Cyber War The Next Threat To National Security And What To Do About It

With the increased dependence on digital and internet technologies, cyber security has come to be regarded as a national security issue, and the number of countries with a published cyber security strategy continues to rise. But these national cyber security strategies often run the risk of failing to address all the cyber security requirements of the many institutions within a given country, and the complex nature of the stakeholders involved and the networks formed by them means that the problem requires an interdisciplinary approach. This book presents papers from the NATO Advanced Research Workshop (ARW) entitled "A Framework for a Military Cyber Defense Strategy", held in Norfolk, Virginia, USA, in April 2016. The workshop focused on key priority areas for cyber defense along with NATO's cyber defense policy implementation and brought together experts with an eclectic mix of backgrounds and specialties from a group of NATO member states and partner countries. The participants considered not only the technical implications of cyber security efforts, but also the legal, strategic, educational and organizational aspects, and the book reflects this wide view of the field and its intricacies, highlighting the complexity of cyber security and the many challenges it presents. This overview of cyber security offers state-of-the-art approaches from a multidisciplinary standpoint, and will be of interest to all those working in the field.

Conflict and Cooperation in Cyberspace: The Challenge to National Security brings together some of the world's most distinguished military leaders, scholars, cyber operators, and policymakers in a discussion of current and future challenges that cyberspace poses to the United States and the world. Maintaining a focus on policy-relevant solutions, it offers a well-reasoned study of how to prepare for war, while attempting to keep the peace in the cyberspace domain. The discussion begins with thoughtful contributions concerning the attributes and importance of cyberspace to the American way of life and global prosperity. Examining the truths and myths behind recent headline-grabbing malicious cyber activity, the book spells out the challenges involved with establishing a robust system of monitoring, controls, and sanctions to ensure cooperation amongst all stakeholders. The desire is to create a domain that functions as a trusted and resilient environment that fosters cooperation, collaboration, and commerce. Additionally, the book: Delves into the intricacies and considerations cyber strategists must contemplate before engaging in cyber war Offers a framework for determining the best ways to engage other nations in promoting global norms of behavior Illustrates technologies that can enable cyber arms control agreements Dispels myths surrounding Stuxnet and industrial control systems General Michael V. Hayden, former director of the National Security Agency and the Central Intelligence Agency, begins by explaining why the policymakers, particularly those working on cyber issues, must come to understand the policy implications of a dynamic domain. Expert contributors from the Air Force Research Institute, MIT, the Rand Corporation, Naval Postgraduate School, NSA, USAF, USMC, and others examine the challenges involved with ensuring improved cyber security. Outlining the larger ethical, legal, and policy challenges facing government, the private sector, civil society, and individual users, the book offers plausible solutions on how to create an environment where there is confidence in the ability to assure national security, conduct military operations, and ensure a vibrant and stable global economy.

An urgent warning from two bestselling security experts--and a gripping inside look at how governments, firms, and ordinary citizens can confront and contain the tyrants, hackers, and criminals bent on turning the digital realm into a war zone. "In the battle raging between offense and defense in cyberspace, Clarke and Knake have some important ideas about how we can avoid cyberwar for our country, prevent cybercrime against our companies, and in doing so, reduce resentment, division, and instability at home and abroad."--Bill Clinton There is much to fear in the dark corners of cyberspace: we have entered an age in which online threats carry real-world consequences. But we do not have to let autocrats and criminals run amok in the digital realm. We now know a great deal about how to make cyberspace far less dangerous--and about how to defend our security, economy, democracy, and privacy from cyber attack. Our guides to the fifth domain -- the Pentagon's term for cyberspace -- are two of America's top cybersecurity experts, seasoned practitioners who are as familiar with the White House Situation Room as they are with Fortune 500 boardrooms. Richard A. Clarke and Robert K. Knake offer a vivid, engrossing tour of the often unfamiliar terrain of cyberspace, introducing us to the scientists, executives, and public servants who have learned through hard experience how government agencies and private firms can fend off cyber threats. With a focus on solutions over scaremongering, and backed by decades of high-level experience in the White House and the private sector, The Fifth Domain delivers a riveting, agenda-setting insider look at what works in the struggle to avoid cyberwar.

