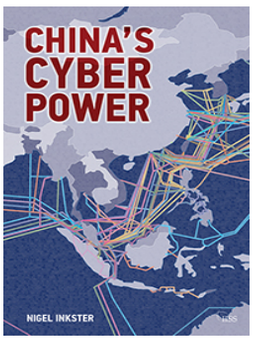

Adelphi Series

ISSN: 1944-5571 (Print) 1944-558X (Online) Journal homepage: https://www.tandfonline.com/loi/tadl20

Introduction

Nigel Inkster

To cite this article: Nigel Inkster (2015) Introduction, Adelphi Series, 55:456, 7-18, DOI: 10.1080/19445571.2015.1181439

To link to this article: https://doi.org/10.1080/19445571.2015.1181439

INTRODUCTION

To mark the first meeting of the NETmundial Initiative's Coordination Council, held in São Paolo on 30 June 2015, China Military Online published an editorial observing that:

> Global internet governance can no longer dispense with China. 2014 was the twentieth anniversary of China's accession to the internet … and, by the end of 2014, China had 649 million users, representing one-fifth of global Netizens. This huge number means that no country in the world can afford to belittle the power of China's internet any longer. Moreover, in line with China's continuing rapid economic development, China's internet industries have developed to the point of being comprehensive, diversified, in-depth and international. Measured by market value, four of the world's top ten internet companies are Chinese … and the vertiginous speed with which China's internet industries have developed now means that China has become a mainstay of the global internet industry.

The piece went on to state that China's voice would have to be heard on issues of global internet governance, and that the country's policies on the area, as articulated by President Xi Jinping, were attracting growing international support.[1]

The NETmundial event primarily brought together representatives of government, civil society and academia from various parts of the world, aiming to encourage discussions on internet governance and to promote the cyber principles purportedly shared by its attendees. However, the initiative was controversial, having grown out of the Brazilian government's reaction to revelations by rogue National Security Agency contractor Edward Snowden about US electronic espionage around the globe, particularly the alleged monitoring of Brazilian President Dilma Rousseff. The Coordination Council included few representatives from the private sector.[2] But, tellingly, China enthusiastically participated in the event, and the NETmundial Initiative enjoyed the support of both the World Economic Forum and the Internet Corporation for Assigned Names and Numbers. The latter creates and controls what is in effect the address book for the internet, and until March 2016 operated under the aegis of the US Department of Commerce.

The Netmundial forum is just one of a growing number that call into question the status quo of an internet that was built almost exclusively by US corporations, and that has from the outset reflected and espoused Western liberal values. The pioneers of the World Wide Web and the internet, people such as Vint Cerf and Tim Berners-Lee, were motivated by a sense of idealism, believing that the medium would enable citizens around the world to communicate freely, and to exchange knowledge and ideas in ways that benefited all of humanity. This vision has to a significant degree been realised. Global communications have been transformed, and knowledge – a commodity that once was scarce and expensive, and that

conferred great power on those able to acquire it – has become cheap, ubiquitous and potentially democratising. However, the internet has also proven to have a dark side, empowering a wide range of malign actors who are no longer constrained by geography, and thereby transforming the global threat landscape.

At the same time, many countries have seen the concept of a global information flow that operated largely outside their control as a challenge to their authority and legitimacy. China and other authoritarian states, especially the Russia of Vladimir Putin, have long been concerned about the security implications of their reliance on information networks almost entirely under the control of the United States and its allies. As early as 1998, Russia introduced a resolution into the UN First Committee on 'Developments in the Field of Information and Telecommunications in the Context of Security'.[3] The resolution was essentially designed to ensure that the issue of cyber security would be addressed in the context of arms control and to emphasise the need for 'information security', the concept that national governments had a right to control content within their sovereign internet spheres. For while the internet purported to be – and in many ways was – borderless, it rapidly became apparent that states could exercise a significant degree of sovereign control through the medium, either by monitoring and filtering content themselves or by demanding that internet service providers and other technology companies did so as a condition of their operating licences.

Global discussions on both internet governance and cyber security have seen the world effectively divide into two camps. One comprises the US and other, predominantly Western, liberal democracies – a group sometimes referred to as the 'like-minded'. They advocate the multi-stakeholder model of internet governance, in which a complex and constantly

evolving network of individuals and interest groups come together to address a range of issues. This approach produced the Internet Engineering Task Force, a non-profit group whose membership is open to anyone with the requisite technical qualifications and whose purpose is 'to make the internet work better by providing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.[4] The US and its allies also espouse an open internet that is in principle free of government restrictions on content, while arguing for a focus on network security – to ensure that the internet can function in a reliable, hygienic manner.

The second camp comprises authoritarian states led by Russia and China. While not explicitly dismissing the multi-stakeholder concept, they advocate a much stronger role for national governments in internet governance, particularly in relation to matters of public policy. Their focus on information security is based on the Soviet-era concept of information warfare, in which a state secures its information space to ensure that its narrative goes unchallenged. This group would like to formalise global internet-governance structures within the UN, in a top-down model that gives a decisive role to national governments. The approach tends to play well with the states of the developing world, which have a digital disadvantage and are vulnerable to the powerful, destabilising forces of globalisation for which the internet has become a prime vector. It is in these states that the next wave of internet expansion will take place, mainly through mobile devices. China increasingly provides both the network infrastructure and hardware enabling this expansion.

The country's erstwhile reticence on global internet governance reflected its relatively late adoption of the internet and initial dependence on US information-technology companies to build its capabilities. China's stance was also a function of its

long-term strategy of keeping a low profile on foreign policy, which had been subordinated to the pursuit of economic development under Deng Xiaoping's 1979 policy of reform and opening up. Following the crackdown in Tiananmen Square on 4 June 1989, China came close to becoming an international pariah, prompting Deng to develop his '24-character strategy', referred to by the Western media as 'hide and bide'.[5] In the wake of the 1996 Taiwan Strait Crisis, which led to the deployment of two US carrier battle groups near China, this strategy was supplemented by Vice-Premier Qian Qichen's dictum that economic development should take precedence over reunification with Taiwan, and that cooperation with Washington should take precedence over confrontation.

It occurred to few Western policymakers and scholars to reflect on what kind of light China hid under a bushel – or the direction in which that light might ultimately be turned. There was a widespread tendency to underestimate the country's potential or to assume that, as it developed economically and a new middle class emerged, political reform towards a Western democratic model would ineluctably follow. Beijing itself did much to contribute to this perception by promoting the concept of *zhongguo heping jueqi* (China's peaceful rise). First espoused by former Central Party School Vice-President Zheng Bijian at the 2003 Boao Conference, the concept held that China's transition to great-power status could be achieved without the disruption and violence that had accompanied the rise of other states.[6] The idea was reinforced in a documentary series produced by China Central Television entitled *The Rise of Great Powers*.

However, the emerging reality suggests that China may now be embarking on a very different course, raising questions in the minds of many in the Western policy community about the country's potential to disrupt the established global order. Henry Kissinger, architect of Sino-American rapprochement

in the 1970s, observed in 2012 that 'enough material exists in China's quasi-official press and research institutes to lend some support to the theory that relations [between Washington and Beijing] are heading for confrontation rather than cooperation'.[7] Since the onset of the 2008 global financial crisis, which confirmed for China's leaders that the Washington Consensus had collapsed, Beijing has become more inclined to challenge if not the validity of post-war international institutions then at least the West's perceived domination of these institutions.

President Xi's promotion of the 'Chinese Dream' – which began in 2012, following his accession to the presidency, and to the far more important chairmanship of the Chinese Communist Party – marks a shift away from 'hide and bide' and towards a reassertion of China's historical standing as a major power (even though the term has been couched in language that defies clear interpretation).[8] Beijing's unrequited desire for a 'new kind of great power relationship' with Washington is another indication of this pursuit of greater respect and recognition. China has been increasingly open about its wish to redesign the post-war global architecture to give emerging states greater influence. Meanwhile, a narrative holding that the US is, and always has been, intrinsically hostile towards China and seeks to subvert or overthrow the Communist Party – a message that has always resonated with an inherently paranoid Leninist leadership – has been articulated ever more frequently in China's official and semi-official mass media, particularly with reference to the internet as a potential mechanism for Western subversion.[9]

Some Western analysts have interpreted the new, more assertive China as the product of a decades-long strategy to replace the US as the leading global power by 2049, the hundredth anniversary of the People's Republic. In this view, the ground for China's rise has been prepared through decep-

tion and concealment designed to lull the West into a false sense of security.[10] Irrespective of whether China has such a strategy, the country has acquired a global network of interests that it has the means to promote and protect, and thus will be a powerful force for change in the twenty-first century. This is a force that Western policymakers, lacking any knowledge of China's language, culture or history, will struggle to understand or accommodate.

The effects of this shift are already manifest in the cyber domain. What was a relatively benign domain for US information-technology companies when China was racing to catch up with Western nations is beginning to give way to a more restrictive environment. As Beijing introduces new legislation on counter-terrorism, national security and cyber security, these firms are increasingly required to provide the government with source codes and to store Chinese data in China. Efforts are also under way to encourage the indigenisation of information and communications technologies (ICTs) in strategically important areas, such as the banking sector.[11] And while China's social-media scene remains relatively lively, the government has progressively constrained the behaviour of prominent bloggers, and there has been a shift away from Sina Weibo, the Chinese equivalent of Twitter, and towards WeChat, a peer-to-peer system that limits the potential for online issues to go viral.[12] In the debate between openness and security that has been at the heart of China's adoption of ICTs, security now appears to be the dominant preoccupation. Beijing's initially piecemeal, reactive approach to managing the internet has become more proactive and systematic, due to the perception that this is key to continuing China's economic and technical progress, as well as to an awareness of the ways in which the mass aggregation of data can potentially enhance political and social control.[13]

Since the First Gulf War, China's military has seized on the implications of modern ICTs for war fighting, particularly in terms of information warfare. China's official position is that the internet should be used only for peaceful purposes, and that the development and use of cyber weapons should be banned. But the People's Liberation Army has formulated an ambitious strategy for fighting 'local wars under informationised conditions', under which cyber capabilities have become a key component of all military exercises.[14] Much has been written by Chinese and Western scholars on the ways in which China might use cyber capabilities for military purposes, including both deterrence and pre-emption, although there is little in official Chinese doctrine that offers clear guidance on how, and in what circumstances, such capabilities should be deployed.

The area of cyber activity for which China is best known, and somewhat notorious, is espionage. Claims that the Chinese state has sanctioned systematic, broad-spectrum industrial espionage targeting US and other Western corporations are heard almost daily, and as a result are no longer considered newsworthy. Combined with Snowden's revelations regarding China, such claims have significantly contributed to a growing climate of mistrust between Washington and Beijing – to the point that they have become an issue in the campaign for the 2016 US presidential elections.[15] And the methodical nature of such attacks has prompted suggestions that China is engaged in economic warfare against the US, although there is little evidence for this contention.[16]

In contrast, China's potential to shape the future of the internet at a global level has attracted little attention from the West's top policymakers. And this issue may in the long term be more significant than state-sponsored cyber commercial espionage in managing China's rise. As part of the country's strategic shift towards greater assertiveness in global cyber negotia-

tions, Lu Wei, head of the Cyberspace Administration of China and an accomplished propagandist, used the World Economic Forum's summer 2014 meeting in Davos as an opportunity to state clearly Beijing's intent to shape internet governance. He reiterated this position at the World Internet Conference held in Wuzhen the following October.[17] Since then, China has patiently implemented a strategy of making slow, steady gains in multiple fora, creating facts on the ground in support of its agenda and making little secret of its aim to erode the US advantage in the cyber domain.

The components of this strategy can be characterised as: harness the country's user community, the largest in the world, as a throw-weight in demanding that foreign businesses operating in China comply with Chinese restrictions and technical criteria; build and support Chinese technology firms such as Huawei, ZTE and Alibaba; construct and operate information networks in the developing world; create cyber-security partnerships such as that established in early 2015 with Russia; champion within the UN the International Code of Conduct for Information Security, in cooperation with Russia, Tajikistan and Uzbekistan; promote Chinese concepts of global cyber governance and cyber security in multiple international fora; advocate the concepts of cyber sovereignty and information security, in an effort to outlaw the kind of covert cyber intrusions in which the US has a significant advantage; maximise Washington's discomfiture following revelations about covert US cyber capabilities, such as those made by Snowden; and develop a domestic legal regime with an extraterritorial element, so that critics based outside Beijing's jurisdiction can be more easily pursued and silenced.

It remains to be seen whether China will succeed in promoting its agenda, and what the implications of such success could be. But Beijing's achievement of any of its main aims would

change both the way in which the internet functions and the way in which states exercise power within that medium. The US and its allies, particularly those within the Five Eyes intelligence alliance (Australia, Canada, New Zealand and the United Kingdom), have until now enjoyed a significant first-mover advantage in their ability to use cyber capabilities in the interests of national security and national advantage. That advantage, though still considerable, is starting to erode quite rapidly. Much of it derives from the ability of the US and the UK to access the major fibre-optic cable networks that carry a significant proportion of global internet traffic, and to benefit from cooperation with major US technology corporations – cooperation that has notably diminished since the Snowden revelations. Meanwhile, the developing world is increasingly wired by China, almost certainly in circumstances that will give the country's intelligence community access to the information transiting those networks. And China will continue to exploit its position as the world's leading manufacturer of ICT equipment to shape global engineering and design standards, and to market its indigenous systems. It is far from unimaginable that China will create a cyber Sinosphere – in effect, a globalised version of something that already exists – that has significant normative influence on global cyber security and governance. The impact of such a development is hard to determine, but, if it were to lead to the establishment of parallel internets or border controls online, the strategic and security implications would likely be profound.

