Cyber War Will Not Take Place

Cybersecurity expert Theresa Payton tells battlefront stories from the global war being conducted through clicks, swipes, internet access, technical backdoors and massive espionage schemes. She investigates the cyberwarriors who are planning tomorrow’s attacks, weaving a fascinating yet bone-chilling tale of Artificial Intelligent mutations carrying out attacks without human intervention, “deepfake” videos that look real to the naked eye, and chatbots that beget other chatbots. Finally, Payton offers readers telltale signs that their most fundamental beliefs are being meddled with and actions they can take or demand that corporations and elected officials must take before it is too late. Payton reveals: How digital voting machines, voting online, and automatic registration may boost turnout but make us more vulnerable to cyberattacks. How trolls from Russia and other nations actively stroke discord among Americans in falsely-generated controversies over race relations, vaccinations, fracking, and other social issues. Whether what we have uncovered from the Mueller investigation so far is only what they wanted us to know.

"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"--

Army's role in the Vietnam War, The Army and Vietnam demonstrates with chilling persuasiveness the ways in which the army was unprepared to fight—lessons applicable to today's wars in Afghanistan and Iraq.

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.

Cyberdeterrence and Cyberwar
Cyber Operations and International Law
The Virtual Weapon and International Order
Cyber War Versus Cyber Realities
Civil Military Disorder and Legal Uncertainty
Soft War

Originally published in hardcover in 2016 by Simon & Schuster.
Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.
The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by 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 Case Against Democracy

Bitskrieg

Tallinn Manual on the International Law Applicable to Cyber Warfare

Techniques, Tactics and Tools for Security Practitioners

Borderless Wars

Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy--and Completely Unprepared for Adulthood--and What That Means for the Rest of Us

This Is How They Tell Me the World Ends

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 Cyber War Will Not Take PlaceOxford University Press

“One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph. Democracy may be one of the most admired ideas ever concocted, but what if it’s also one of the most harebrained? After many years of writing about democracy for a living, David Harsanyi has concluded that it’s the most overrated, overused, and misunderstood idea in political life. The less we have of it the better. “Democracy” is not synonymous with “freedom.” It is not the opposite of tyranny. In fact, the Founding Fathers knew that democracy can lead to tyranny. That’s why they built so many safeguards against it into the Constitution. Democracy, Harsanyi argues, has made our government irrational, irresponsible, and

invasive. It has left the American people with only two options—domination by the majority or a government that can't possibly work. The modern age has imbued democracy with the mystique of infallibility. But Harsanyi reminds us that the vast majority of political philosophers, including the founders, have thought that responsible, limited government based on direct majority rule over a large, let alone continental scale was a practical impossibility. In The People Have Spoken, you'll learn: Why the Framers of our Constitution were intent on establishing a republic, not a "democracy" How democracy undermines self-government How shockingly out of touch with reality most voters really are Why democracy is an economic wrecking ball—and an invitation to a politics of envy and corruption How the great political philosophers from Plato and Aristotle to Burke and Tocqueville predicted with uncanny accuracy that democracy could lead to tyranny Harsanyi warns that if we don't recover the Founders' republican vision, "democracy" might very well spell the end of American liberty and prosperity.

Understanding Intangible Warfare

What Everyone Needs to Know

Cybersecurity

Inside Cyber Warfare

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

There Will Be Cyberwar

Law and Ethics for Virtual Conflicts

Originally published in hardcover in 2019 by Doubleday.

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 updated and expanded edition of Cyberspace in Peace and War by Martin C. Libicki presents a comprehensive understanding of cybersecurity, cyberwar, and cyber-terrorism. From basic concepts to advanced principles, Libicki examines the sources and consequences of system compromises, addresses strategic aspects of cyberwar, and defines cybersecurity in the context of military operations while highlighting unique aspects of the digital battleground and strategic uses of cyberwar. This new edition provides updated analysis on cyberespionage, including the enigmatic behavior of Russian actors, making this volume a timely and necessary addition to the cyber-practitioner's library. Cyberspace in Peace and War guides readers through the complexities of cybersecurity and cyberwar and challenges them to understand the topics in new ways. Libicki provides the technical and geopolitical foundations of cyberwar necessary to understand the policies, operations, and strategies required for safeguarding an increasingly online infrastructure.

