Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure

The Shadow WarCyber Security: Threats and Responses for Government and BusinessThe Russia-China AxisArtificial Intelligence, China, Russia, and the Global OrderRussia- on a path to cyber sovereignty?The Fifth DomainCybersecurityAt the Nexus of Cybersecurity and Public PolicySecurity Relations between China and the European UnionConflict and Cooperation in the Global CommonsLove and WarCyber Policy in ChinaThe Red WebCyber SecurityThe Cybersecurity DilemmaNational Security Strategy of the United StatesThe Hacker and the StateThe Oxford Handbook on the United NationsEmerging Cyber Threats and Cognitive VulnerabilitiesChina and CybersecurityChina, Russia, and Twenty-First Century Global GeopoliticsCyber Threat!Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at RiskDroit Et Politique ÉtrangèreCyberpower and National SecurityEvery Nation for ItselfThe Perfect WeaponSmart Grid Cyber Security Potential Threats, Vulnerabilities and RisksSandwormDawn of the Code WarChallenges to Security in SpaceThe U.S.-China Military ScorecardInside Cyber WarfareConfronting an "Axis of Cyber"?Cyber Threats from China, Russia, and IranInternet Governance in an Age of Cyber InsecurityCurrent and Emerging Trends in Cyber OperationsCyber Threats from China, Russia, and

IranThe Hacked World OrderCyber War

The Shadow War

U.S. interests lie in the continuation of a single, open, globally interconnected network for the free exchange of ideas and the conduct of economic activity. Criminals and rogue nations are threatening that paradigm, exploiting fundamental weaknesses in the architecture of the Internet. Cybersecurity and homeland security expert Robert K. Knake urges the United States to promote its vision for a secure Internet through existing international forums. His report provides a clear statement of U.S. national interest in cyberspace and develops an agenda for promoting it within Internet governance organizations. Knake maintains that the U.S. Department of State must be staffed and funded to coordinate the promotion of this agenda across the federal government with important private sector players. He further recommends the development of a treaty to ban the targeting of civilian infrastructure in cyberspace and the application of diplomatic and economic pressure to expand the number of countries that are party to the existing Convention on Cybercrime. By taking these steps, the United States can help develop both the technical and legal mechanisms to address security concerns in cyberspace while maintaining the vision of a unified, global Internet.

Cyber Security: Threats and Responses

for Government and Business

The experts of the International Working Group-Landau Network Centro Volta (IWG-LNCV) discuss aspects of cyber security and present possible methods of deterrence, defense and resilience against cyber attacks. This SpringerBrief covers state-of-the-art documentation on the deterrence power of cyber attacks and argues that nations are entering a new cyber arms race. The brief also provides a technical analysis of possible cyber attacks towards critical infrastructures in the chemical industry and chemical safety industry. The authors also propose modern analyses and a holistic approach to resilience and security of Industrial Control Systems. The combination of contextual overview and future directions in the field makes this brief a useful resource for researchers and professionals studying systems security, data security and data structures. Advanced-level students interested in data security will also find this brief a helpful guide to recent research.

The Russia-China Axis

Today, space has become a seamless part of many military and civilian activities. The advantages the United States holds in space capabilities will drive some nations to improve their abilities to access and operate in space. Moreover, some actors will seek counterspace capabilities that target the perceived United States and allied reliance on space, including the ability to use secure satellite communications, precision strike capabilities, and ISR assets. As the number of spacefaring nations grows and as some actors integrate space and counterspace capabilities into military operations, these trends will pose a challenge to U.S. space dominance and present new risks for assets on orbit.

Artificial Intelligence, China, Russia, and the Global Order

Following the acclaim for The End of the Free Market, Ian Bremmer is back with Every Nation for Itself, where he addresses the next big issue for the shifting world economy. 'Smart and snappy provides the most cogent prediction of how the politics of a post-America world will play out' New Statesman What happens when nobody's running the world? The United States is in financial crisis and can't hold onto the reins of the G-20. But China has no interest in international leadership, Europe is trying to save the euro, and emerging powers like Brazil and India are focused on domestic development. No government has the time, resources or political capital needed to take an international lead. The world power structure is about to have a vacancyat the top. Welcome to the G-Zero world, in which no single country has the power to shape a truly global agenda. That means we are about to see 20 years of conflict over economics, finance and climate change. Bestselling author and strategist Ian Bremmer reveals how world powers are rapidly turning into gated communities, locked in competition. Who will prevail? 'A prodigy in the US global commentariat. Mr Bremmer's rehearsal of the consequences should make us all wise up' Financial Times 'An author who is always full of insights' George Osborne Ian Bremmer is the president of the world's leading global political risk research and consulting firm, Eurasia Group. He has written for the Wall Street Journal, Washington Post, Newsweek, and Harvard Business Review. His six books include The J Curve and The End Of The Free Market.