Conquering cyber attacks requires a multi-sector, multi-modal approach Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information. Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include: The information at risk The true extent of the threat The potential consequences across sectors The multifaceted approach to defense The growing cyber threat is fundamentally changing the nation's economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe.

A Private and Public Partnership Approach to Critical Infrastructure Protection

Managing Cyber Attacks in International Law, Business, and Relations

Cyber Threats and Nuclear Weapons

Inside Cyber Warfare

Cyber War: the Next Threat to National Security and What to Do about It

National Security and Information Warfare

Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats

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

Cyberterrorism involves a premeditated act; its goal is to intentionally take actions - or threaten to use actions - against computers, networks, and other critical infrastructures to inflict damage in order to further ideological, political, or other types of objectives, or to intimidate any person in furtherance of such objectives. Technological developments have seen the virtual domain evolve dramatically, and the 21st century marked acceleration in both- the online world and the threats that arise from it. The recent years have experiences not only an enhanced access to the internet worldwide, greater capabilities of programs and a wider range of services. Computers have also brought technical, political, social and economic problems, with malware being born at a higher frequency than the cures for it. Controls over targets and over attackers have become exceedingly difficult to achieve; and in the latter- practically impossible. This book is analyzes cyberterrorism from various perspectives. By and large, cyberterrorism refers to the use of the Internet or information technologies (i.e., computers), from both internal and external networks, to launch electronic attacks.

Richard A. Clarke warned America once before about the havoc terrorism would wreak on our national security—and he was right. Now he warns us of another threat, silent but equally dangerous. 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, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. This is the first book about the war of the future—cyber war—and a convincing argument that we may already be in peril of losing it.

With billions of computers in existence, cyberspace, 'the virtual world created when they are connected,' is said to be the new medium of power. Computer hackers operating from anywhere can enter cyberspace and take control of other people's computers, stealing their information, corrupting their workings, and shutting them down. Modern societies and militaries, both pervaded by computers, are supposedly at risk. As Conquest in Cyberspace explains, however, information systems and information itself are too easily conflated, and persistent mastery over the former is difficult to achieve. The author also investigates how far 'friendly conquest' in cyberspace extends, such as the power to persuade users to adopt new points of view. He discusses the role of public policy in managing cyberspace conquests and shows how the Internet is becoming more ubiquitous and complex, such as in the use of artificial intelligence.

War, Sabotage, and Fear in the Cyber Age

Law and Ethics for Virtual Conflicts

20 Years of Digital Exploitation and Cyber Warfare

Mapping the Cyber Underworld

Strategic Cyber Defense

Dark Territory

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.

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

Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyberwarfare takes the reader on a journey from the terrorist attacks of 9/11 onwards and the massive insatiable appetite, focus and investment by the Five Eyes agencies, in particular the U.S., to build the capability of digital eavesdropping and industrial espionage. With tens of trillions of dollars moving throughout hundreds of thousands of staff, and many contractors draining the country of intelligence and technical capability, the quest was simple and the outcome horrifying. No one in the world has connected the dots, until now. From digital eavesdropping and manipulation of the agencies to Stuxnet, this book covers how the world's first use of digital code and digital certificates for offensive purposes against the Iranians and their nuclear power facilities, caused collateral damage. Proceeding to today's SolarWinds attack, code-named Sunburst, the same methods of exploitation and manipulation originally used by the agencies are now being used against companies and governments with devastating effects. The SolarWinds breach has caused knock-on breaches to thousands of client companies including the U.S. government and is estimated to cost more than one trillion dollars. The monster has truly been turned against its creator and due to the lack of security and defence, breaches are occurring daily at an alarming rate. The U.S. and UK governments have little to no answer. The book also contains a chapter on breaches within the COVID-19 sector from research to immunisation and the devastating December 2020 breach of SolarWinds.

