KING'S College LONDON

Mapping and Evaluating China's Cyber Power

Greg Austin

Lau China Institute *Policy Paper Series*

Series Editor: Dr Sam Beatson

Editor's Introduction

China is portrayed by the media as potentially threatening through state and army links to industry and investments and resultant security risk investigations by recipient governments. The Hinkley Point development programme worth £18 billion ($23.7 billion USD) in its construction and offering potentially 25,000 jobs over the lifetime of the power station has been stalled by ministerial intervention at the highest level in the UK after MI5 raised concerns, according to the prime minister Theresa May's chief of staff[1]. Moreover, telecoms provider Huawei has been under investigations ordered by the UK head of national security concerning its cyber security centre operations based in Banbury. Although cleared of wrongdoing in 2013, the Huawei Cyber Security Evaluation Centre (HCSEC) continues to require an oversight board consisting of senior UK government and telecoms sector representatives in addition to Huawei executives in order to keep the government informed and mitigate risks[2]. Australia upheld its ban on Huawei bidding on broadband projects in 2013 and on 11 August, 2016, Australia blocked the acquisition of Ausgrid electricity infrastructure company by Chinese investors citing a classified security rationale[3]. The US has a Committee on Foreign Investment in the United States (CFIUS) to investigate foreign investment and thus certain Chinese projects require its stamp of approval and the US has discouraged doing business with China in sectors such as Huawei's. Cyber power and security are the watchwords.

However, China has its own domestic challenges in developing itself along cyber power lines, both in terms of ownership and control of the technology, which may be foreign, and competing with other countries who have made their own leaps in innovation and technological progress, both in industry and informatisation of administrative functions. This paper focuses on deepening our understanding of China's cyber power.

Professor Greg Austin is a world leading authority on national security and cyber power who has consulted for the UK and the Australian governments. His paper presents evidence of China's cyber power ambitions and argues that research to date has neglected the dynamics of China's cyber power in favour of a sort of 'cyber power assets accumulated' approach. The paper contends that China wishes to indigenise its cyber power capabilities, including taking back control of informatisation resources from foreign powers. However, due to a self-admitted weakness in science and technology, China faces challenges in keeping apace with other countries in cyber power terms. It is argued that China requires either to make (e.g. innovate), take (e.g. adopt), spoil (e.g. disrupt) or acquiesce (e.g. co-operate) in cyber power development. The author goes on to suggest for the first time a preliminary framework for understanding China's cyber power in depth from these perspectives.

Dr Sam Beatson
sam.beatson@kcl.ac.uk

Room 340N
Lau China Institute
King's College London
Strand,
London,
WC2R 2LS

[1] Swinford, S. & Gosden, E., 2016. Theresa May delays Hinkley nuclear decision amid concerns over Chinese involvement [Online] Available at: http://www.telegraph.co.uk/business/2016/07/29/theresa-may-delays-hinkley-nuclear-decision-amid-concerns-over-c/ [Accessed 06 09 2016]
[2] HCSEC Oversight Board, 2016. Second Annual Report. [Online] Available at: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2016 [Accessed 06 09 2016]
[3] Beatson, S., 2016. Mainland firms can exploit HK's advantages for overseas acquisitions [Online] Available at: http://www.chinadailyasia.com/opinion/2016-08/23/content_15483757.html [Accessed 06 09 2016]

This Page is Intentionally Blank

Mapping and Evaluating China's Cyber Power

Professor Greg Austin
Professor at the Australian Centre for Cyber Security
University of New South Wales

Published online on 8 September, 2016 as part of the Lau China Institute *Policy Paper Series*

Abstract

In February 2014, President Xi Jinping declared his intent to do everything necessary for China to become a cyber power. In July 2016, the government clarified its ambitions in a set of new strategy documents, adding not just a timeline but also a decidedly combative tone to the aspirations. Both announcements, backed up with substantial administrative and policy reforms, reflect deep and entrenched dissatisfaction within the leadership over the pace of accumulation by China of the attributes of power in cyber space. These attributes include such goals as having a globally dominant information and communications technology (ICT) sector, leadership in the science of ICTs, and building first class military capability for cyber-enabled war. But beyond a focus on such foundations of power, there is little consistent articulation by Chinese leaders of just how the country can and should exercise cyber power in the process of accumulating the attributes. They appear to have conflicted views on the relationship between the attributes of cyber power and the exercise of it in dynamic contexts. This field of inquiry is an undeveloped area in China studies. Relying on political science we propose an initial and provisional template for mapping the dynamic aspect of China's exercise of cyber power. The mapping leads us in the direction of three conclusions though these are not developed at length in this paper: (a) China is more likely to be a spoiler in cyber space rather than a dominating or dominant power; (b) that said, the collaborative aspects of the exercise of cyber power by China are likely to outweigh its spoiler effects; and (c) the country's approach to a nationally-framed concept of cyber power is probably self-defeating.

Introduction

In February 2014, President Xi Jinping declared his intent to do everything necessary for China to become a cyber power (Xinhua, 2014). The announcement, backed up by administrative reforms[1], reflected deep dissatisfaction within the leadership in respect of the pace of innovation in the country in the civilian economy field. Xi was also forced to act because of rising concerns about United States cyber military and espionage activities, in part revealed by Edward Snowden in June 2013 but in larger part revealed by increasing efforts by the United States to develop its cyber military power. This concern was evidenced by a change in the title of China's leading policy group at that time to include cyber security as well as informatisation[2]. The cyber power decision revealed in February 2014 had been made behind closed doors in December 2013.

Since then, the government and Chinese Communist Party (CCP) have been hyperactive on many related fronts: political, legal, economic, military, organizational and diplomatic. By September 2016, with almost three years gone since Xi and his fellow leaders agreed on the new cyber ambition, they are still not satisfied. They announced new and detailed plan in line with their five-year plan process, and set a seemingly more robust ambition: becoming a 'stronghold' of cyber power (Zhang, 2016), using language that interpreted in the *South China Morning Post* as the ambition to become a 'cyber superpower' (Zuo, 2016).

Chinese leaders are not always clear on what the term 'cyber power' might mean. At times, they emphasise the foundational aspects: the economic, scientific, technical or military resources they command in cyber space. At other times, they focus on the dynamic aspects: how well does China perform in its efforts to persuade or force other actors to do its bidding in cyber space or on cyber space policy issues? The balance between the two (resources versus the exercise of power) in leadership statements reveals a preference for concentrating on power resources to the neglect of power dynamics in cyber space or on cyber space issues. Scholarly attention to this subject has for the most part followed that preference, thereby privileging the foundations of power to the relative neglect of the dynamics of China's exercise of cyber power.

Relying on political science, this paper proposes an initial template for mapping the dynamic aspect of China's use of cyber power. The first part looks briefly at how China's leaders in mid-2016 are assessing their current progress toward accumulating the resources or foundations of cyber power. The second and main part of the article looks at how successful China can be in its exercise of cyber power by outlining in sequence: the country's policy practices in the recent past (its use of cyber power); political science approaches to power and their adaptation for the information age; and finally how we can begin to apply key conclusions from political science to the case of mapping China's exercise of cyber power. The terrain is not fully-mapped. Rather, this paper provides a provisional template for analysis, paving the way for a more comprehensive evaluation.

[1] At this time, China announced that Xi had added to his portfolio of leadership roles that of Chair of the country's Leading Group on Informatisation. The group has been in existence since 1996, and progressively upgraded, but never previously headed by a General Secretary of the CCP.

[2] 'Informatisation' is not such a common term in English, but as used in China it means application of advanced information and communications technology to all walks of life (political, economic and military). Within the economy, it extends well beyond IT products (such as computers or smart phones) to include the application of information systems in sectors as diverse as health, agriculture, environment and taxation.

Foundations of Cyber Power

The Xi announcement of the cyber power ambition in February 2014 signified recognition that China was still lagging in cyber power and not catching up as quickly as the leaders wanted (Austin, 2014). The new ambition has seen many implementing measures since then. For example, in September 2014, Xi told the country it needed a new cyber military strategy. In December 2014, the government introduced new regulations for cyber security intended to help promote the rapid growth of China's domestic cyber security industry. In May 2015, the country issued a new Military Strategy in which the government declared for the first time in such a document the idea that cyber space along with outer space have 'become new commanding heights in strategic competition among all parties' (Xinhua, 2015). The same month, the National People's Congress released a draft bill on National Security (passed in July) that gave a special place to cyber security in its provisions for strengthening government control over foreign technologies and related investment in China. Also in July 2015, China released a draft law on network security with sweeping new provisions on control of foreign technologies and data management. The same year, the Chinese armed forces set up a new Strategic Support Force to begin to maximise its advance in practical applications of military cyber capability.