Russia- on a path to cyber sovereignty?

The Fifth Domain

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.

Cybersecurity

With important new revelations into the Russian hacking of the 2016 Presidential campaigns "[Andrei Soldatov is] the single most prominent critic of Russia's surveillance apparatus." -Edward Snowden After the Moscow protests in 2011-2012, Vladimir Putin became terrified of the internet as a dangerous means for political mobilization and uncensored public debate. Only four years later, the Kremlin used that same platform to disrupt the 2016 presidential election in the United States. How did this transformation happen? The Red Web is a groundbreaking history of the Kremlin's massive online-surveillance state that exposes just how easily the internet can become the means for repression, control, and geopolitical warfare. In this bold, updated edition, Andrei Soldatov and Irina Borogan offer a perspective from Moscow with new and previously unreported details of the 2016 hacking operation, telling the story of how Russia came to embrace the disruptive potential of the web and interfere with democracy around the world.

At the Nexus of Cybersecurity and Public Policy

Ideas of masculinity and femininity become sharply defined in war-reliant societies, resulting in a presumed enmity between men and women. This so-called "battle of the sexes" is intensified by the use of misogyny to encourage men and boys to conform to the demands of masculinity. These are among Tom Digby's fascinating insights shared in Love and War, which describes the making and manipulation of gender in militaristic societies and the sweeping consequences for men and women in their personal, romantic, sexual, and professional lives. Drawing on cross-cultural comparisons and examples from popular media, including sports culture, the rise of "gonzo" and "bangbus" pornography, and "internet trolls," Digby describes how the hatred of women and the suppression of empathy are used to define masculinity, thereby undermining relations between women and men—sometimes even to the extent of violence. Employing diverse philosophical methodologies, he identifies the cultural elements that contribute to heterosexual antagonism, such as an enduring faith in male force to solve problems, the glorification of violent men who suppress caring emotions, the devaluation of men's physical and emotional lives, an imaginary gender binary, male privilege premised on the subordination of women, and the use of misogyny to encourage masculine behavior. Digby tracks the "collateral damage" of this disabling misogyny in the lives of both men and women, but ends on a hopeful note. He ultimately finds the link between war and gender to be dissolving in many societies: war is becoming slowly de-gendered, and gender is becoming slowly de-militarized.

Security Relations between China and the European Union

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

Conflict and Cooperation in the Global Commons

This book provides a comprehensive analysis of the Chinese-Russian bilateral relationship, grounded in a historical perspective, and discusses the implications of the burgeoning 'strategic partnership' between these two major powers for world order and global geopolitics. The volume compares the national worldviews, priorities, and strategic visions for the Chinese and Russian leadership, examining several aspects of the relationship in detail. The energy trade is the most important component of economic ties, although both sides desire to broaden trade and investments. In the military realm, Russia sells advanced arms to China, and the two countries engage in regular joint exercises. Diplomatically, these two Eurasian powers take similar approaches to conflicts in Ukraine and Syria, and also cooperate on non-traditional security issues including preventing coloured revolutions, cyber management, and terrorism. These issue areas illustrate four themes. Russia and China have common interests that cement their partnership, including security, protecting authoritarian institutions, and re-shaping aspects of the global order. They are key players not only influencing regional issues, but also international norms and institutions. The Sino-Russian partnership presents a potential counterbalance to the United States and democratic nations in shaping the contemporary and emerging geopolitical landscape. Nevertheless, the West is still an important partner for China and Russia. Both seek better relations with the

West, but on the basis of 'mutual respect' and 'equality'. Lastly, Russia and China have frictions in their relationship, and not all of their interests overlap. The Sino-Russian relationship has gained considerable momentum, particularly since 2014 as Moscow turned to Beijing attempting to offset tensions with the West in the aftermath of Russia's annexation of Crimea and intervention in Ukraine. However, so far, China and Russia describe their relationship as a comprehensive 'strategic partnership', but they are not 'allies'.

