Cyber Security Law The China Approach

CYBER SECURITY LAWCyber security is an increasingly important domain today. Countries across the world are concerned about breaches of cyber security which could prejudicially impact their sovereignty and their national security. Consequently, cyber security law as a discipline has emerged. This Book will aim to look at what exactly is this emerging discipline of cyber security law. How the said discipline has been defined? What is the significance of cyber security and connected legal, policy and regulatory issues? How significant is this new discipline of cyber security law likely to be in the coming times? This Book has been written in the simple layman language to analyze complicated technical issues connected with legalities concerning breaches of computer networks and computer systems. This Book is authored by Pavan Duggal (http://www.pavanduggal.com), Asia's and India's foremost expert on Cyberlaw and Mobile Law, who has been acknowledged as one of the top four cyber lawyers of the world. This Book's Author runs his niche law firm Pavan Duggal Associates, Advocates (http://pavanduggalassociates.com/) which is working on all aspects concerning technology and the law. © Pavan Duggal, 2015

Explains the rapid rise of China's innovation system and provides a roadmap for the prospects of China's AI development.

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.

The emergence of severe acute respiratory syndrome (SARS) in late 2002 and 2003 challenged the global public health community to confront a novel epidemic that spread rapidly from its origins in southern China until it had reached more than 25 other countries within a matter of months. In addition to the number of patients infected with the SARS virus, the disease had profound economic and political repercussions in many of the affected regions. Recent reports of isolated new SARS cases and a fear that the disease could reemerge and spread have put public health officials on high alert for any indications of possible new outbreaks. This report examines the response to SARS by public health systems in individual countries, the biology of the SARS coronavirus and related coronaviruses in animals, the economic and political fallout of the SARS epidemic, quarantine law and other public health measures that apply to combating infectious diseases, and the role of international organizations and scientific cooperation in halting the spread of SARS. The report provides an illuminating survey of findings from the epidemic, along with an assessment of what might be needed in order to contain any future outbreaks of SARS or other emerging infections.

CyberBRICS

Cyber Security: Law and Guidance

The Privacy, Data Protection and Cybersecurity Law Review

Blockchain and Trustworthy Systems

Law as a Weapon of War

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

21st Century Chinese Cyberwarfare draws from a combination of business, cultural, historical and linguistic sources, as well as the author's personal experience, to attempt to explain China to the uninitiated. The objective of the book is to present the salient information regarding the use of cyber warfare doctrine by the People's Republic of China to promote its own interests and enforce its political, military and economic will on other nation states. The threat of Chinese Cyberwarfare can no longer be ignored. It is a clear and present danger to the experienced and innocent alike and will be economically, societally and culturally changing and damaging for the nations that are targeted.

Undisputedly, China has become the world's manufacturing powerhouse, accounting for around half of all personal computers, digital cameras and kitchen appliances. However, the country is fast transitioning from low-cost manufacturing to a higher-value, innovation-led economy, a critical transformation that is at the heart of this new title. Companies are the essential engines of the wealth-creation process, particularly in the areas of internet and mobile telecommunications, and firms such as Tencent and Xiaomi are showing clear potential to become major players. Demonstrating strong commitment to the country's relentless progress in the realm of innovation, the Chinese government has encouraged the development of a business environment in which firms can experiment, operate and thrive. Created in China provides an examination of the critical human factors at play, as well as re-assessing some of the metrics traditionally used to describe and measure China's capacity for innovation. As Chinese firms begin to transform the country into a truly global innovator, the emerging patterns of future innovation are identified and reviewed. New and dynamic practices are arising that are recognisably Chinese, yet at the same time capable of competing on the world stage. Following the successes of firms such as Huawei, Haier and Lenovo, a growing number of technology-focused firms are now turning their attention towards markets outside of China – a development that will not only benefit the country but will provide exciting opportunities for businesses throughout the world.

