fall of capitalism, and the recent political developments and unrest in the Middle East.

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.

Mapping the Cyber Underworld

Cyberspace and the "First Battle" in 21st-century War

What Everyone Needs to Know

Virtual Terror

Cyber War Will Not Take Place

The Future of War

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.

Wars often start well before main forces engage. In the 19th and early 20th centuries, combat often began when light cavalry units crossed the border. For most of the 20th century, the "first battle" typically involved dawn surprise attacks, usually delivered by air forces. While a few of these attacks were so shattering that they essentially decided the outcome of the struggle or at least dramatically shaped its course -- the Israeli air force's attack at the opening of the June 1967 Six-Day War comes to mind -- in most cases the defender had sufficient strategic space -- geographic and/or temporal -- to recover and eventually redress the strategic balance to emerge victorious. The opening moments of World War II for Russia and the United States provide two examples. The first battle in the 21st century, however, may well be in cyberspace. Coordinated cyber attacks designed to shape the larger battlespace and influence a wide range of forces and levers of power may become the key feature of the next war. Early forms of this may have already been seen in Estonia and Georgia. Control of cyberspace may thus be as decisive in the network-dependent early 21st century as control of the air was for most of the 20th century. In the future, cyber attacks may be combined with other means to inflict paralyzing damage to a nation's critical infrastructure as well as psychological operations designed to create fear, uncertainty, and doubt, a concept we refer to as "infrastructure and information operations." The cyber sphere itself is, of course, a critical warfighting domain that hosts countless information infrastructures, but the rise of network-based control systems in areas as diverse as the power grid and logistics has widened the threat posed by network attacks on opposing infrastructures. Given the increasing dependence of the U.S. military and society on critical infrastructures, this cyber-based first battle is one that we cannot afford to lose. And yet we might.

The information revolution has transformed both modern societies and the way in which they conduct warfare. Cyber Warfare and the Laws of War analyses the status of computer network attacks in international law and examines their treatment under the laws of armed conflict. The first part of the book deals with the resort to force by states and discusses the threshold issues of force and armed attack by examining the permitted responses against such attacks. The second part offers a comprehensive analysis of the applicability of international humanitarian law to computer network attacks. By examining the legal framework regulating these attacks, Heather Harrison Dinniss addresses the issues associated with this method of attack in terms of the current law and explores the underlying debates which are shaping the modern laws applicable in armed conflict.

An award-winning military historian, professor, and political adviser delivers the definitive story of warfare in all its guises and applications, showing what has driven and continues to drive this uniquely human form of political violence. Questions about the future of war are a regular feature of political debate, strategic analysis, and popular fiction. Where should we look for new dangers? What cunning plans might an aggressor have in mind? What are the best forms of defense? How might peace be preserved or conflict resolved? From the French rout at Sedan in 1870 to the relentless contemporary insurgencies in Iraq and Afghanistan, Lawrence Freedman, a world-renowned military thinker, reveals how most claims from the military futurists are wrong. But they remain influential nonetheless. Freedman shows how those who have imagined future war have often had an idealized notion of it as confined, brief, and decisive, and have regularly taken insufficient account of the possibility of long wars-hence the stubborn persistence of the idea of a knockout blow, whether through a dashing land offensive, nuclear first strike, or cyberattack. He also notes the lack of attention paid to civil wars until the West began to intervene in them during the 1990s, and how the boundaries between peace and war, between the military, the civilian, and the criminal are becoming increasingly blurred. Freedman's account of a century and a half of warfare and the (often misconceived) thinking that precedes war is a challenge to hawks and doves alike, and puts current strategic thinking into a bracing historical perspective.

Kinetic, Connected and Synthetic

Computer Crimes, Laws, and Policing in the 21st Century

Cyberwars in the Middle East

Cyber Warfare: A Documentary and Reference Guide

Cyber Operations and International Law

ICCWS 2022 17th International Conference on Cyber Warfare and Security

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

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.

"Cyber war is coming," announced a land-mark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain? Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways. The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponised code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country's critical infrastructure? How serious is the threat of "pure" cyber espionage, of exfiltrating data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?

"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.

Fourteen Analogies

Understanding Cyber Conflict

Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology

Cyber Warfare