Love and War

In this updated edition of The Hacked World Order, cybersecurity expert Adam Segal offers unmatched insight into the new, opaque global conflict that is transforming geopolitics. For more than three hundred years, the world wrestled with conflicts between nation-states, which wielded military force, financial pressure, and diplomatic persuasion to create "world order." But in 2012, the involvement of the US and Israeli governments in Operation "Olympic Games," a mission aimed at disrupting the Iranian nuclear program through cyberattacks, was revealed; Russia and China conducted massive cyber-espionage operations; and the world split over the governance of the Internet. Cyberspace became a battlefield. Cyber warfare demands that the rules of engagement be completely reworked and all the old niceties of diplomacy be recast. Many of the critical resources of statecraft are now in the hands of the private sector, giant technology companies in particular. In this new world order, Segal reveals, power has been well and truly hacked.

Cyber Policy in China

The United States is a nation in crisis. While Washington’s ability to address our most pressing challenges has been rendered nearly impotent by ongoing partisan warfare, we face an array of foreign-policy crises for which we seem increasingly unprepared. Among these, none is more formidable than the unprecedented partnership developing between Russia and China, suspicious neighbors for centuries and fellow Communist antagonists during the Cold War. The two longtime foes have drawn increasingly close together because of a confluence of geostrategic, political, and economic interests—all of which have a common theme of diminishing, subverting, or displacing American power. While America’s influence around the world recedes—in its military and diplomatic power, in its political leverage, in its economic might, and, perhaps most dangerously, in the power and appeal of its ideas—Russia and China have seen their influence increase. From their support for rogue regimes such as those in Iran, North Korea, and Syria to their military and nuclear buildups to their aggressive use of cyber warfare and intelligence theft, Moscow and Beijing are playing the game for keeps. Meanwhile America, pledged to “leading from behind,” no longer does much leading at all. In The Russia-China Axis, Douglas E. Schoen and Melik Kaylan systematically chronicle the growing threat from the Russian-

Chinese Axis, and they argue that only a rebirth of American global leadership can counter the corrosive impact of this antidemocratic alliance, which may soon threaten the peace and security of the world.

The Red Web

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 Security

Information security is a critical consideration for any organization that depends on info. systems and computer networks to carry out its mission or business. It is especially important for gov¿t. agencies, where maintaining the public's trust is essential. The need for a vigilant approach to info. security has been demonstrated by the pervasive and sustained computerbased (cyber) attacks againimpactst the U.S. and others that continue to pose a potentially devastating to systems and the operations and critical infrastructures that they support. This report describes: (1) cyber threats to fed. info. systems and cyberbased critical infrastructures; and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. Ill.

The Cybersecurity Dilemma

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.

National Security Strategy of the United States

A RAND study analyzed Chinese and U.S. military capabilities in two scenarios (Taiwan and the Spratly Islands) from 1996 to 2017, finding that trends in most, but not all, areas run strongly against the United States. While U.S. aggregate power remains greater than China's, distance and geography affect outcomes. China is capable of challenging U.S. military dominance on its immediate periphery—and its reach is likely to grow in the years ahead.

The Hacker and the State

The Oxford Handbook on the United Nations

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.

Emerging Cyber Threats and Cognitive Vulnerabilities

Analyzing Russia’s sovereign democracy regime this paper draws a conclusion that in the medium term future the Kremlin control over the Internet is bound to intensify. Examining the most recent changes in the Russian legal systems as far as the freedom of the Internet is concerned it becomes evident that the events in the Arab world and the unrest at home in 2011 has put the Kremlin on a road towards greater Internet control. Events in the Ukraine and Snowden revelations are accelerating the process as well as are wining more Russians to the Kremlin way of thinking. Finally this paper attempts to forecast possible actions by the Russian government towards the Internet freedom in the years leading to the Duma elections in 2016 and the Presidential elections in 2018.

China and Cybersecurity

This Handbook provides in one volume an authoritative and independent treatment of the UN's seventy-year history, written by an international cast of more than 50 distinguished scholars, analysts, and practitioners. It provides a clear and penetrating examination of the UN's development since 1945 and the challenges and opportunities now facing the organization. It assesses the implications for the UN of rapid changes in the world - from technological innovation to shifting foreign policy priorities - and the UN's future place in a changing multilateral landscape. Citations and additional readings contain a wealth of primary and secondary references to the history, politics, and law of the world organization. This key reference also contains appendices of the UN Charter, the Statute of the International Court of Justice, and the Universal Declaration of Human Rights.

China, Russia, and Twenty-First Century Global Geopolitics

Originally published in hardcover in 2019 by Doubleday.

Cyber Threat!