This book is the first one that comprehensively discusses cyberspace sovereignty in China, reflecting China ' s clear attitude in the global Internet governance: respecting every nation ' s right to independently choose a development path, cyber management modes and Internet public policies and to participate in the international cyberspace governance on an equal footing. At present, the concept of cyberspace sovereignty is still very strange to many people, so it needs to be thoroughly analyzed. This book will not only help scientific and technical workers in the field of cyberspace security, law researchers and the public understand the development of cyberspace sovereignty at home and abroad, but also serve as reference basis for the relevant decision-making and management departments in their work.

This book analyzes China ' s foreign technology acquisition activity and how this has helped its rapid rise to superpower status. Since 1949, China has operated a vast and unique system of foreign technology spotting and transfer aimed at accelerating civilian and military development, reducing the cost of basic research, and shoring up its power domestically and abroad—without running the political risks borne by liberal societies as a basis for their creative developments. While discounted in some circles as derivative and consigned to perpetual catch-up mode, China ' s "hybrid" system of legal, illegal, and extralegal import of foreign technology, combined with its indigenous efforts, is, the authors believe, enormously effective and must be taken seriously. Accordingly, in this volume, 17 international specialists combine their scholarship to portray the system ' s structure and functioning in heretofore unseen detail, using primary Chinese sources to demonstrate the perniciousness of the problem in a manner not likely to be controverted. The book concludes with a series of recommendations culled from the authors ' interactions with experts worldwide. This book will be of much interest to students of Chinese politics, US foreign policy, intelligence studies, science and technology studies, and International Relations in general.

Behavior, Power and Diplomacy

Bulk Collection

The Cybersecurity Dilemma

21st Century Chinese Cyberwarfare

How Chinas' Cyber Security Law Affects International Business, Trade in Services and the Electronic data Transfer

The Next Wave

Tallinn Manual 2.0 expands on the highly influential first edition by extending its coverage of the international law governing cyber operations to peacetime legal regimes. The product of a three-year follow-on project by a new group of twenty renowned international law experts, it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule. Although Tallinn Manual 2.0 represents the views of the experts in their personal capacity, the project benefitted from the unofficial input of many states and over fifty peer reviewers.

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.

This is an open access title available under the terms of a CC BY-NC-ND 4.0 International licence. It is free to read at Oxford Scholarship Online and offered as a free PDF download from OUP and selected open access locations. This book is the culmination of nearly six years of research initiated by Fred Cate and Jim Dempsey to examine national practices and laws regarding systematic government access to personal information held by private-sector companies. Leading an effort sponsored by The Privacy Projects, they commissioned a series of country reports, asking national experts to uncover what they could about government demands on telecommunications providers and other private-sector companies to disclose bulk information about their customers. Their initial research found disturbing indications of systematic access in countries around the world. These data collection programs, often undertaken in the name of national security, were cloaked in secrecy and largely immune from oversight, posing serious threats to personal privacy. After the Snowden leaks confirmed these initial findings, the project morphed into something more ambitious: an effort to explore what should be the rules for government access to private-sector data, and how companies should respond to government demands for access. This book contains twelve updated country reports plus eleven analytic chapters that present descriptive and normative frameworks for assessing national surveillance laws, survey evolving international law and human rights principles applicable to government surveillance, and describe oversight mechanisms. It also explores the concept of accountability and the role of encryption in shaping the surveillance debate. Cate and Dempsey conclude by offering recommendations for both governments and industry.

The book examines the extent to which Chinese cyber and network security laws and policies act as a constraint on the emergence of Chinese entrepreneurialism and innovation. Specifically, how the contradictions and tensions between data localisation laws (as part of Network Sovereignty policies) affect innovation in artificial intelligence (AI). The book surveys the globalised R&D networks, and how the increasing use of open-source platforms by leading Chinese AI firms during 2017–2020, exacerbated the apparent contradiction between Network Sovereignty and Chinese innovation. The drafting of the Cyber Security Law did not anticipate the changing nature of globalised AI innovation. It is argued that the deliberate deployment of what the book refers to as 'fuzzy logic' in drafting the Cyber Security Law allowed regulators to subsequently interpret key terms regarding data in that Law in a fluid and flexible fashion to benefit Chinese innovation.

