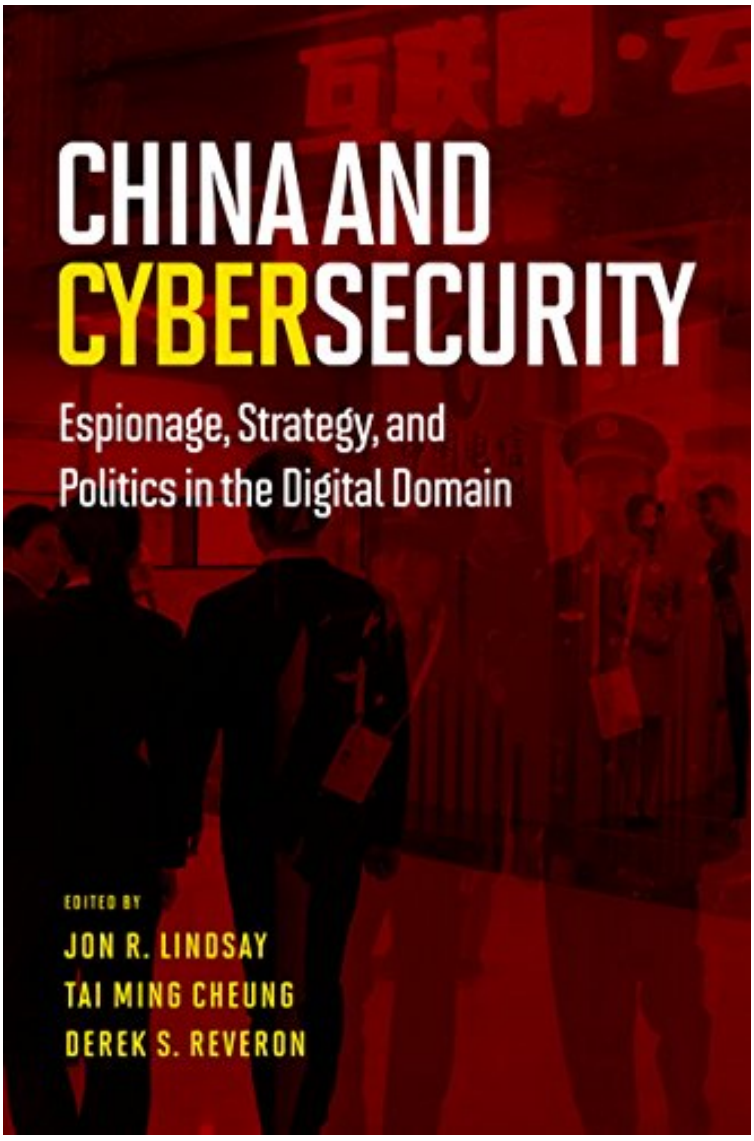
China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain

From Oxford University Press
*audiobook | *ebooks | Download PDF | ePub | DOC*



#836428 in eBooks 2015-03-02 2015-03-02File Name: B00U6DQRHG | File size: 42.Mb

From Oxford University Press : China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain before purchasing it in order to gage whether or not it would be worth my time, and all praised China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain:

1 of 1 people found the following review helpful. Well structured, researched and argued piece of work.By John EllisThe authors, an ensemble cast of academics, industry practitioners, and subject matter experts have painstakingly examined the multidimensional nature of Chinese activities in cyberspace, both domestically and