Emerging Cyber Threats and Cognitive Vulnerabilities identifies the critical role human behavior plays in cybersecurity and provides insights into how human decision-making can help address rising volumes of cyberthreats. The book examines the role of psychology in cybersecurity by addressing each actor involved in the process: hackers, targets, cybersecurity practitioners and the wider social context in which these groups operate. It applies psychological factors such as motivations, group processes and decision-making heuristics that may lead individuals to underestimate risk. The goal of this understanding is to more quickly identify threat and create early education and prevention strategies. This book covers a variety of topics and addresses different challenges in response to changes in the ways in to study various areas of decision-making, behavior, artificial intelligence, and human interaction in relation to cybersecurity. Explains psychological factors inherent in machine learning and artificial intelligence Discusses the social psychology of online radicalism and terrorist recruitment Examines the motivation and decision-making of hackers and "hacktivists" Investigates the use of personality psychology to extract secure information from individuals

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk

“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. Buchanancaptures 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.

Droit Et Politique Étrangère

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Cyberpower and National Security

This timely and compelling book presents a broad study of all key cyber security issues of the highest interest to government and business as well as their implications. • Takes a broad approach to the problems of cyber security, covering every important issue related to the threats cyber security poses to government and business • Provides detailed coverage of the political, financial, data protection, privacy, and reputational problems caused by cyber attacks • Offers a forward-looking approach, discussing emerging trends that will bring new challenges to those charged with enhancing cyber security • Makes insightful suggestions into how nations and businesses can take steps to enhance their cyber security

Every Nation for Itself

The Perfect Weapon

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.

Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks

More than ever, international security and economic prosperity depend upon safe access to the shared domains that make up the global commons: maritime, air, space, and cyberspace. Together these domains serve as essential conduits through which international commerce, communication, and governance prosper. However, the global commons are congested, contested, and competitive. In the January 2012 defense strategic guidance, the United States confirmed its commitment “to continue to lead global efforts with capable allies and partners to assure access to and use of the global commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities.” In the face of persistent threats, some hybrid in nature, and their consequences, Conflict and Cooperation in the Global Commons provides a forum where contributors identify ways to strengthen and maintain responsible use of the global commons. The result is a comprehensive approach that will enhance, align, and unify commercial industry, civil agency, and military perspectives and actions.

Sandworm

SOON TO BE AN HBO® DOCUMENTARY FROM AWARD-WINNING DIRECTOR JOHN MAGGIO * "An important--and deeply sobering--new book about cyberwarfare" (Nicholas Kristof, New York Times), now updated with a new chapter. The Perfect Weapon is the startling inside story of how the rise of cyberweapons transformed geopolitics like nothing since the invention of the atomic bomb. Cheap to acquire, easy to deny, and usable for a variety of malicious purposes, cyber is now the weapon of choice for democracies, dictators, and terrorists. Two presidents--Bush and Obama--drew first blood with Operation Olympic Games, which used malicious code to blow up Iran's nuclear centrifuges, and yet America proved remarkably unprepared when its own weapons were stolen from its arsenal and, during President Trump's first year, turned back on the United States and its allies. And if Obama would begin his presidency by helping to launch the new era of cyberwar, he would end it struggling unsuccessfully to defend against Russia's broad attack on the 2016 US election. Moving from the White House Situation Room to the dens of Chinese government hackers to the boardrooms of Silicon Valley, New York Times national security correspondent David Sanger reveals a world coming face-to-face with the perils of technological revolution, where everyone is a target. "Timely and bracing . . . With the deep knowledge and bright clarity that have long characterized his work, Sanger recounts the cunning and dangerous development of cyberspace into the global battlefield of the 21st century." --Washington Post

Dawn of the Code War

Over the past decade, the EU and China have expanded their relations beyond a focus on economic and trade issues to the sphere of security. Taking a broad definition of security, a multidisciplinary approach, and a comparative perspective (including scholars from both Europe and China), this book provides an in-depth analysis of the extent to which the EU and China not only express similar threat concerns, or make declarations about joint responses, but also adopt concrete measures in the pursuance of security cooperation. In particular, the book seeks to explore a range of key themes in the field of EU-China security cooperation such as nuclear proliferation, international terrorist threats and cyber attacks. Besides providing an overview of the areas where security cooperation exists and where it does not, it also highlights the aspects of convergence and divergence and the reasons for their occurrence.