The Oxford Handbook of the International Law of Global Security

Reflections on building a community of common future in cyberspace

Cybersecurity Regulations in the BRICS Countries

Learning from SARS

International Cybersecurity and Privacy Law in Practice

Hacking, Trust and Fear Between Nations

What new directions in China"s digital economy mean for us all China is the largest homogenous digital market on Earth: unified by language, culture, and mobile payments. Not only a consumer market of unrivaled size, it"s also a vast and hyperactive innovation ecosystem for new technologies. And as China"s digital economy moves from a consumer-focused phase to an enterprise-oriented one, Chinese companies are rushing to capitalize on ways the newer wave of tech--the Internet of Things, AI, blockchain, cloud computing, and data analytics (iABCD)--can unlock value for their businesses from non-traditional angles. In China"s Data Economy, Winston Ma--investment professional, capital markets attorney, adjunct professor of digital economy, and bestselling author--details the profound global implications of this new direction, including how Chinese apps for services such as food delivery expand so quickly they surpass their U.S. models within a couple of years, and how the sheer scale and pace of Chinese innovation might lead to an AI arms race in which China and the U.S. vie aggressively for leadership. How China"s younger netizens participate in their evolving digital economy as consumers, creators, and entrepreneurs Why Online/Office (OMO, Online-merge-with-Offline) integration is viewed as the natural next step on from the O2O (Online-to-Offline) model used in the rest of the world The ways in which traditional Chinese industries such as retail, banking, and insurance are innovating to stay in the game What emerging markets can learn from China as they leapfrog past the personal computer age altogether, diving straight into the mobile-first economy Anyone interested in what"s next for Chinese digital powerhouses--investors, governments, entrepreneurs, international business players--will find this an essential guide to what lies ahead as China"s flexes new digital muscles to create new forms of value and challenge established tech giants across the world.

This companion provides the most comprehensive and up-to-date comparative overview of the cyber-security strategies and doctrines of the major states and actors in Europe, North America, South America, Africa, and Asia. The volume offers an introduction to each nation's cyber-security strategy and policy, along with a list of resources in English that may be consulted for those wishing to go into greater depth. Each chapter is written by a leading academic or policy specialist, and contains the following sections: overview of national cyber-security strategy; concepts and definitions; exploration of cyber-security issues as they relate to international law and governance; critical examinations of cyber partners at home and abroad; legislative developments and processes; dimensions of cybercrime and cyberterrorism; implications of cyber-security policies and strategies. This book will be of much interest to students and practitioners in the fields of cyber-security, national security, strategic studies, foreign policy, and international relations.

Volume 38 of the Chinese (Taiwan) Yearbook of International Law and Affairs publishes scholarly articles and essays on international and transnational law, as well as compiles official documents on the state practice of the Republic of China (Taiwan) in 2020.