In the Digital Age of the twenty-first century, the question is not if you will be targeted, but when. For an enterprise to be fully prepared for the immanent attack, it must be actively monitoring networks, taking proactive steps to understand and contain attacks, enabling continued operation during an incident, and have a full recovery plan already in place. Are you prepared? If not, where does one begin?Cybersecurity expert Ray Rothrock has provided for businesses large and small a must-have resource that highlights the tactics used by today ’ s hackers, vulnerabilities lurking in networks, and strategies not just for surviving attacks, but actually thriving while under assault. Businesses and individuals will understand better the threats they face, be able to identify and address weaknesses, and respond to exploits swiftly and effectively.From data theft to downed servers, from malware to human error, cyber events can be triggered anytime from anywhere around the globe. Digital Resilience provides the resilience-building strategies your business needs to prevail–no matter what strikes.

Cyber Operations and International Law

Understanding the Fundamentals of Cyber Warfare in Theory and Practice

Cyber Warfare

Zero Day

Inside America's War on Terror

Challenges & Opportunities

America's Battle Against Russia, China, and the Rising Global Cyber Threat

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

Cyber WarThe Next Threat to National Security and What to Do About ItHarper Collins

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.

WINNER OF THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 The instant New York Times bestseller A Financial Times and The Times Book of the Year 'A terrifying exposé' The Times 'Part John le Carré . . . Spellbinding' New Yorker We plug in anything we can to the internet. We can control our entire lives, economy and grid via a remote web control. But over the past decade, as this transformation took place, we never paused to think that we were also creating the world's largest attack surface. And that the same nation that maintains the greatest cyber advantage on earth could also be among its most vulnerable. Filled with spies, hackers, arms dealers and a few unsung heroes, This Is How They Tell Me the World Ends is an astonishing and gripping feat of journalism. Drawing on years of reporting and hundreds of interviews, Nicole Perlroth lifts the curtain on a market in shadow, revealing the urgent threat faced by us all if we cannot bring the global cyber arms race to heel.

Techniques, Tactics and Tools for Security Practitioners

Cyberpower and National Security

The Coming Cyber War

Cyber Threat!

Confronting the Global Threat of Cyberterrorism

The Evolution of Cyber War

The Threat In Cyberspace

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

You Can't See It, but it's there, hidden in your home PC. A threat so potent it could destroy massive amounts of data and shut down power plants, fuel supplies, space satellites, the armed forces, millions of computers, and even parts of the Internet. A virtually undetectable but devastating new weapon is cyberwarfare, the next wave of terrorism, and it could be launched from your very own computer. Thousands of computer super-viruses, monster worms, and zombies created by terrorists and rogue governments are the new tools of war with the potential for catastrophic results.

This book presents a novel framework to reconceptualize Internet governance and better manage cyber attacks. Specifically, it makes an original contribution by examining the potential of polycentric regulation to increase accountability through bottom-up action. It also provides a synthesis of the current state of cybersecurity research, bringing features of the cloak and dagger world of cyber attacks to light and comparing and contrasting the cyber threat to all relevant stakeholders. Throughout the book, cybersecurity is treated holistically, covering outstanding issues in law, science, economics, and politics. This interdisciplinary approach is an exemplar of how strategies from different disciplines as well as the private and public sectors may cross-pollinate to enhance cybersecurity. Case studies and examples illustrate what is at stake and identify best practices. The book discusses technical issues of Internet governance and cybersecurity while presenting the material in an informal, straightforward manner. The book is designed to inform readers about the interplay of Internet governance and cybersecurity and the potential of polycentric regulation to help foster cyber peace.