Challenges to Security in Space

The Internet has given rise to new opportunities for the public sector to improve efficiency and better serve constituents. But with an increasing reliance on the Internet, digital tools are also exposing the public sector to new risks. This accessible primer focuses on the convergence of globalization, connectivity, and the migration of public sector functions online. It examines emerging trends and strategies from around the world and offers practical guidance for addressing contemporary risks. It supplies an overview of relevant U.S. Federal cyber incident response policies and outlines an organizational framework for assessing risk.

The U.S.-China Military Scorecard

This book explores current and emerging trends in policy, strategy, and practice related to cyber operations conducted by states and non-state actors. The book examines in depth the nature and dynamics of conflicts in the cyberspace, the geopolitics of cyber conflicts, defence strategy and practice, cyber intelligence and information security.

Inside Cyber Warfare

CNN’s Chief National Security Correspondent reveals the invisible fronts of twenty-first century warfare and identifies the ongoing battles being waged—often without the public’s full knowledge—from disinformation campaigns to advanced satellite weaponry. The United States is currently under attack from multiple adversaries—yet most Americans have no idea of the dangers threatening us. In this eye-opening book, military and intelligence expert and seasoned reporter Jim Sciutto traces the expanding web of attacks that together amount to an undeclared but deeply dangerous war on America. With in-depth reporting from Ukraine to the South China Sea, Cuba to the earth’s atmosphere, unprecedented access to America’s Space Command, and new information from inside the intelligence agencies tracking election interference, Sciutto draws on his deep knowledge, high-level contacts, and personal experience as a journalist and diplomat to paint the most comprehensive and vivid picture of a nation targeted by a new and disturbing brand of warfare. America is engaged in a Shadow War on multiple fronts, with multiple enemies. The practitioners include America’s most familiar adversaries: Russia, China, North Korea, and Iran. But unlike conventional warfare, these conflicts are conducted in the shadows, with no formal declaration and often use multiple sources, from influential businessmen and lawyers to hackers.

And it is happening today. But America is adapting and fighting back. In The Shadow War, Sciutto introduces the dizzying array of soldiers, sailors, submariners and their commanders, space engineers, computer scientists, and civilians who are on the front lines of this new kind of forever war. Intensive and disturbing, this invaluable and important work opens our eyes and makes clear that future war is here.

Confronting an "Axis of Cyber"?

Few doubt that China wants to be a major economic and military power on the world stage. To achieve this ambitious goal, however, the PRC leadership knows that China must first become an advanced information-based society. But does China have what it takes to get there? Are its leaders prepared to make the tough choices required to secure China’s cyber future? Or is there a fundamental mismatch between China’s cyber ambitions and the policies pursued by the CCP until now? This book offers the first comprehensive analysis of China’s information society. It explores the key practical challenges facing Chinese politicians as they try to marry the development of modern information and communications technology with old ways of governing their people and conducting international relations. Fundamental realities of the information age, not least its globalizing character, are forcing the pace of technological change in China and are not fully compatible with the old PRC ethics of stability, national industrial strength and sovereignty. What happens to China in future decades will depend on the ethical choices its leaders are willing to make today. The stakes are high. But if China’s ruling party does not adapt more aggressively to the defining realities of power and social organization in the information age, the ‘China dream’ looks unlikely to become a reality.

Cyber Threats from China, Russia, and Iran

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.

Internet Governance in an Age of Cyber Insecurity

Given the wide-ranging implications for global competition, domestic political systems and daily life, US policymakers must prepare for the impacts of new artificial intelligence (AI)-related technologies. Anticipating AI's impacts on the global order requires US policy makers' awareness of certain key aspects of the AI-related technologies--and how those technologies will interact with the rapidly changing global system of human societies. One area that has received little in-depth examination to date is how AI-related technologies could affect countries' domestic political systems--whether authoritarian, liberal democratic, or a hybrid of the two--and how they might impact global competition between different regimes. This work highlights several key areas where AI-related technologies have clear implications for globally integrated strategic planning and requirements.

Current and Emerging Trends in Cyber Operations

Cyber Threats from China, Russia, and Iran

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.

The Hacked World Order

The new US National Cyber Strategy points to Russia, China, North Korea and Iran as the main international actors responsible for launching malicious cyber and information warfare campaigns against Western interests and democratic processes. Washington made clear its intention of scaling the response to the magnitude of the threat, while actively pursuing the goal of an open, secure and global Internet. The first Report of the ISPI Center on Cybersecurity focuses on the behaviour of these “usual suspects”, investigates the security risks implicit in the mounting international confrontation in cyberspace, and highlights the current irreconcilable political cleavage between these four countries and the West in their respective approaches “in and around” cyberspace.

Cyber War

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN’S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION