Nigel Inkster, ***China's Cyber Power***, Routledge, 2016

Publishing a book on hot-button issues such as the *China's Cyber Power* is challenging. There has been so much published on the subject of cyber security, although complex China's cyber security analysis has random been published. Therefore, the chance for a book to be visible and have a significant impact is high. Published in the mid 2016 *China's Cyber Power* by Nigel Inkster at least reveals itself to be a serious project which covers a wide range of issues related to cyber security, including China's global engagement.

The book is divided into four chapters. The first chapter *Evolution of the Chinese Internet: Freedom and Control*, provides a useful overview of the development of internal sources of information and communication technologies (ICT). This includes economic factors, sources of technological innovation, information control, and rule of law. The author provides the roots of Chinese economic and science development, that lead to grow of ICT. The second chapter, *Cyber Espionage* examines intelligence as Chinese foreign policy and strategy tools. The chapter includes brief overview of China's intelligence structures, intelligence tradecraft, the role of public administration on intelligence, Chinese cyber capabilities and global intelligence power. The third chapter, *Military Cyber Capabilities* focuses on cyber domain in Chinese military development. This refers Chinese military traditions, political attitudes and objectives of People's Liberation Army (PLA), and technological development of military capabilities in cyber area. The last chapter *Battle for the Soul of the Internet* analyses cyber policy as domestic policy objective. The chapter includes agenda such as cyber governance and cyber security in a long term strategic context.

The *China's Cyber Power* by Nigel Inkster offers a timely and useful analysis of different aspects and issues related to Chinese cyber security, including historical context. Selected chapters, such as *Evolution of the Chinese Internet: Freedom and Control* and *Battle for the*

Soul of the Internet are particularly useful for a wider audience, whether for the experts, researchers as well as students. Other chapters are particularly addressed to professionals that are interests in Chinese foreign policy and Chinese military capabilities.

Nigel Inkster argued that the cyber domain is an increasingly critical factor in the country's pursuit of strength through modernisation, and protection from perceived threats, whether internal or external. Beijing sees cyberspace as crucial to the next phase of economic development, not only for realising the potential of the digital economy but also for developing the next generation of technologies, which will provide employment opportunities in the place of an industrial era manufacturing sector progressively less able to do so. The author find that Chinese leadership sees the cyber domain as having significant capacity to facilitate both governance and social control. The attitudes of Chinese Communist Party (CCP) to monitoring and managing internet content, particularly exchanges on social media, and the leadership appears to spent huge resources. N. Inkster indicated that the Party's propagandists and ideologues maybe developing a vision for the Chinese cyber domain that enables it to exercise control over citizens by both filtering the information they access and compiling such detailed electronic data on individuals, including their entire browsing history and all their social-media posts. The leadership has an equally strong apprehension of the vulnerabilities arising from dependence on systems that have been developed and operated by Western corporations, largely in accordance with Western rules and values. This perception of vulnerability has sparked efforts to reduce China's dependence on Western technologies and networks. As N. Inkster argued the Cyberspace Administration of China has repeatedly said that foreign companies aspiring to work in the country will have to accept Chinese rules, including those on monitoring and filtering online content.

N. Inkster in his book argued that cyber policy lies at the heart of China's domestic- reform agenda, and has it begun to influence fundamentally the state's approach to foreign policy and international security. In the 21st century, an awareness of the risks posed by the cyber domain has deepened an ingrained sense of Chinese insecurity. In the author' opinion the cyber domain has become the principal vector not only for the country's economic power, growing military capacity and stability, but also for the importance of securing a global cyber environment that facilitates their domestic agenda and minimises external threats. N. Inkster argued that global cyber governance and cyber security have become key battlegrounds for China. The adoption of a much more strident and assertive foreign policy, leading to suggestions that the era of 'hide and bide' is coming to an end, and facilitate China position on the international rules for the cyber security. International organisations and fora of discussion are dominated by China and its proponents such as Russia, Belarus, Malaysia, Pakistan, Egypt and many G77 countries. They have been important components of the multi-stakeholder system and successfully advocate that countries with different social systems and cultural traditions would handle the transition to the information society differently and that the security of the state would be a high priority.

As N. Inkster find, cyber power and cyber war can be viewed as the most recent phase in the ongoing revolution in international relations and military affairs. However, N. Inkster does not define the meaning of cyber power. In the most general sense, power may refer to any kind of influence exercised by objects, individuals, or groups upon each other. These broad and deceptively simple definition represents a grave dilution of the concept. Consequently, the meaning of cyber power shall be provided. In the other words, the question what are the cyber power like, should be addressed. The second weakness of the assumption by N. Inkster is absence of broader context of the international aspects of the Chinese cyber status, including existing distribution of power in Asia and Pacific. To wave the first chapter, an introduction to the understanding of Chinese cyber domain, the second chapter *Cyber Espionage* shall deeply focus on the international echoes of the activity of Chinese intelligent in cyber area. The author provides an interesting overview of the intelligence in the *Chinese policy and strategy*, however there are few examples of possible Chinese' intelligence operations, and cyber espionage linked with China. In subsection *Global intelligence power*, that is dedicated to Chinese cyber activities by intelligence structures, the author focuses in a narrow way to the problem of its global context. Past, current, and future data are vulnerable to spies and eavesdroppers in unprecedented ways. This, raises several questions that N. Inkster does not examine such as: will cyber espionage be more likely to cause conflict than traditional spying has done, what can states do to gain the benefits of intelligence collection, and how cyberspace capabilities and operations pose new policy dilemmas?

In spite of these lacunae, the book offers an interesting assumption of China's cyber power and is a valuable reference for academics and practitioners. It is difficult to dispute N. Inkster' conclusion that China appears to believe that it can have its cake and eat it: gaining the economic benefits that come with global connectivity while excluding information seen as detrimental to political and social stability.

Robert Śnitko

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Humanistyczny