International Cybersecurity and Privacy Law in Practice balances privacy and cybersecurity legal knowledge with technical knowledge and business acumen needed to provide adequate representation and consultation both within an organization, such as a government entity or business, and when advising these organizations as external counsel. Although organizations collect information, including personal data, in increasing volume, they often struggle to identify privacy laws applicable to complex, multinational technology implementations. Jurisdictions worldwide now include specific cybersecurity obligations in privacy laws and have passed stand-alone cybersecurity laws. To advise on these compliance matters, attorneys must understand both the law and the technology to which it applies. This book provides an innovative, in-depth survey and analysis of international information privacy and cybersecurity laws worldwide, an introduction to cybersecurity technology, and a detailed guide on organizational practices to protect an organization's interests and anticipate future compliance developments. It also introduces cybersecurity industry standards, developing cybersecurity legal developments, and international data localization laws. What's in this book: This book explores international information privacy laws applicable to private and public organizations, including employment and marketing-related compliance requirements and industry-specific guidance. It introduces a legal approach based on industry best practices to creating and managing an effective cybersecurity and privacy program that includes the following and more: prompt, secure ways to identify threats, manage vulnerabilities, and respond to "incidents"; defining the accountability of the "data controller" within an organization; roles of transparency and consent; privacy notice as contract; rights of revocation, erasure, and correction; de-identification and anonymization procedures; records retention; and data localization. Regulations and applicable "soft law" will be explored in detail for a wide variety of jurisdictions, including an introduction to the European Union's Global Data Protection Regulation (GDPR), China's Cybersecurity Law, the OECD and APEC Guidelines, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and many other national and regional instruments. How this will help you: This book is an indispensable resource for attorneys who must advise on strategic implementation of new technologies, advise on the impact of certain laws to the enterprise, interpret complex cybersecurity and privacy contractual language, and participate in incident response and data breach activities. It will also be of value to other practitioners from a broader perspective, such as compliance and security personnel, who need a reference exploring privacy and data protection laws and their connection with security technologies.

Espionage, Strategy, and Politics in the Digital Domain

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws

Cyber Security, Artificial Intelligence, Data Protection & the Law

Third International Conference, BlockSys 2021, Guangzhou, China, August 5–6, 2021, Revised Selected Papers

Chinese Cyber Crime

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

Chinese Cyber Crime is the first comprehensive book describing the hacking underworld within the People's Republic of China. Based upon direct field research and experience with Chinese hackers this book goes where no other has gone before. China's latest national security law and draft cyber security sovereignty law are introduced and reviewed in applicability to China's efforts to control nefarious Chinese cybercrime. Industry advice and guidance aptly provided by Tommy Stiansen, CTO, Norse Corporation.

This collection explores the relevance of global trade law for data, big data and cross-border data flows. Contributing authors from different disciplines including law, economics and political science analyze developments at the World Trade Organization and in preferential trade venues by asking what future-oriented models for data governance are available and viable in the area of trade law and policy. The collection paints the broad picture of the interaction between digital technologies and trade regulation as well as provides in-depth analyses of critical to the data-driven economy issues, such as privacy and AI, and different countries' perspectives. This title is also available as Open Access on Cambridge Core.

In today□s litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider□s The Manager□s Guide to Cybersecurity Law: Essentials for Today□s Business, lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, □My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security.□ In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore □ and prepare to apply □ cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure □ and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy □ and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department.

How China is Becoming a Global Innovator

Cyber Dragon: Inside China's Information Warfare and Cyber Operations

China's Rule of Law in Cybersecurity Over the Past 40 Years

Cyberspace Sovereignty

Cybersecurity Law, Standards and Regulations, 2nd Edition

Essentials for Today's Business

On a global scale, the central tool for responding to complex security challenges is public international law. This handbook provides a comprehensive and systematic overview of the relationship between international law and global security.

Chinese Internet Law represents a comprehensive, systematic, and up-to-date introduction to the Chinese laws governing the use of the Internet, also known as the information network. This book introduces the framework of China¿s legal system and the different levels of laws applicable to the Internet. It explores Internet law in China by carving out several key areas and exploring a wide range of topics, such as domain name, operation of an Internet service business, electronic contract and signature, intellectual property, e-commerce, and much more. By presenting many case illustrations, this book stresses the practical application of the law that is faced by both individuals and organizations in Chinese cyberspace. Further, with analysis of cases based on theoretical underpinnings, this book is particularly valuable to legal and business academics as well as professionals who have an interest in understanding Internet regulations and related activities in China. Identifies applicable Chinese laws governing the use of the Internet Explores systematic updates with easy-to-understand interpretations of legal doctrines, principles, and statutes Practice-focused cases with illustrations exemplify how Chinese Internet laws are currently enforced Comprehensive and broad-spectrum coverage of a myriad of topics with regard to cyberspace Perfect for legal and business academics, as well as professionals who have an interest in the regulation of the Internet