In May 2016, Xi said that science and technology (S&T) is the bedrock of the country's power and that 'Great scientific and technological capacity is a must for China to be strong' (Xinhua, 2016a). In June, he characterised China's current status in S&T (not just information-related fields) as weak: 'The situation that our country is under others' control in core technologies of key fields has not changed fundamentally, and the country's S&T foundation remains weak' (Xinhua, 2016b). Also in 2016, he publicly endorsed a formula for what the transition to 2050 looks like. China should aim to become one of the most innovative countries by 2020 and a leading innovator by 2030 before realising the objective of becoming a world-leading S&T power by the centenary anniversary of the founding of the People's Republic of China (PRC) in 2049 (Xinhua, 2016c). Xi made more general invocations in connection with the April 2016 meeting of the Leading Group on Informatisation and Cyber Security.

Soon after, when the World Economic Forum published its annual 'Network Readiness Index' comparing the cyber capability of 143 countries, China was sitting in 59th place, down from 36th in 2011; and lower than countries like Montenegro, Mauritius and Turkey (World Economic Forum, 2016). China's position arises in part because of the per capita comparisons in the index which distort the relative wealth and technological capabilities of countries. China has, of course, made great strides, but the United States, Japan, Korea, Singapore and Europe have raced ahead as well. As noted in the World Bank and State Council Research Development Centre (2013) jointly produced report *China 2030*, 'innovation at the technology frontier is quite different in nature from simply catching up technologically' (p. 17).

In July 2016, the government translated these general ambitions for S&T announced by Xi in June into specific cyber power goals for China:

> 2020: 'key technologies achieve an advanced international level, the competitiveness of information industry upgrades significantly on a global scale, and informatisation becomes the leading force of modernization'
>
> 2025: 'establish an internationally advanced mobile communication network … and rid the country of its dependence on foreign key technologies'; aim for 'well-developed advanced technologies industries, leading applications and infallible cyber security; with major transnational internet information enterprises and competitiveness taking shape'
>
> 2050: 'informatisation will play a pivotal role in establishing a prosperous, democratic, civilized and harmonious modern socialist country'; be a cyber power and a 'leader in the development of informatisation around the globe'
>
> Zhang (2016)

The government also released six sets of policy guidance that had been in preparation since 2014 on the following broad subjects:

> 1. 'Coordinated promotion of IT technologies in central and local governments, and between the Party, government and military…. coordinating the roles of the market and government, focusing on interim and long-term targets, and major issues of informatisation in various fields'
> 2. Development of core technologies
> 3. Boosting informatisation 'in economics, politics, culture, society, and also mentions ecology, national defence and the military'
> 4. Building a people-oriented approach to implementation of the strategy
> 5. Highlighting the role of informatisation in international affairs and strengthening China's influence on the global cyber stage
> 6. Ensuring national cyber security.
>
> Ibid.

For the current leaders, one of the primary goals of policy is to rid China of foreign control over core technologies. They see the major pathway to this goal as the rapid consolidation of the domestic ICT sector and its projection on the global stage. They are also very anxious to overcome their technological inferiority through greater indigenization of cyber-related industries, even if this strategy runs up against world trade norms as many governments and corporate leaders have argued.

China's Exercise of Cyber Power

At the same time, the vision is not simply a technocratic one. Chinese leaders have become more fearful of what they call 'hostile Western influences' and they have become more aggressive since Xi came to office in acting against such influences. In fact, one can see the cyber power announcement as likely to be most important to Chinese leaders in terms of their intent to tighten their grip on internal security (Yuen, 2015). The vision of cyber power appears to be one that prioritises consolidation of the attributes of cyber power and the application of such power to keep the CCP in power. The over-arching vision therefore has techno-nationalist and authoritarian dimensions.

In December 2015, Xi spelled out China's situation in broad terms, making it clear that the country faced major challenges affecting state sovereignty and national security in cyber space affairs. These included 'unbalanced development, inadequate rules and inequitable order… infringements of individual privacy and intellectual property rights as well as cyber crimes… cyber surveillance, cyber attack and cyber terrorism' (Ministry of Foreign Affairs of the PRC, 2015). In other words, China's power was being contested or challenged in cyber space and its power was not up to meeting the challenges to the extent that the leadership wanted.

Between late 2013 and today, China has taken a number of steps to rectify this situation. On the international stage, for example, the Wuzhen conference series, which commenced in late 2014, is one major manifestation of China's goal of increasing its power over the international environment. Other initiatives by China since February 2014 in norm development and global cyber space affairs, including an agreement with the United States not to engage in state-sponsored commercial espionage, are a very clear demonstration of how Xi understands the 'cyber power' ambition. The character of this activity is simultaneously intended to promote China's power position but also protect its deteriorating position in the face of intense competition and pressure from other cyber powers. It is this dimension of the cyber power ambition—how does and how will China exercise cyber power and how far will it be subject to the cyber power of others—that is main subject of this paper.