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 Manipulated

How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar

The Perfect Weapon

A Multidisciplinary Approach

Deterring Cyber Warfare

Cyber Attacks and the New Normal of Geopolitics

The People Have Spoken (and They Are Wrong)

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.

While the deterrence of cyber attacks is one of the most important issues facing the United States and other nations, the application of deterrence theory to the cyber realm is problematic. This study introduces cyber warfare and reviews the challenges associated with deterring cyber attacks, offering key recommendations to aid the deterrence of major cyber attacks.

New technologies are changing how we protect our citizens and wage our wars. Among militaries, everything taken for granted about the ability to maneuver and fight is now undermined by vulnerability to “weapons of mass disruption”: cutting-edge computer worms, viruses, and invasive robot networks. At home, billions of household appliances and other “smart” items that form the Internet of Things risk being overtaken, then added to the ranks of massive, malicious “zombie” armies. The age of Bitskrieg is here, bringing vexing threats that range from the business sector to the battlefield. In this new book, world-renowned cyber security expert John Arquilla looks unflinchingly at the challenges posed by cyberwarfare – which he argues have neither been met nor mastered. He offers fresh solutions for protecting against enemies that are often anonymous, unpredictable and capable of projecting force and influence vastly disproportionate to their size, strength or wealth. The changes called for require radical rethinking of military and security affairs, diplomacy, even the routines of our daily lives.

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

Cyber War
Cyberwar and Revolution
The Hacker and the State
Bolstering Strategic Stability in Cyberspace
Espionage, Strategy, and Politics in the Digital Domain
The New Challenge of Cyberwarfare
Hacking, Trust and Fear Between Nations

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.

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

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

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

Dark Territory
War, Sabotage, and Fear in the Cyber Age
@War
In Search of Cyber Peace
The Strategic Dimensions of Offensive Cyber Operations
Surviving Cyberwar
International Norms for Emerging-Technology Weapons

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.

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

Uncovering the class conflicts, geopolitical dynamics, and aggressive capitalism propelling the militarization of the internet Global surveillance, computational propaganda, online espionage, virtual recruiting, massive data breaches, hacked nuclear centrifuges and power grids—concerns about cyberwar have been mounting, rising to a fever pitch after the alleged Russian hacking of the U.S. presidential election and the Cambridge Analytica scandal. Although cyberwar is widely discussed, few accounts undertake a deep, critical view of its roots and consequences. Analyzing the new militarization of the internet, Cyberwar and Revolution argues that digital warfare is not a bug in the logic of global capitalism but rather a feature of its chaotic, disorderly unconscious. Urgently confronting the concept of cyberwar through the lens of both Marxist critical theory and psychoanalysis, Nick Dyer-Witheford and Svitlana Matviyenko provide a wide-ranging examination of the class conflicts and geopolitical dynamics propelling war across digital networks. Investigating the subjectivities that cyberwar mobilizes, exploits, and bewilders, and revealing how it permeates the fabric of everyday life and implicates us all in its design, this book also highlights the critical importance of the emergent resistance to this digital militarism—hacktivism, digital worker dissent, and off-the-grid activism—for effecting different, better futures.

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.

A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

Inside the Cyberwar to Hijack Elections and Distort the Truth

Bytes, Bombs, and Spies

Mapping the Cyber Underworld

The Evolution of Cyber War

Building the Scientific Foundation

iGen

An investigation into how the Pentagon, NSA, and other government agencies are uniting with corporations to fight in cyberspace, the next great theater of war.

"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"--

"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.

Cyber-warfare is often discussed, but rarely truly seen. When does an intrusion turn into an attack, and what does that entail? How do nations fold offensive cyber operations into their strategies? Operations against networks mostly occur to collect intelligence, in peacetime. Understanding the lifecycle and complexity of targeting adversary networks is key to doing so effectively in conflict. Rather than discussing the spectre of cyber war, Daniel Moore seeks to observe the spectrum of cyber operations. By piecing together operational case studies, military strategy and technical analysis, he shows that modern cyber operations are neither altogether unique, nor entirely novel. Offensive cyber operations are the latest incarnation of intangible warfare--conflict waged through non-physical means, such as the information space or the electromagnetic spectrum. Not all offensive operations are created equal. Some are slow-paced, clandestine infiltrations requiring discipline and patience for a big payoff; others are short-lived attacks meant to create temporary tactical disruptions. This book first seeks to understand the possibilities, before turning to look at some of the most prolific actors: the United States, Russia, China and Iran. Each has their own unique take, advantages and challenges when attacking networks for effect.

