cyber security law the china approach

#cybersecurity law #China cybersecurity #data security China #cyber regulations China #China internet policy

Explore China's unique approach to cybersecurity law, examining the regulations, policies, and measures implemented to govern cyberspace, data security, and internet activities within the country. Understand how China's cybersecurity strategy differs from other global approaches and the potential implications for businesses and individuals operating within its jurisdiction. This analysis delves into the key aspects of Chinese cybersecurity legislation and its impact on the digital landscape.

Research on the Rule of Law of China’s Cybersecurity

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.

China’s New Cyber Policy: Implication, Alterations, and Implementation

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.--

Research on the Rule of Law of China's Cybersecurity

All states are challenged by the need to protect national security while maintaining the rule of law, but the issue is particularly complex in the China–Hong Kong context. This timely and important book explores how China conceives of its national security and the position of Hong Kong. It considers the risks of introducing national security legislation in Hong Kong, and Hong Kong's sources of resilience against encroachments on its rule of law that may come under the guise of national security. It points to what may be needed to maintain Hong Kong's rule of law once China's 50-year commitment to its autonomy ends in 2047. The contributors to this book include world-renowned scholars in comparative

public law and national security law. The collection covers a variety of disciplines and jurisdictions, and both scholarly and practical perspectives to present a forward-looking analysis on the rule of law in Hong Kong. It illustrates how Hong Kong may succeed in resisting pressure to advance China's security interests through repressive law. Given China's growing international stature, the book's reflections on China's approach to security have much to tell us about its potential impact on the global political, security, and economic order.

China's National Security

An exploration of the current state of global trade law in the era of Big Data and AI. This title is also available as Open Access on Cambridge Core.

Big Data and Global Trade Law

This book provides a governance perspective on China’s digital authoritarianism by examining the political and institutional dynamics of the country’s internet sector in a historical context. Using leading theories of authoritarian institutions, it discusses China’s approach to the internet and methods of implementation in terms of party-state institutions and policy processes. This provides a much-needed ‘inside out’ perspective on digital authoritarianism that avoids the perception of China as some coherent and static monolith. The study also offers a powerful rationale for China’s cyber sovereignty as an externalisation of its domestic internet governance framework and broader political-economic context. As China shifts from rule-taker to rule-maker in world politics, the Chinese Dream (zhongguo meng) is now going global. Beijing’s digital authoritarian toolkit is being promoted and exported to other authoritarian regimes, making China a major driver of digital repression at the global level.

China’s Digital Authoritarianism

China's emergence as a great power in the twenty-first century is strongly enabled by cyberspace. Leveraged information technology integrates Chinese firms into the global economy, modernizes infrastructure, and increases internet penetration which helps boost export-led growth. China's pursuit of "informatization" reconstructs industrial sectors and solidifies the transformation of the Chinese People's Liberation Army into a formidable regional power. Even as the government censors content online, China has one of the fastest growing internet populations and most of the technology is created and used by civilians. Western political discourse on cybersecurity is dominated by news of Chinese military development of cyberwarfare capabilities and cyber exploitation against foreign governments, corporations, and non-governmental organizations. Western accounts, however, tell only one side of the story. Chinese leaders are also concerned with cyber insecurity, and Chinese authors frequently note that China is also a victim of foreign cyber -- attacks -- predominantly from the United States. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain is a comprehensive analysis of China's cyberspace threats and policies. The contributors -- Chinese specialists in cyber dynamics, experts on China, and experts on the use of information technology between China and the West -- address cyberspace threats and policies, emphasizing the vantage points of China and the U.S. on cyber exploitation and the possibilities for more positive coordination with the West. The volume's multi-disciplinary, cross-cultural approach does not pretend to offer wholesale resolutions. Contributors take different stances on how problems may be analyzed and reduced, and aim to inform the international audience of how China's political, economic, and security systems shape cyber activities. The compilation provides empirical and evaluative depth on the deepening dependence on shared global information infrastructure and the growing willingness to exploit it for political or economic gain.

China and Cybersecurity

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.

Cybersecurity in China

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.