We might assess many of the developments in the recent past as ominous and presaging some sort of confrontation between China, with its increasing intent to exercise cyber power, and the West, with its cyber power imagined to be either static or in relative decline. However, this reading would not represent the totality of the Chinese leadership's position on the balance to be struck between China's aspirations for sovereign capabilities and a globalised cyber industrial complex.

On the one hand, even a superficial reading of new Chinese laws and draft bills impacting on cyber policy reveals unusual and positive attention given to the importance of international economic relations. Chinese leaders know, as leading specialists in China and elsewhere recognise, that the country's cyber sector will remain highly dependent on foreign technology transfer and investment from the most advanced countries for many years, probably decades.

On the other hand, in spite of reports of a blacklist of US-based companies that have been named publicly by Edward Snowden as participating in cyber espionage against China (Pasick, 2015), it continues to solicit and accept massive investments from them. For example, in June 2015, Cisco's incoming CEO, Chuck Robbins, announced in a visit to China that the company would invest USD $10 billion in China (Cisco - The Network, 2015), a move widely seen as an effort to rebuild trust with China.

China's formal position is that the foundations or attributes of its own cyber power can only be built through international collaboration, not just with the sixty or so like-minded countries, such as Russia, who support Chinese positions in international forums, but also with the technology-leading countries, like the United States and Japan, and their partners in Europe. By 2015, after a decade of multilateral efforts by many states including China, this understanding helped drive China to sign up (unofficially) to consider expansive new norms agreed upon by the UN Group of Governmental Experts on cooperative relations in security aspects of cyber space (Marks, 2015). The political weight we can attach to China's support for diplomacy as a foundational element of cyber power is reflected more convincingly in a formal agreement with Russia, in which the two countries agree not to undertake actions like 'unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack' (Austin, 2016, p. 199).

Thus at the outset of pursuit of China's ambition to accumulate the attributes of cyber power there is a fundamental conflict or contradiction. In classic chauvinistic fashion, China wants to rid itself of foreign technological control but says it needs to participate in a global system of the exercise of cyber power to even begin the journey. Moreover, President Xi has specifically identified the need for China and the United States to work together to avoid the 'Thucydides trap', the propensity for conflict between an emergent power and an established power because of hubris or fear.

There is no agreement inside or outside China on how to assess even the foundations of the country's power, let alone the dynamic aspects of the exercise of power. The best overview of this lack of consensus is given by one of China's leading advocates of its claims to power, Yan Xuetong. In a 2006 article on measurement of China's comprehensive national power, he observed that leading research centres in China (Tsinghua University, the Chinese Academy of Social Sciences, the Academy of Military Sciences and the China Institute of Contemporary International Relations) have systems ranging from between seven and eight general categories, but between 23 indices and up to 115 sub-indexes (Yan, 2006). He also mentioned a host of analytical assumptions and political biases that impact such assessments, and not unsurprisingly suggested a 'power class' approach that fits comfortably with the Chinese Communist Party's propaganda themes. This is the idea that the current standing of China is only to be expected given the past distribution of international power under the old-class based approaches to international relations and national economic development.

In his 2006 article, Yan rightly concluded that 'when forecasting China's future power status, we should not only take account of the speed of China's power growth but also the growth of the other states' power.' He also said that we needed to understand the character of China's power and the conditions for its growth or decline (Yan, 2006, p. 22). Yan's analysis makes plain that an understanding or measurement of a country's power status is entirely based upon the reason why the question about it has been posed. A state's power does not exist unless it is perceived and it is the act of perception or analysis, and the framing of a purpose for the question, that begins to define it.

The same lack of consensus exists in Chinese efforts to measure its degree of informatisation and how far it has travelled towards establishing the foundations of becoming a 'cyber power'. In 2002, the Ministry of Information Industry released details of its National Informatisation Quotient (NIQ), which had been under development for the previous eight years (People's Daily, 2002). It was mandated to be the national standard but subsequent work, and competing efforts in the academic establishment showed that it was to a considerable degree unfit for purpose (Austin, 2014, p. 7). The national index was also intended to allow China to measure progress against its own baselines, year on year, but was also intended to allow comparisons with other countries. But it is an index based largely on physical outputs, such as numbers of users or numbers of computers produced.