For a Western world that set the framework of the post-war global order and became accustomed to running the show, managing the emergence of China as a major global power was always going to be the greatest strategic challenge of the first half of the twenty-first century. The cyber domain has been a powerful enabler of China's rise, and will be a critical avenue

through which the country's emerging power is expressed and exercised. It is impossible to predict the form that this exercise of power will ultimately take, although it is by no means inevitable that China's influence will be malign. Indeed, the emergence of a China that is self-confident, secure and willing to invest in the preservation and policing of the global commons could prove to be a force for good. Thus, it will be increasingly crucial for Western policymakers to have a clear, realistic understanding of China's cyber power, as well as of the effects of this power on both China's and the West's global interests. This book examines China's evolving cyber domain and online culture, alleged large-scale cyber espionage, cyber capabilities in the military and 'hard security' domains, and international cyber policies and strategies, before offering some reflections on how these important new phenomena can be managed and accommodated.

Notes

1 'Quanqiu hulianwang zhili xiankai xin pianzhang, zhongguo cheng zhudao liliang zhi yi', China Military Online, 2 July 2015, http://www.81.cn/jwgz/2015-07/02/content_6565967.htm.

2 Kieren McCarthy, 'Internet Governance Group Pushes on without, er, Internet Organisations', *Register*, 24 December 2014, http://www.theregister.co.uk/2014/12/24/internet_governance_group_pushes_forward_without_internet_organizations/.

3 Tim Maurer, 'Cyber Norm Emergence at the United Nations – An Analysis of Activities at the UN Regarding Cyber-Security', Belfer Center for Science and International Affairs, September 2011, p. 21, http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

4 Internet Engineering Task Force, 'Mission Statement', https://www.ietf.org/about/mission.html.

5 The most comprehensive version of this strategy is as follows: observe dispassionately; secure our position; deal calmly with events; conceal our capacities and bide our time; cultivate a low profile; never take a leadership role (冷静观察；站稳脚跟；沉着应付；韬光养晦； 善于守拙；绝不当头). Deng Xiaoping, *Collected Works*, vol. 3 (Beijing: People's Publishing House, 1993).

6 Zheng Bijian, 'China's "Peaceful Rise" to Great-Power Status', *Foreign Affairs*, vol. 84, no. 5, September–October 2005.

7 Henry A. Kissinger, 'The Future of US–Chinese Relations', *Foreign Affairs*, vol. 91, no. 2, March–April 2012, pp. 44–5.

8 'What Does Xi Jinping's China Dream Mean?', BBC, 6 June 2013, http://www.bbc.co.uk/news/world-asia-china-22726375.

9 See Wu Zhenghua, 'Jue buneng rang hulianwang chengwei renxin liushidi', *People's Liberation Daily*, 13 May 2015, http://jz.chinamil.com.cn/gd/2015-05/13/content_6488193.htm.

10 See Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2015).

11 'China Said to Plan Sweeping Shift from Foreign Technology to Own', Bloomberg, 17 December 2014, http://www.bloomberg.com/news/articles/2014-12-17/china-said-to-plan-sweeping-shift-from-foreign-technology-to-own.

12 'Has China Silenced Its Bloggers?', BBC, 12 July 2015, http://www.bbc.co.uk/news/blogs-trending-33464788.

13 Rogier Creemers, 'Internet Plus: Technology at the Centre of Chinese Politics', in European Council on Foreign Relations, *China Analysis*, July 2015, http://www.ecfr.eu/page/-/CA_1507_Governing_the_Web.pdf.

14 Anthony H. Cordesman, *Chinese Strategy and Military Power in 2014: Chinese, Japanese, Korean, Taiwanese and US Perspectives* (Washington DC: Center for Strategic and International Studies, 2014), pp. 121–3.

15 'Hillary Clinton Accuses China of "Stealing US Secrets"', BBC, 5 July 2015, http://www.bbc.co.uk/news/world-us-canada-33399711.

16 James A. Lewis and Simon Hansen, 'China's Cyberpower: International and Domestic Priorities', Australian Strategic Policy Institute, November 2014, pp. 2–4, https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf.

17 David Bandurski, 'Lu Wei: The Internet Must Have Brakes', China Media Project, 11 September 2014, http://cmp.hku.hk/2014/09/11/36011/.