Cyber Security, Artificial Intelligence, Data Protection & the Law

New Approaches to Human Security in the Asia-Pacific offers a distinctly Asia-Pacific-oriented perspective to one of the most discussed components of international security policy, human security. This volume of regional experts assess countries that have either spearheaded this form of security politics (Japan and Australia) or have recently advanced to become a key player on various aspects of human security in both a domestic and global context (China). The authors provide an interesting investigation into the continued relevance and promise of the human security paradigm against more 'traditional' security approaches. Accordingly the book will appeal to readers across a wide band of the social sciences (international relations, security studies, development studies and public policy) and to practitioners and analysts working in applied settings.

New Approaches to Human Security in the Asia-Pacific

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.

Cyberspace Sovereignty

In China, State Sovereignty and International Legal Order, Phil C.W. Chan explores the nexus between China’s exercise of State sovereignty and international legal order, and the locus in which State sovereignty resides in international law and foreign policy-making.

China, State Sovereignty and International Legal Order

This study explores U.S. policy options for managing cyberspace relations with China via agreements and norms of behavior. It considers two questions: Can negotiations lead to meaningful agreement on norms? If so, what does each side need to be prepared to exchange in order to achieve an acceptable outcome? This analysis should interest those concerned with U.S.-China relations and with developing norms of conduct in cyberspace.

Getting to Yes with China in Cyberspace

This revised and expanded edition of the Research Handbook on International Law and Cyberspace brings together leading scholars and practitioners to examine how international legal rules, concepts and principles apply to cyberspace and the activities occurring within it. In doing so, contributors highlight the difficulties in applying international law to cyberspace, assess the regulatory efficacy of these rules and, where necessary, suggest adjustments and revisions. More specifically, contributors explore the application of general concepts and principles to cyberspace such as those of

sovereignty, power, norms, non-intervention, jurisdiction, State responsibility, human rights, individual criminal responsibility and international investment law and arbitration. Contributors also examine how international law applies to cyber terrorism, cyber espionage, cyber crime, cyber attacks and cyber war as well as the meaning of cyber operations, cyber deterrence and the ethics of cyber operations. In addition, contributors consider how international and regional institutions such as the United Nations, the European Union, NATO and Asia-Pacific institutions and States such as China and Russia approach cyber security and regulation. This Research Handbook is an essential resource for scholars of international law, international relations and public and private law as well as for legal practitioners and policymakers.

Research Handbook on International Law and Cyberspace

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.

International Cybersecurity and Privacy Law in Practice

Place is inextricably linked to history by way of culture, language, philosophy, faith and the development of worldviews. The richness and depth of experience of the Asia-Pacific region has been under-studied, over-simplified and under-appreciated. This book addresses that lacuna in the subject area of international humanitarian law. Drawing on authoritative perspectives and interviews with experts in and on this topic, including four of the region's most distinguished international judges, forty-one chapters thematically examine the development of international humanitarian law; practice and application of international humanitarian law; implementation and enforcement of international humanitarian law; and looking to the future and enhancing compliance with international humanitarian law. The expert contributors draw out unique features, providing fresh insights to scholarship. Contributions on and from the area also grapple with the regional commitments to humanitarianism generally, illuminating how and why international humanitarian law might be more readily accepted or ignored in armed conflicts in the region.

Asia-Pacific Perspectives on International Humanitarian Law

Although the Right to Leave and Return (RLR) is a fundamental human right, each State has the sovereign right to regulate RLR in accordance with its own laws. In the case of China, the country's communist political system has significantly affected the development of RLR and the country's approach to it. As a rule, China's approach is restrictive. As part of its reform and 'opening up' policies, China has embarked on a range of reforms to liberalise RLR, but the reforms lack cohesion and focus, and remain restrictive. Given its past and its complex social and economic conditions, China may have some justifications for its approach, but on balance, has more to gain from adopting a more liberal approach. The issue of RLR in China is crucial both for the future of China, and for development of RLR in the world. The Right to Leave and Return (RLR) and Chinese Migration Law provides a comprehensive and systematic review of the RLR in international and Chinese migration law. It has been written on the basis of Chinese statutes pertinent to the RLR, also of relevant international instruments and key cases. It investigates RLR in international migration law and practice; analyses RLR in the context of China, and identifies its driving factors; investigates the conditions and practical concerns relevant to the protection of RLR; and concludes with recommendations on how the Chinese regulatory regime governing RLR can be improved.