More than a few Chinese researchers have indirectly challenged the narrowness of the NIQ by striving to develop more qualitative measures, see e.g. Zhang (2015); Zhang, et al. (2013) and Tao & Yu (2015). These assessments confirm the view that China is struggling to meet its informatisation ambitions in areas like development of the skills base. A 2015 assessment by a Chinese scholar showed China as sitting at half the level of development of the average of developed economies and only matching, not surpassing, the average level of developing countries. Based on both Chinese and non-Chinese assessments of the country's informatisation broadly defined, China does sit well down in the international grades, with the World Economic Forum's recent annual rankings of China—61st, 62nd and 59th in 2014, 2015 and 2016—not being too far off the mark compared with some Chinese assessments in terms of placing China very much in the middle of the pack.

Separate from the economic or social analysis of the foundations of China's power, there is a less well-developed body of work in China around the geopolitical dimensions drawing inspiration from Western conceptions of comprehensive national power. One of the best examples is the effort by the

Director of the Institute of Information and Social Development Studies in the Chinese Institute of Contemporary International Relations, Li Zhang (2012) who drew on the work of UK and US scholars to postulate seven aspects of cyber power:

1. Internet and information technology (IT) capabilities
2. IT industry capabilities
3. Internet market capabilities
4. Degree of influence of Internet culture on the society
5. Internet diplomacy/foreign policy capabilities
6. Cyber military strength
7. National intent and a cyberspace strategy.[3]

Zhang (2012, pp. 802-803)

Of these, only 5 and 7 appear to relate to the exercise of cyber power on the international stage. Indirectly, 4 relates to domestic political power where the state tries to guide the influence of the internet on society. Even so, Zhang concluded that in terms of cyber power, 'the United States' strength is unequalled, giving it a strong position with unmatched advantages' (p. 803).

The richer and more convincing assessments of China's cyber power come not from such indexes but detailed studies of how China exercises its power in cyber space. For the domestic scene, there is a large amount of scholarship and continuing daily commentary that assess the intimidating power of the Chinese government in supressing political opposition at home or blocking information from outside the country. As summarised elsewhere, the government's interest in pursuing an i-dictatorship is significantly enhanced by China's development of cyber surveillance, geo-blocking, and taking down content considered politically dangerous (Austin, 2014, pp. 62-74; Inkster, 2016).

On the international stage, Xi has put China in a position of 'rising power' and 'aspiring power' in cyber space affairs, a concept that is deeply rooted in a neo-realist or techno-nationalist vision, at the same time as it acts out an internationalist agenda of cooperation and exchange. In this respect, China is no different from the United States which, as Henry Kissinger noted in *Diplomacy*, can (and should) simultaneously pursue both realist (Rooseveltian) and liberal (Wilsonian) impulses (Kissinger, 1994, pp. 29-55). But as Yan (2006) notes, it is hard to understand the quality (the reality) of China's cyber power without studying the 'growth of other states' powers' (p. 22). At least he is heading in the direction of studying diplomatic interaction through which state power is realised.

The Political Science of Power in the Information Age

Power is used here in a political sense to mean the ability of one party to influence another party to do what they would not otherwise have done. This is the relational approach to the study of power.[4] It can be contrasted with the concept of 'power as resources', where the mere possession of money, military means or networks (elements of national power) becomes a foundation for comparing the power status of different countries. This latter approach underpins the concept of balance of power (Baldwin, 2013, p. 281).

[3] The author is grateful to Munish Sharma for drawing this article to his attention.

[4] For a comprehensive overview of the concept of power in political science and international relations theory and discourse, see Baldwin (2013)

Drawing on a number of sources, but especially Baldwin, we can identify the following key insights into the study of power in the past century that are relevant to unpacking the complexity of analysis of the exercise of state power:

