Deception And Counter Deception Morphisec

Conquest in Cyberspace
Cyber War
Information Warfare and Security
How Spies Think
A Fierce Domain
Click Here to Kill Everybody: Security and Survival in a Hyper-connected World
Planning Armageddon
Managing Cyber Risk
Cyber Warfare
The Bombers and the Bombed
Countdown to Zero Day
Cloud Architecture Patterns
How Statesmen Think
Networks and Netwars
Gulf War Air Power Survey
Rebuilding European Democracy
Information Theory and Statistics
The Rise and Fall of Intelligence
Schneier on Security
Understanding Cyber Conflict
Cyber Blockades
Playing President
Bombing to Win
Almost Looks Like Work
Emerging Security Technologies and EU Governance
Deception
Cyberspace and National Security
Strategic Cyber Security
Cyber Attacks and the Law of War
In Athena's Camp
Not War, Not Peace?
Nuclear Statecraft
Hacking Exposed Wireless
Turkey Under Erdoğan
Power in Uncertain Times
Cybersecurity, Privacy and Freedom Protection in the Connected World
Navigating the Cybersecurity Career Path
RYU SDN Framework - English Edition
Counterdeception Principles and Applications for National Security
Afghan Endgames

MCKEE JOURNEY

Conquest in Cyberspace Harvard University Press
Netwar-like cyberwar-describes a new spectrum of conflict that is emerging in the wake of the information revolution. Netwar includes conflicts waged, on the one hand, by terrorists, criminals, gangs, and ethnic extremists; and by civil-society activists (such as cyber activists or WTO protestors) on the other. What distinguishes netwar is the networked organizational structure of its practitioners-with many groups actually being leaderless-and their quickness in coming together in swarming attacks. To confront this new type of conflict, it is crucial for governments, military, and law enforcement to begin networking themselves.
Cyber War Penguin UK
In recent years serious concerns emerged over the state of European democracy. Many democracy indices are reporting a year-on-year drift towards less liberal politics in the countries of the European Union. Polls regularly suggest that the voters are coming to question democratic norms more seriously than for many decades. Here, Richard Youngs assesses these risks as many analysts, journalists and politicians stressed the danger of Europe descending into an era of conflict, driven by xenophobic nationalism and nativist authoritarians slowly dismantling liberal democratic rights. In 2020, the Covid-19 pandemic has intensified these fears. There is another side of the democratic equation, however. Youngs argues that governments, EU institutions, political parties, citizens and civil society organisations have gradually begun to push back in defence of democracy. With each chapter, Youngs shows how many governmental, political and social actors have developed responses to Europe's democratic malaise at multiple levels. Europe's democracy problems have been grave and far-reaching. Yet, a spirit of democratic resistance has slowly taken shape. This book argues that the pro-democratic fightback may be belated, but it is real and has assumed significant traction with various types of democratic reform underway, including citizen initiatives, political-party changes, digital activism and EU-level responses.
Information Warfare and Security Cornell University Press
This book examines America's evolving strategy on the international security environment, and comprehensively analyzes how different strategies position states to compete in the present and future, manage risk, and prevail despite uncertainty.
How Spies Think Independently Published
Land the perfect cybersecurity role—and move up the ladder—with this insightful resource Finding the right position in cybersecurity is challenging. Being successful in the profession takes a lot of work. And becoming a cybersecurity leader responsible for a security team is even more difficult. In Navigating the Cybersecurity Career Path, decorated Chief Information Security Officer Helen Patton delivers a practical and insightful discussion designed to assist aspiring cybersecurity professionals entering the industry and help those already in the industry advance their careers and lead their first security teams. In this book, readers will find: Explanations of why and how the cybersecurity industry is unique and how to use this knowledge to succeed Discussions of how to progress from an entry-level position in the industry to a position leading security teams and programs Advice for every stage of the cybersecurity career arc Instructions on how to move from single contributor to team leader, and how to build a security program from scratch Guidance on how to apply the insights included in this book to the reader's own situation and where to look for personalized help A unique perspective based on the personal experiences of a cybersecurity leader with an extensive security background Perfect for aspiring and practicing cybersecurity professionals at any level of their career, Navigating the Cybersecurity Career Path is an essential, one-stop resource that includes everything readers need to know about thriving in the cybersecurity industry.