This book provides a comparison and practical guide of the data protection laws of Canada, China (Hong Kong, Macau, Taiwan), Laos, Philippines, South Korea, United States and Vietnam. The book builds on the first book Data Protection Law. A Comparative Analysis of Asia-Pacific and European Approaches, Robert Walters, Leon Trakman, Bruno Zeller. As the world comes to terms with Artificial Intelligence (AI), which now pervades the daily lives of everyone. For instance, our smart or Iphone, and smart home technology (robots, televisions, fridges and toys) access our personal data at an unprecedented level. Therefore, the security of that data is increasingly more vulnerable and can be compromised. This book examines the interface of cyber security, AI and data protection. It highlights and recommends that regulators and governments need to undertake wider research and law reform to ensure the most vulnerable in the community have their personal data protected adequately, while balancing the future benefits of the digital economy.

"International military interventions can be extremely costly in terms of monetary resources, logistical challenges, and possible soldier and civilian casualties, as well as the potential for catastrophic results to international relations and agreements. In one such example of these enormous potential costs, the US and UK wished to stop a Russian ship from delivering ammunition to the Assad regime in Syria in 2012. Intercepting or confronting a Russian ship in transit could have erupted into open conflict, so they sought an alternative, non-confrontational maneuver: instead of military intervention, the UK persuaded the ship's insurer, London's Standard Club, to withdraw the ship's insurance. This loss of insurance caused the ship to return to Russia, thus avoiding an international clash as well as the delivery of deadly weapons to Syria. This use of legal maneuvering in lieu of armed force is known as "lawfare" and is becoming a critical strategic platform. In Lawfare, author Orde Kittrie's draws on his experiences as a lawfare practitioner, US State Department attorney, and international law scholar in analyzing the theory and practice of the strategic leveraging of law as an increasingly powerful and effective weapon in the current global security landscape. Lawfare incorporates case studies of recent offensive and defensive lawfare by the United States, Iran, China, and by both sides of the Israeli-Palestinian conflict and includes dozens of examples of how lawfare has thus been waged and defended against. Kittrie notes that since private attorneys can play important and decisive roles in their nations' national security plans through their expertise in areas like financial law, maritime insurance law, cyber law, and telecommunications law, the full scope of lawfare's impact and possibilities are just starting to be understood. With international security becoming an ever complicated minefield of concerns and complications, understanding this alternative to armed force has never been more important"--

Lawfare

China, Russia, and Twenty-First Century Global Geopolitics

Cyber Policy in China

Chinese (Taiwan) Yearbook of International Law and Affairs, Volume 38, 2020

Beyond Espionage

Systematic Government Access to Private-sector Data

This book stems from the CyberBRICS project, which is the first major attempt to produce a comparative analysis of Internet regulations in the BRICS countries – namely, Brazil, Russia, India, China, and South Africa. The project has three main objectives: 1) to map existing regulations; 2) to identify best practices; and 3) to develop policy recommendations in the various areas that compose cybersecurity governance, with a particular focus on the strategies adopted by the BRICS countries to date. Each study covers five essential dimensions of cybersecurity: data protection, consumer protection, cybercrime, the preservation of public order, and cyberdefense. The BRICS countries were selected not only for their size and growing economic and geopolitical relevance but also because, over the next decade, projected Internet growth is expected to occur predominantly in these countries. Consequently, the technology, policy and governance arrangements defined by the BRICS countries are likely to impact not only the 3.2 billion people living in them, but also the individuals and businesses that choose to utilize increasingly popular applications and services developed in BRICS countries according to BRICS standards. Researchers, regulators, start-up innovators and other Internet stakeholders will find this book a valuable guide to the inner workings of key cyber policies in this rapidly growing region.

The second edition of the definitive guide to cybersecurity law, updated to reflect recent legal developments The revised and updated second edition of Cybersecurity Law offers an authoritative guide to the key statutes, regulations, and court rulings that pertain to cybersecurity. Written by an experienced cybersecurity lawyer and law professor, the second edition includes new and expanded information that reflects the latest changes in laws and regulations. The book includes material on recent FTC data security consent decrees and data breach litigation. Topics covered reflect new laws, regulations, and court decisions that address financial sector cybersecurity, the law of war as applied to cyberspace, and recently updated guidance for public companies' disclosure of cybersecurity risks. This important guide: Provides a new appendix, with 15 edited opinions covering a wide range of cybersecurity-related topics, for students learning via the caselaw method Includes new sections that cover topics such as: compelled access to encrypted devices, New York's financial services cybersecurity regulations, South Carolina's insurance sector cybersecurity law, the Internet of Things, bug bounty programs, the vulnerability equities process, international enforcement of computer hacking laws, the California Consumer Privacy Act, and the European Union's Network and Information Security Directive Contains a new chapter on the critical topic of law of cyberwar Presents a comprehensive guide written by a noted expert on the topic Offers a companion Instructor-only website that features discussion questions for each chapter and suggested exam questions for each chapter Written for students and professionals of cybersecurity, cyber operations, management-oriented information technology (IT), and computer science, Cybersecurity Law, Second Edition is the up-to-date guide that covers the basic principles and the most recent information on cybersecurity laws and regulations. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He was a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

This book provides a comprehensive and systematic review of China's rule of law on cybersecurity over the past 40 years, from which readers can have a comprehensive view of the development of China's cybersecurity legislation, supervision, and justice in the long course of 40 years. In particular, this book combines the development node of China's reform and opening up with the construction of the rule of law for cybersecurity, greatly expanding the vision of tracing the origin and pursuing the source, and also making the study of the rule of law for China's cybersecurity closer to the development facts of the technological approach.--

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.

Governing Cyberspace

Big Data and Global Trade Law

Cyber Law in China

Research on the Rule of Law of China's Cybersecurity

Created in China

Getting to Yes with China in Cyberspace

This book provides a framework for assessing China's extensive cyber espionage efforts and multi-decade modernization of its military, not only identifying the "what" but also addressing the "why" behind China's focus on establishing information dominance as a key component of its military efforts. • Provides a detailed overview and thorough analysis of Chinese cyber activities • Makes extensive use of Chinese-language materials, much of which has not been utilized in the existing Western literature on the subject • Enables a better understanding of Chinese computer espionage by placing it in the context of broader Chinese information warfare activities • Analyzes Chinese military modernization efforts, providing a context for the ongoing expansion in China's military spending and reorganization • Offers readers policy-relevant insight into Chinese military thinking while maintaining academic-level rigor in analysis and source selection

In today's litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider's Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, "My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security." In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

EDWARD O. WILSON MEETS BARRY listening to the stories of local villagers; and examining the journals of conquistadors and explorers-they realize that the sea is but a ghost of what it once was.As they bear witness to the web of connections that ties humans to the Sea of Cortez, the students find themselves suspended between past and future-and imagine a way forward as they come to see one another, and themselves, in a new light. In a voice that resounds with compassionate humanity, Telling Our Way to the Sea captures the complex beauty of a marine world and the people whom Hirsh explores it with. - Winner of the 2013 National Outdoor Book Award - Literary natural history at its finest, for readers of Edward O. Wilson, Alan Weisman, and Bill McKibben

This study explores U.S. policy options for managing cyberspace relations with China via agreements and norms of behavior. If negotiations can lead to meaningful norms, this report looks at what each side might offer to achieve an acceptable outcome.