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

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

The Right to Leave and Return and Chinese Migration Law

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 Privacy, Data Protection and Cybersecurity Law Review

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 Cybersecurity Dilemma

The first work to examine data privacy laws across Asia, covering all 26 countries and separate jurisdictions, and with in-depth analysis of the 14 which have specialized data privacy laws. Professor Greenleaf demonstrates the increasing world-wide significance of data privacy and the international context of the development of national data privacy laws as well as assessing the laws, their powers and their enforcement against international standards.

CyberBRICS

Non-international armed conflicts now far outnumber international ones, but the protection afforded by international law to combatants and civilian is not always clear. This book will set out the legal rules and state practice applicable to internal armed conflicts, drawing on armed conflicts from the US civil war to present day.

Cyber Policy in China

Following a general introduction, the book assembles its information and guidance in seven main areas of practice: the regulatory framework of the electronic communications market; software protection, legal protection of databases or chips, and other intellectual property matters; contracts with regard to software licensing and network services, with special attention to case law in this area; rules with regard to electronic evidence, regulation of electronic signatures, electronic banking, and electronic commerce; specific laws and regulations with respect to the liability of network operators and service providers and related product liability; protection of individual persons in the context of the processing of personal data and confidentiality; and the application of substantive criminal law in the area of ICT.

Asian Data Privacy Laws

Examines the interplay between artificial intelligence and international economic law, and its effects on global economic order. This title is also available as Open Access.

The Law of Non-International Armed Conflict

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.

Cyber Law in China

This volume "is the result of the China Maritime Studies Institute's annual conference in Newport during May 2010, which involved the participation of almost a dozen Chinese specialist presenters, who were able to exchange ideas with their American counterparts."--p. 2

Artificial Intelligence and International Economic Law

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

Bulk Collection

This publication has been issued in implementation of the United Nations Disarmament Information Programme as a handy, convenient and attractive reference tool containing the report of the Secretary-General on verification in all its aspects, including the role of the UN in the field of verification. It also contains additional material related to the publication of the report. The publication continues the Disarmament Study Series and should serve as a valuable addition to the reference section of public and university libraries, permanent missions, research institutes and specialized non-governmental organisations.

Not Congruent But Quite Complementary

Drawing on Chinese military writings, this report finds that China’s strategic-deterrence concepts are evolving in response to Beijing’s changing assessment of its external security environment and a growing emphasis on protecting its emerging interests in space and cyberspace. China also is rapidly closing what was once a substantial gap between the People’s Liberation Army’s strategic weapons capabilities and its strategic-deterrence concepts.

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

This Handbook is a detailed introduction to the numerous academic perspectives that apply to the study of the internet as a political, social and communicative phenomenon. Covering both practical and theoretical angles, established researchers from around the world discuss everything: the foundations of internet research appear alongside chapters on understanding and analyzing current examples of online activities and artifacts. The material covers all continents and explores in depth subjects such as networked gaming, economics and the law. The sheer scope and breadth of topics examined in this volume, which ranges from on-line communities to e-science via digital aesthetics, are evidence that in today’s world, internet research is a vibrant and mature field in which practitioners have long since stopped considering the internet as either an utopian or dystopian "new" space, but instead approach it as a medium that has become an integral part of our everyday culture and a natural mode of communication. This Second International Handbook of Internet Research is an updated version of the first International Handbook of Internet Research that came out in 2010. Since then, the field has changed, and this new version retains a number of the key updated chapters from the first handbook, as well as completely new chapters.

Developments in the Field of Information and Telecommunications in the Context of International Security

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.

China’s Evolving Approach to “Integrated Strategic Deterrence”

The best country-by-country assessment of human rights. The human rights records of more than ninety countries and territories are put into perspective in Human Rights Watch's signature yearly report. Reflecting extensive investigative work undertaken by Human Rights Watch staff, in close partnership with domestic human rights activists, the annual World Report is an invaluable resource for journalists, diplomats, and citizens, and is a must-read for anyone interested in the fight to protect human rights in every corner of the globe.

Second International Handbook of Internet Research

This is a comprehensive commentary on Chinese bilateral investment treaties (BITs), which are being increasingly used in Chinese foreign investment policy. It will define BITs' role, analyse and interpret their key provisions, and discuss the future of China's investment programme.

APEC Privacy Framework

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

Created in China

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.*

World Report 2020

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.

Chinese Investment Treaties