In a very short time, individuals and companies have harnessed cyberspace to create new industries, a vibrant social space, and a new economic sphere that are intertwined with our everyday lives. At the same time, individuals, subnational groups, and governments are using cyberspace to advance interests through malicious activity. Terrorists recruit, train, and target through the Internet, hackers steal data, and intelligence services conduct espionage. Still, the vast majority of cyberspace is civilian space used by individuals, businesses, and governments for legitimate purposes. Cyberspace and National Security brings together scholars, policy analysts, and information technology executives to examine current and future threats to cyberspace. They discuss various approaches to advance and defend national interests, contrast the US approach with European, Russian, and Chinese approaches, and offer new ways and means to defend interests in cyberspace and develop offensive capabilities to compete there. Policymakers and strategists will find this book to be an invaluable resource in their efforts to ensure national security and answer concerns about future cyberwarfare.

Stuxnet to Sunburst

Cyberspace and National Security

Against All Enemies

Digital Resilience

The Perfect Weapon

The Fifth Domain

A Multidisciplinary Perspective

The inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.

Richard Clarke has been one of America's foremost experts on counterterrorism measures for more than two decades. He has served under four presidents from both parties, beginning in Ronald Reagan's State Department becoming America's first Counter-terrorism Czar under Bill Clinton and remaining for the first two years of George W. Bush's administration. He has seen every piece of intelligence on Al-Qaeda from the beginning; he was in the Situation Room on September 11th and he knows exactly what has taken place under the United State's new Department of Homeland Security. Through gripping, thriller-like scenes, he tells the full story for the first time and explains what the Bush Administration are doing.

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Will the world's next war be fought in cyberspace? "It's going to happen," said former National Defense University Professor Dan Kuehl. So much of the world's activity takes place on the internet now - including commerce, banking and communications -- the Pentagon has declared war in cyberspace an inevitability. For more than a year, Washington Post reporter Robert O'Harrow has explored the threats proliferating in our digital universe. This ebook, Zero Day: The Threat in Cyberspace, is a compilation of that reporting. With chapters built around real people, including hackers, security researchers and corporate executives, this book will help regular people, lawmakers and businesses better understand the mind-bending challenge of keeping the internet safe from hackers and security breaches -- and all out war.

The Secret History of Cyber War

National Security Dilemmas

Dawn of the Code War

Cyberdeterrence and Cyberwar

Winner of the FT & McKinsey Business Book of the Year Award 2021

The Next Threat to National Security and What to Do About It

International Norms for Emerging-Technology Weapons

"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"--

Richard A. Clarke warned America once before about the havoc terrorism would wreak on our national security -- and he was right. Now he warns us of another threat, silent but equally dangerous. Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. This is the first book about the war of the future -- cyber war -- and a convincing argument that we may already be in peril of losing it. Cyber War goes behind the "geek talk" of hackers and computer scientists to explain clearly and convincingly what cyber war is, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. From the first cyber crisis meeting in the White House a decade ago to the boardrooms of Silicon Valley and the electrical tunnels under Manhattan, Clarke and coauthor Robert K. Knake trace the rise of the cyber age and profile the unlikely characters and places at the epicenter of the battlefield. They recount the foreign cyber spies who hacked into the office of the Secretary of Defense, the control systems for U.S. electric power grids, and the plans to protect America's latest fighter aircraft. Economically and militarily, Clarke and Knake argue, what we've already lost in the new millennium's cyber battles is tantamount to the Soviet and Chinese theft of our nuclear bomb secrets in the 1940s and 1950s. The possibilities of what we stand to lose in an all-out cyber war -- our individual and national security among them -- are just as chilling. Powerful and convincing, Cyber War begins the critical debate about the next great threat to national security.

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

Exploring the negative social impact of cyber-attacks, this book takes a closer look at the challenges faced by both the public and private sectors of the financial industry. It is widely known amongst senior executives in both sectors that cybercrime poses a real threat, however effective collaboration between individual financial institutions and the public sector into detecting, monitoring and responding to cyber-attacks remains limited. Addressing this problem, the authors present the results from a series of interviews with cybersecurity professionals based in Canada in order to better understand the potential risks and threats that financial institutions are facing in the digital age. Offering policy recommendations for improving cybersecurity protection measures within financial institutions, and enhancing the sharing of information between the public and private sector, this book is a timely and invaluable read for those researching financial services, cybercrime and risk management, as well as finance professionals interested in cybersecurity.