A Fierce Domain Bloomsbury Publishing
Reflections on, and interviews with, US presidents from Nixon to George W. Bush, from “one of the best reporters of our time” (Joan Didion, New York Times–bestselling author of The White Album). Robert Scheer’s interviews with and profiles of US presidents have shaped journalism history. Scheer developed close journalistic relationships with Richard Nixon, Jimmy Carter, Ronald Reagan, Bill Clinton, and George H. W. Bush, and his reporting on them had a tangible impact on national debate—with examples including the famed 1976 Playboy interview in which then-candidate Jimmy Carter admitted to have lusted in his heart; and the 1980 interview with the Los Angeles Times during which the senior Bush confessed to Scheer his dream of a “winnable nuclear war.” In Playing President, Robert Scheer offers an unparalleled insight into the presidential mind, analyzing administrations from Nixon to George W. Bush, offering insights that will surprise the reader—particularly those with rigid preconceptions about the decision-making processes of our leaders. Also included are reprints of Scheer’s famous presidential interviews, along with previously unpublished interview transcripts and select writings.
Click Here to Kill Everybody: Security and Survival in a Hyper-connected World Cambridge University Press
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.
Planning Armageddon Akashic Books
What individuals, corporations, and governments need to know about information-related attacks and defenses! Every day, we hear reports of hackers who have penetrated computer networks, vandalized Web pages, and accessed sensitive information. We hear how they have tampered with medical records, disrupted emergency 911 systems, and siphoned money from bank accounts. Could information terrorists, using nothing more than a personal computer, cause planes to crash, widespread power blackouts, or financial chaos? Such real and imaginary scenarios, and our defense against them, are the stuff of information warfare-operations that target or exploit information media to win some objective over an adversary. Dorothy E. Denning, a pioneer in computer security, provides in this book a framework for understanding and dealing with information-based threats: computer break-ins, fraud, sabotage, espionage, piracy, identity theft, invasions of privacy, and electronic warfare. She describes these attacks with astonishing, real examples, as in her analysis of information warfare operations during the Gulf War. Then, offering sound advice for security practices and policies, she explains countermeasures that are both possible and necessary. You will find in this book: A comprehensive and coherent treatment of offensive and defensive information warfare, identifying the key actors, targets, methods, technologies, outcomes, policies, and laws; A theory of information warfare that explains and integrates within a single framework operations involving diverse actors and media; An accurate picture of the threats, illuminated by actual incidents; A description of information warfare technologies and their limitations, particularly the limitations of defensive technologies. Whatever your interest or role in the emerging field of information warfare, this book will give you the background you need to make informed judgments about potential threats and our defenses against them.
0201433036B04062001

Managing Cyber Risk John Wiley & Sons
This sweeping history of the development of professional, institutionalized intelligence examines the implications of the fall of the state monopoly on espionage today and beyond. During the Cold War, only the alliances clustered around the two superpowers maintained viable intelligence endeavors, whereas a century ago, many states could aspire to be competitive at these dark arts. Today, larger states have lost their monopoly on intelligence skills and capabilities as technological and sociopolitical changes have made it possible for private organizations and even individuals to unearth secrets and influence global events. Historian Michael Warner addresses the birth of professional intelligence in Europe at the beginning of the twentieth century and the subsequent rise of US intelligence during the Cold War. He brings this history up to the present day as intelligence agencies used the struggle against terrorism and the digital revolution to improve capabilities in the 2000s. Throughout, the book examines how states and other entities use intelligence to create, exploit, and protect secret advantages against others, and emphasizes how technological advancement and ideological competition drive intelligence, improving its techniques and creating a need for intelligence and counterintelligence activities to serve and protect policymakers and commanders. The world changes intelligence and intelligence changes the world. This sweeping history of espionage and intelligence will be a welcomed by practitioners, students, and scholars of security studies, international affairs, and intelligence, as well as general audiences interested in the evolution of espionage and technology.
Cyber Warfare RYU project team
This book provides an opportunity for investigators, government officials, systems scientists, strategists, assurance researchers, owners, operators and maintainers of large, complex and advanced systems and infrastructures to update their knowledge with the state of best practice in the challenging domains whilst networking with the leading representatives, researchers and solution providers. Drawing on 12 years of successful events on information security, digital forensics and cyber-crime, the 13th ICGS3-20 conference aims to provide attendees with an information-packed agenda with representatives from across the industry and the globe. The challenges of complexity, rapid pace of change and risk/opportunity issues associated with modern products, systems, special events and infrastructures. In an era of unprecedented volatile, political and economic environment across the world, computer-based systems face ever more increasing challenges, disputes and responsibilities, and whilst the Internet has created a global platform for the exchange of ideas, goods and services, it has also created boundless opportunities for cyber-crime. As an increasing number of large organizations and individuals use the Internet and its satellite mobile technologies, they are increasingly vulnerable to cyber-crime threats. It is therefore paramount that the security industry raises its game to combat these threats. Whilst there is a huge adoption of technology and smart home devices, comparably, there is a rise of threat vector in the abuse of the technology in domestic violence inflicted through IoT too. All these are an issue of global importance as law enforcement agencies all over the world are struggling to cope.
The Bombers and the Bombed Penguin
Even in its earliest history, cyberspace had disruptions, caused by malicious actors, which have gone beyond being mere technical or criminal problems. These cyber conflicts exist in the overlap of national security and cybersecurity, where nations and non-state groups use offensive and defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes. A two-year study, resulting in the new book -- A Fierce Domain: Cyber Conflict, 1986 to 2012 -- has made the following conclusions, which are very different from those that policymakers are usually told: Cyber conflict has changed only gradually over time, making historical lessons especially relevant (though usually ignored). The probability and consequence of disruptive cyber conflicts has been hyped while the impact of cyber espionage is consistently underappreciated. The more strategically significant the cyber conflict, the more similar it is to conflict in the other domains ? with one critical exception.
Countdown to Zero Day Georgetown University Press
From Iraq to Bosnia to North Korea, the first question in American foreign policy debates is increasingly: Can air power alone do the job? Robert A. Pape provides a systematic answer. Analyzing the results of over thirty air campaigns, including a detailed reconstruction of the Gulf War, he argues that the key to success is attacking the enemy's military strategy, not its economy, people, or leaders. Coercive air power can succeed, but not as cheaply as air enthusiasts would like to believe.Pape examines the air raids on Germany, Japan, Korea, Vietnam, and Iraq as well as those of Israel versus Egypt, providing details of bombing and governmental decision making. His detailed narratives of the strategic effectiveness of bombing range from the classical cases of World War II to an extraordinary reconstruction of airpower use in the Gulf War, based on recently declassified documents. In this now-classic work of the theory and practice of airpower and its political effects, Robert A. Pape helps military strategists and policy makers judge the purpose of various air strategies, and helps general readers understand the policy debates.
Cloud Architecture Patterns Bloomsbury Publishing USA
Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.
How Statesmen Think Stanford University Press
The information revolution--which is as much an organizational as a technological revolution--is transforming the nature of conflict across the spectrum: from open warfare, to terrorism, crime, and even radical social activism. The era of massed field armies is passing, because the new information and communications systems are increasing the lethality of quite small units that can call in deadly, precise missile fire almost anywhere, anytime. In social conflicts, the Internet and other media are greatly empowering individuals and small groups to influence the behavior of states. Whether in military or social conflicts, all protagonists will soon be developing new doctrines, strategies, and tactics for swarming their opponents--with weapons or words, as circumstances require. Preparing for conflict in such a world will require shifting to new forms of organization, particularly the versatile, hardy, all-channel network. This shift will prove difficult for states and professional militaries that remain bastions of hierarchy, bound to resist institutional redesign. They will make the shift as they realize that information and knowledge are becoming the key elements of power. This implies, among other things, that Mars, the old brute-force god of war, must give way to Athena, the well-armed goddess of wisdom. Accepting Athena as the patroness of this information age represents a first step not only for preparing for future conflicts, but also for preventing them.
Networks and Netwars Crown
Today, the use of denial and deception (D&D) is being used to compensate for an opponents military superiority, to obtain or develop weapons of mass destruction, and to violate international agreements and sanctions. This technical volume offers a comprehensive overview of the concepts and methods that underlie strategic deception and provides an in-depth understanding of counter deception.
Gulf War Air Power Survey Princeton University Press
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.
Rebuilding European Democracy Georgetown University Press
In 1949, John Von Neumann-a mathematician and an early architect of computing systems-presented at the University of Illinois a series of lectures called the Theory and Organization of Complicated Automata, where he explored the possibility of developing machines that self-replicate.1 Von Neumann envisioned machines that could build self-copies and pass on their programming to their progeny. While his ideas had legitimate applications, such as large-scale mining, many observers also consider it to be the theoretical precursor to the modern-day computer virus.2 Self-replication is a defining characteristic of computer viruses and worms. Through self-replication, computer code populates computer systems exponentially. Computer viruses and worms have the capacity for constructive applications, but they are most often malware-malicious software that is hostile, intrusive, and unwelcome.