Cybersecurity in China

Dawn of the Code War

China and Cybersecurity

The Manager's Guide to Cybersecurity Law

Analysis within the scope of the General Agreement on Trade in Services

Cyber norms and other ways to regulate responsible state behavior in cyberspace is a fast-moving political and diplomatic field. The academic study of these processes is varied and interdisciplinary, but much of the literature has been organized according to discipline. Seeking to cross disciplinary boundaries, this timely book brings together researchers in fields ranging from international law, international relations, and political science to business studies and philosophy to explore the theme of responsible state behavior in cyberspace. . Divided into three parts, Governing Cyberspace first looks at current debates in and about international law and diplomacy in cyberspace. How does international law regulate state behaviour and what are its limits? How do cyber superpowers like China and Russia shape their foreign policy in relation to cyberspace? The second focuses on power and governance. What is the role for international organisations like NATO or for substate actors like intelligence agencies? How do they adapt to the realities of cyberspace and digital conflict? How does the classic balance of power play out in cyberspace and how do different states position themselves? The third part takes a critical look at multistakeholder and corporate diplomacy. How do global tech companies shape their role as norm entrepreneurs in cyberspace, and how do their cyber diplomatic efforts relate to their corporate identity?

This book constitutes the thoroughly refereed post conference papers of the Third International Conference on Blockchain and Trustworthy Systems, Blocksys 2021, held in Guangzhou, China, in August 2021.*The 38 full papers and the 12 short papers were carefully reviewed and selected from 98 submissions. The papers are organized in topical sections: Contents Blockchain and Data Mining; Performance Optimization of Blockchain; Blockchain Security and Privacy; Theories and Algorithms for Blockchain; Blockchain and Internet of Things; Blockchain and Smart Contracts; Blockchain Services and Applications; Trustworthy System Development.*

Implementing appropriate security measures will be an advantage when protecting organisations from regulatory action and litigation in cyber security law: can you provide a defensive shield? Cyber Security: Law and Guidance provides an overview of legal developments in cyber security and data protection in the European Union and the United Kingdom, focusing on the key cyber security laws and related legal instruments, including those for data protection and payment services. Additional context is provided through insight into how the law is developed outside the regulatory frameworks, referencing the 'Consensus of Professional Opinion' on cyber security, case law and the role of professional and industry standards for security. With cyber security law destined to become heavily contentious, upholding a robust security framework will become an advantage and organisations will require expert assistance to operationalise matters. Practical in approach, this comprehensive text will be invaluable for legal practitioners and organisations. It covers both the law and its practical application, helping to ensure that advisers and organisations have effective policies and procedures in place to deal with cyber security. Topics include: - Threats and vulnerabilities - Privacy and security in the workplace and built environment - Importance of policy and guidance in digital communications - Industry specialists' in-depth reports - Social media and cyber security - International law and interaction between states - Data security and classification - Protecting organisations - Cyber security: cause and cure Cyber Security: Law and Guidance is on the indicative reading list of the University of Kent's Cyber Law module.

This book offers the first benchmarking study of China's response to the problems of security in cyber space. There are several useful descriptive books on cyber security policy in China published between 2010 and 2016. As a result, we know quite well the system for managing cyber security in China, and the history of policy responses. What we don't know so well, and where this book is useful, is how capable China has become in this domain relative to the rest of the world. This book is a health check, a report card, on China's cyber security system in the face of escalating threats from criminal gangs and hostile states. The book also offers an assessment of the effectiveness of China's efforts. It lays out the major gaps and shortcomings in China's cyber security policy. It is the first book to base itself around an assessment of China's cyber industrial complex, concluding that China does not yet have one. As Xi Jinping said in July 2016, the country's core technologies are dominated by foreigners.

China's Quest for Foreign Technology

Chinese Internet Law

Cybersecurity Law

Inside China's Information Warfare and Cyber Operations

Preparing for the Next Disease Outbreak: Workshop Summary

China's Hacking Underworld

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 andinvestments. 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 includingpreventing 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 keyplayers 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 onthe 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 withthe 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'.

Routledge Companion to Global Cyber-Security Strategy

Cyber Security Law

China's Data Economy: How Its Innovation Power Is Shaping the Future of AI, Media, and the Global Or Der