internationally.China, in less than 40 years has undertaken dramatic economic reform and growth to become the worldrsquo;s second-largest economy. With its rise, China has dramatically shaped and influenced the world economic balance and political landscape, and one can only expect some revisionism from a power rising as spectacularly as China.Nowhere is this revisionism more apparent than in the area of cyberspace where the Chinese are clearly squaring off against the hegemony of the United States in this highly strategic and politically charged domain.A key theme that appears to repeat itself in this book as in other writings on the Chinese intelligence apparatus is its focus on controlling the lsquo;peoplersquo; for the goal of maintaining the power of the Chinese Communist Party with an emphasis on combating the lsquo;three evilsrsquo; of separatism, terrorism, and religious extremists. This focus does seem somewhat disproportionate to that of developed western democracies whose intelligence apparatus are less concerned with controlling the lsquo;peoplersquo; but rather about International Relations (IR), military secrets and defence against both domestic and foreign terrorists.Beyond the lsquo;three evilsrsquo;, China has invested heavily in cyber espionage to aid its economic and military development. An interesting observation is an asymmetrical vulnerability that exists between China and the West. As one of the authors Nigel Inkster aptly phrases it, ldquo;there is much that China wishes to steal from the West but little that the West wants to steal from China, with much of the West needs in the areas of political and military secretsrdquo; (p46).The crux of the charge against from mainstream foreign media and commentators is the proposition that China conducts cyber espionage with the view of commercial gain (unlike its western counterparts), yet the authors offer a compelling assessment and view that these claims are somewhat exaggerated.Their argument is based mainly on the inefficiencies of the intelligence-to-innovation process and the long-term impact that lsquo;baking inrsquo; the reliance of foreign ST intelligence into the innovation system would undermine long-term investment in indigenous research and development and innovation.An area that the authors could have explored deeper was the relationship and use of the lsquo;Chinese hacker undergroundrsquo; as a proxy to obtain key industrial secrets for the state as well as non-state sponsored industrial espionage. The author Nigel Inkster raises the question to what degree does the top leadership have a policy grip on the Chinese intelligence community and their activities, and Irsquo;m of the opinion that historically it has not.While the authors put forward a strong argument that it is not necessarily a policy of the Chinese government to hack for commercial gain, speculation exists in the public domain that much activity is perhaps happening outside of the remit and control of the administration. As a result, of this non-state sanctioned hacking, Chinarsquo;s image continues to be tarnished, further fuelling the foreign media and assessment of Chinarsquo;s cyber espionage activities.Governance of Cyberspace, challenging the US hegemonyThe section on National Cyber Security Policy is influenced heavily by Chinese authors and commentators, which provides a refreshing perspective on the topic. At the top of the agenda is the subtle but clear message that China sees itself as a victim of the US hegemony in cyberspace and looks to counter this by seeking the management of the main Internet services away from strongly influenced and controlled U.S. entities into the broader international community.The complex topic of human rights, internet censorship (or safety as the Chinese leaders phrase it), and the western lead anti-Chinese sentiment is tackled nicely. However, it would be useful to have seen a stronger Chinese flavour to the assessment and ensuing text.Western nations have most certainly politicised the Internet as a fundamental human right and something that should be free and open. Naturally, the Chinese leadership view this is an attack on their communist ideals, and leverage it to incite nationalistic spirit to counter western ideologies and influence. While this book does not specifically mention Chinarsquo;s policy on cyber sovereignty, it certainly discusses various machinations of what the doctrine of cyber sovereignty entails.Internet CensorshipThe different political ideologies between the Chinese and the Western commentators appear to be most pronounced when viewed through the lens of cyber sovereignty and internet censorship. The Chinese writers seldom depart from the partyrsquo;s official rhetoric that without Internet safety (censorship) there can be no national security, which loops back to the section earlier on the Chinarsquo;s intelligence apparatus and their focus on the lsquo;three evilsrsquo; and the protection and preservation of the lsquo;partyrsquo;.Interestingly, research exists that suggests that the Chinese leadership have allowed more online criticism against the party and regional governments in recent years as can yet are still somewhat cautious and focused on social mobilisation. It is somewhat disappointing that the authors did not look to examine how Chinese netizens themselves perceive their relative freedoms on the Internet. Especially how the central government has loosened its control in certain areas and allowed netizens to voice discontent at certain events, for example, the Wenzhou train crash in 2011.Overall, an excellent reference and assessment of Chinarsquo;s activities in cyberspace. That said, several topic areas and lines of enquiry could benefit from further research such as non-state sponsored activities in the field of industrial espionage and what are the likely scenarios and consequences of the political toiling between China and the West in the governance of cyberspace.1 of 1 people found the following review helpful. Five StarsBy sophieLove it, super informative and great collection of articles by various authors with multiple analytical angles.0 of 0 people found the following review helpful. Well Done!By TrogAn exceptionally well reserached and written book on China and cyber security

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.

"This multifaceted book discusses doctrines, motives, purposes, and capabilities of Chinese activities in cyberspace, internal and external. The chapters authored by Chinese writers, including one current member of the People's Liberation Army, are especially illuminating. Particularly striking are their attempts to create new terms to describe this new sphere of geopolitical activity, and their overall optimism over the possibility of international management of cyberspace." ---NICHOLAS Gordan in Asian of Books, Sept 2015.nbsp;From the AuthorChinese cyber espionage is commonly portrayed in the West as a major threat to economic and national security. From China's perspective, the United States poses a major cyber threat to other countries because of its outsized influence over the internet, willingness to use of cyber weapons against its adversaries, and exploitation of major firms like Microsoft and Google for intelligence. Mistrust and confusion have complicated internet politics on both sides of the Pacific. To get beyond the hype, an understanding of China and cybersecurity requires a combination of international and interdisciplinary perspectives. This book brings a balance of technical, political, economic, legal, and strategic analysis by authors from China, the United States, Canada, and the United Kingdom. Even though the contributors to this volume do not always agree with one another--an important point in itself--they reveal underlying political and economic dynamics which will remain relevant even as new facts and opinions emerge in a fast-changing domain. This volume contributes substantively to our understanding of China and cybersecurity, both complex topics on their own, by exploring how China's domestic political and economic system shapes its cyber activities. The collaboration also stands as an example of how Chinese and Western experts can work together to improve trust and understanding in an area of great mutual concern.About the AuthorJon R. Lindsay's research examines the impact of technology on international security and strategy and has been published in leading academic journals such as International Security, Security Studies, Journal of Strategic Studies, and Technology and Culture. He holds a PhD in political science from the Massachusetts Institute of Technology and an MS in computer science and BS in symbolic systems from Stanford University. He is an officer in the U.S. naval reserve with seventeen years of experience including assignments in Asia, Europe, Latin America, and the Middle East. Tai Ming Cheung, director of the University of California Institute on Global Conflict and Cooperation, is a long-time analyst of Chinese and East Asian defense and national security affairs with particular expertise on the political economy of science, technology, and innovation and their impact on national security matters. Dr. Cheung was based in Asia from the mid-1980s to 2002 covering political, economic and strategic developments in greater China. He was also a journalist and political and business risk consultant in northeast Asia. Dr. Cheung received his PhD from the War Studies Department at King's College, London University.Derek S. Reveron is a professor of national security affairs and the EMC Informationist Chair at the U.S. Naval War College. He specializes in strategy development, non-state security challenges, and U.S. defense policy. He has published nine books including U.S. Foreign Policy and Defense Strategy: The Evolution of an Incidental Superpower (2015), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World (2012) and Human Security in a Borderless World (2011). He received a a PhD in public policy analysis from the University of Illinois at Chicago.