Information Theory and Statistics Kenneth Geers
Before the First World War, the British Admiralty conceived a plan to win rapid victory in the event of war with Germany-economic warfare on an unprecedented scale.This secret strategy called for the state to exploit Britain's effective monopolies in banking, communications, and shipping-the essential infrastructure underpinning global trade-to create a controlled implosion of the world economic system. In this revisionist account, Nicholas Lambert shows in lively detail how naval planners persuaded the British political leadership that systematic disruption of the global economy could bring about German military paralysis. After the outbreak of hostilities, the government shied away from full implementation upon realizing the extent of likely collateral damage-political, social, economic, and diplomatic-to both Britain and neutral countries. Woodrow Wilson in particular bristled at British restrictions on trade. A new, less disruptive approach to economic coercion was hastily improvised. The result was the blockade, ostensibly intended to starve Germany. It proved largely ineffective because of the massive political influence of economic interests on national ambitions and the continued interdependencies of all countries upon the smooth functioning of the global trading system. Lambert's interpretation entirely overturns the conventional understanding of British strategy in the early part of the First World War and underscores the importance in any analysis of strategic policy of understanding Clausewitz's "political conditions of war."
The Rise and Fall of Intelligence Routledge
An incisive account of Erdoğan’s Turkey – showing how its troubling transformation may be short-lived Since coming to power in 2002 Recep Tayyip Erdoğan has overseen a radical transformation of Turkey. Once a pillar of the Western alliance, the country has embarked on a militaristic foreign policy, intervening in regional flashpoints from Nagorno-Karabakh to Libya. And its democracy, sustained by the aspiration to join the European Union, has given way to one-man rule. Dimitar Bechev traces the political trajectory of Erdoğan’s populist regime, from the era of reform and prosperity in the 2000s to the effects of the war in neighboring Syria. In a tale of missed opportunities, Bechev explores how Turkey parted ways with the United States and Europe, embraced Putin’s Russia and other revisionist powers, and replaced a frail democratic regime with an authoritarian one. Despite this, he argues that Turkey’s democratic instincts are resilient, its economic ties to Europe are as strong as ever, and Erdoğan will fail to achieve a fully autocratic regime.
Schneier on Security Georgetown University Press
The United States and its allies have been fighting the Taliban and al-Qaeda in Afghanistan for a decade in a war that either side could still win. While a gradual drawdown has begun, significant numbers of US combat troops will remain in Afghanistan until at least 2014, perhaps longer, depending on the situation on the ground and the outcome of the US presidential election in 2012. Given the realities of the Taliban’s persistence and the desire of US policymakers—and the public—to find a way out, what can and should be the goals of the US and its allies in Afghanistan? Afghan Endgames brings together some of the finest minds in the fields of history, strategy, anthropology, ethics, and mass communications to provide a clear, balanced, and comprehensive assessment of the alternatives for restoring peace and stability to Afghanistan. Presenting a range of options—from immediate withdrawal of all coalition forces to the maintenance of an open-ended, but greatly reduced military presence—the contributors weigh the many costs, risks, and benefits of each alternative. This important book boldly pursues several strands of thought suggesting that a strong, legitimate central government is far from likely to emerge in Kabul; that fewer coalition forces, used in creative ways, may have better effects on the ground than a larger, more conventional presence; and that, even though Pakistan should not be pushed too hard, so as to avoid sparking social chaos there, Afghanistan’s other neighbors can and should be encouraged to become more actively involved. The volume’s editors conclude that while there may never be complete peace in Afghanistan, a self-sustaining security system able to restore order swiftly in the wake of violence is attainable.
Understanding Cyber Conflict Georgetown University Press
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.

• Chicka Chicka Boom Boom (board Book)
• Harry Potter Paperback Box Set (books 1-7) By J. K. Rowling
• Stone Maidens
• Never Never: A Romantic Suspense Novel Of Love And Fate By Colleen Hoover
• Our Class Is A Family (our Class Is A Family & Our School Is A Family) By Shannon Olsen
• The Summer I Turned Pretty (summer I Turned Pretty, The) By Jenny Han
• To Kill A Mockingbird
• The Shadow Work Journal: A Guide To Integrate And Transcend Your Shadows By Keila Shaheen