The Challenge to National Security

The Next War Zone

Cyber War Versus Cyber Realities

The Basics of Cyber Warfare

In Search of Cyber Peace

Threatcasting

Cybersecurity

"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?

"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"--

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.

A contemporary primer on the leading arguments about U.S. national security, National Security Dilemmas addresses the major challenges and opportunities that are live-issue areas for American policymakers and strategists today. Colin S. Gray provides an in-depth analysis of a policy and strategy for deterrence; the long-term U.S. bid to transform its armed forces' capabilities, with particular reference to strategic surprise, in the face of many great uncertainties; the difficulty of understanding and exploiting the challenge of revolutionary change in warfare; the problems posed by enemies who fight using irregular methods; and the awesome dilemmas for U.S. policy over the options to wage preventive and preemptive warfare. With forty years' experience as a strategist, within and outside of government, Gray uses a problem-solving motif throughout the book, suggesting solutions to the challenges he identifies. The book's master narrative is that the United States must take a more considered strategic approach to its security dilemmas. Too often, the country's leaders decide on a policy and then move to take action, all the while neglecting to devise a plan that would connect its political purposes to military means. While many of Gray's judgments here are critical of current ideas and behavior, he crafted them as helpful guides should planners adopt them when revising policies and approaches. Strategy is a practical matter; truly it is the zone wherein theory meets practice. This text can be used as an expert guide to the major national security challenges of today. It both explains the structure of these challenges and provides useful answers. With a foreword by Lt. Gen. Paul K. Van Riper, USMC (Ret.), Bren Chair, Marine Corps University, Quantico, Virginia.

Fourteen Analogies

Countering Cyber Threats to Financial Institutions

How to Manage the Growing Risk of Cyber Attacks

Conquest in Cyberspace

Cyber War Will Not Take Place

The Impact on U.S. National and International Security

The Cyber Threat and Globalization

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 pol 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, 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.

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.

The technology controlling United States nuclear weapons predates the Internet. Updating the technology for the digital era is necessary, but it comes with the risk that anything digital can be hacked. Moreover, using new systems for both nuclear and non-nuclear operations will lead to levels of nuclear risk hardly imagined before. This book is the first to confront these risks comprehensively. With Cyber Threats and Nuclear Weapons, Herbert Lin provides a clear-eyed breakdown of the cyber risks to the U.S. nuclear enterprise. Featuri series of scenarios that clarify the intersection of cyber and nuclear risk, this book guides readers through a little-understood element of the risk profile that government decision-makers should be anticipating. What might have happened if the Cuban Missile Crisis took place in the age of Twitter, with unvetted information swirling around? What if an adversary announced that malware had compromised nuclear systems, clouding the confidence of nuclear decision-makers? Cyber Threats and Nuclear Weapons, the first book to consider risks across the entire nuclear enterprise, concludes with crucial advice on how government can manage the tensions between new nuclear capabilities and increasing cyber risk. This is an invaluable handbook for those ready to confront the unique challenges of cyber nuclear risk.

This book is designed for those who want a better grasp of the nature and existential threat of today's information wars. It uses a conceptual approach to explain the relevant concepts as well as the structural challenges and responsibilities with which policy makers struggle and practitioners must work.

Cyber War

What Everyone Needs to Know

Conflict and Cooperation in Cyberspace

Cyber Conflict in the International System

What Executives, the Board, and You Should Know

Threats, Opportunities, and Power in a Virtual World

Understanding Cyber Conflict

The safety of your home, family, and business starts right in front of you-with the computer on your desk and the smart phone in your hands. Be prepared. Read this book.

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.

This book creates a framework for understanding and using cyberpower in support of national security. Cyberspace and cyberpower are now critical elements of international security. United States needs a national policy which employs cyberpower to support its national security interests.

Originally published in hardcover in 2016 by Simon & Schuster.

Is Your Company Ready for the Next Cyber Threat?

This Is How They Tell Me the World Ends

CUCKOO'S EGG