Managing Cyber Attacks in International Law, Business, and Relations

The Fifth Domain

Cyber Conflict in the International System

Introduction to Cyber-Warfare

Cyberspace in Peace and War, Second Edition

The Rise of the Military-Internet Complex

China and Cybersecurity

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

This book examines in depth the major recent cyber attacks that have taken place

in the United States and around the world including a discussion of the 2016 election. This book discusses the implications of such attacks and offers solutions to the vulnerabilities that made these attacks possible.

"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?

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.

The Cybersecurity Dilemma
The Army and Vietnam
Cyber War Will Not Take Place
The Secret History of Cyber War
Offensive Cyber Operations
Sandworm
Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats

Just war theory focuses primarily on bodily harm, such as killing, maiming, and torture, while other harms are often largely overlooked. At the same time, contemporary international conflicts increasingly involve the use of unarmed tactics, employing 'softer' alternatives or supplements to kinetic power that have not been sufficiently addressed by the ethics of war or international law. Soft war tactics include cyber-warfare and economic sanctions, media warfare, and propaganda, as well as non-violent resistance as it plays out in civil disobedience,

boycotts, and 'lawfare.' While the just war tradition has much to say about 'hard' war - bullets, bombs, and bayonets - it is virtually silent on the subject of 'soft' war. Soft War: The Ethics of Unarmed Conflict illuminates this neglected aspect of international conflict.

An urgently needed examination of the current cyber revolution that draws on case studies to develop conceptual frameworks for understanding its effects on international order The cyber revolution is the revolution of our time. The rapid expansion of cyberspace brings both promise and peril. It promotes new modes of political interaction, but it also disrupts interstate dealings and empowers non-state actors who may instigate diplomatic and military crises. Despite significant experience with cyber phenomena, the conceptual apparatus to analyze, understand, and address their effects on international order remains primitive. Here, Lucas Kello adapts and applies international relations theory to create new ways of thinking about cyber strategy. Kello draws on a broad range of case studies, including the Estonian crisis, the Olympic Games operation against Iran, and the cyber attack against Sony Pictures. Synthesizing qualitative data from government documents, forensic reports of major incidents and interviews with senior officials from around the globe, this important work establishes new conceptual benchmarks to help security experts adapt strategy and policy to the unprecedented challenges of our times.

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.

As seen in Time, USA TODAY, The Atlantic, The Wall Street Journal, and on CBS This Morning, BBC, PBS, CNN, and NPR, iGen is crucial reading to understand how the children, teens, and young adults born in the mid-1990s and later are vastly different from their Millennial predecessors, and from any other generation. With generational divides wider than ever, parents, educators, and employers have an urgent need to understand today’s rising generation of teens and young adults. Born in the mid-1990s up to the mid-2000s, iGen is the first generation to spend their entire adolescence in the age of the smartphone. With social media and texting replacing other activities, iGen spends less time with their friends in person—perhaps contributing to their unprecedented levels of anxiety, depression, and loneliness. But technology is not the only thing

that makes iGen distinct from every generation before them; they are also different in how they spend their time, how they behave, and in their attitudes toward religion, sexuality, and politics. They socialize in completely new ways, reject once sacred social taboos, and want different things from their lives and careers. More than previous generations, they are obsessed with safety, focused on tolerance, and have no patience for inequality. With the first members of iGen just graduating from college, we all need to understand them: friends and family need to look out for them; businesses must figure out how to recruit them and sell to them; colleges and universities must know how to educate and guide them. And members of iGen also need to understand themselves as they communicate with their elders and explain their views to their older peers. Because where iGen goes, so goes our nation—and the world.

Digital Subterfuge in Global Capitalism

Cyberwar is Coming!

Cyber Warfare

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