- the concept of power as resources is meaningless unless one can answer the question 'power over what and in which circumstances' (the relational dimension) (ibid., p. 276)
- at best, a description of a state's power resources is an indicator of potential power and an estimate of potential power must always refer back to the plans or intentions of the state, (ibid., p. 277) (Does it plan global domination, a local war, or peaceful coexistence?)
- static power resources in one field (say economic power) are not fungible for (transferrable to) exercise of power in other fields (say military power needed to coerce other states)
- similarly, power assets in one military domain (such as nuclear warfighting) may not be usable at all in other military domains (such as low intensity conflict or counter-insurgency warfare) (ibid., p. 278)
- the exercise of power is driven entirely by the context (place, time, actors, diplomatic practice, international norms, and any special features of the political environment)
- where a state or two states hold overwhelming weight in one field (such as nuclear war-fighting capability), another state with lesser power resources in the same field has more influence in that field on the power of other lesser states than on the power of the states with overwhelming capability
- a state that appears weaker in power resources can employ political strategies in the exercise of relational power to overcome the asymmetry
- the *domain* of influence of a state (its power) will be different from that of other states (most at best can claim some regional influence, while only a few can claim global influence and then not necessarily in all fields)
- the *scope* of the exercise of power by most states will be limited to various identifiable sectors of activity (such as economic policy, international finance, science and technology, naval warfare, information technology manufacturing, or counter-terrorism policing)
- a state can exercise influence in the same context alongside other states, but it may not be as powerful as often as some of the other powerful actors in that context
- exercise of power can employ symbolic means ('appeals to normative symbols… discourses, propaganda, framing and narratives') (ibid., p. 275)
- the exercise of power is often contested especially where new behaviours or new (returning) actors are involved since such action usually disturbs status quo interests
- there has to be a chronological perspective (a country's economic power can decline over time or the apparent initial success of a military invasion in year one can look very different in year five)
- a moral or ethical perspective is essential: in what ways is an exercise of power conducive to international order and peace, economic prosperity or the protection of political and civil rights.

Baldwin makes two profound judgements. The first is easy to understand. He says that scholars would be better off abandoning the rather impossible task of measuring and comparing elements of national power to see which state is more powerful in the abstract. As a substitute for that, he calls on scholars to consider a focus on 'measuring the distribution of power within specified scopes and domains' (as defined above). The second is a little more complex and is related to statistical methodology. He suggests that political science approaches that posit power as the driving force (the independent variable) and outcomes as the dependent variables may be misrepresenting reality. He asks how differently (and more accurately) would scholars see power in international affairs if they took it as an outcome (a dependent variable) and not the main driver (ibid., p. 288). Just what he posits as a useful substitute independent variable to replace power is not entirely clear. My interpretation of his

line of argument is that he favours giving pride of place to context: how does a given set of relationships, changing over time, drive changes in the exercise of power. The independent variable and driver of outcomes is a 'given set of relationships' rather than 'power resources' expressed independently of context.

This translated in the briefest of forms for the purposes of this paper would suggest that the most fruitful form of analysis of China's exercise of its cyber power would be to posit as the independent variable something like the totality of China's cyber relations with the United States, Japan, Russia, the European Union, India and arguably even Taiwan and North and South Koreas. Could this sort of thinking or insight underpin the signature foreign policy setting of China under President Xi: 'a new type of great power relations'. If China can set these right, then it will maximise its exercise of power and minimise hostile or antagonistic exercise of power against China.

This is a perspective based exclusively on political science approaches somewhat independent of the information age. If we ask how we might adapt it to account for any special features of the cyber age, we begin to move toward an even richer analytical model.

As Nye suggests in his landmark essay on cyber power, there seems to be some aspect of cyber power that undermines the sense of power concentration (polarity) normally associated with classical conceptions of power, either hard or soft (Nye Jr, 2010, pp. 1-2). Nye calls this phenomenon a 'diffusion' of power under the influence of the cyber technologies and the political economy of the globalised ICT sector. Philosophers of the information age, like Floridi, have called this aspect 'distributed authority' (Floridi, 2013, pp. 261-276). Floridi has gone much farther, identifying other characteristics of the information age, such as synchronization, localization and correlation. So at least for Nye and Floridi, and I certainly agree, power in the cyber age is not international power as classically understood or debated. A state's power today can only be understood with reference to the new character of politics, political economy and war arising from the information age.

The defining characteristic of state power in the information age appears to be that it is enmeshed, entangled even, in a global web of power networks, defined as much by the power of giant information utilities (such as Google and Microsoft)[5] and international investment as it is by global (non-national) diffusion of the component scientific and labour inputs into the national informatisation enterprise. Thus, what is left to the state is to try to draw the boundary between its sovereign power, this borderless information world, and the determination of other states to shape that boundary of sovereignty. In this light, we can see China's claim to cyber power, internet sovereignty or information sovereignty as not just a determination to draw a fairly firm line around sovereign capability but also a political statement that this is a highly-contested (possibly futile) task. This suggestion is supported to some degree by the well-argued case by Forsyth and Pope (2014) that 'international order is inevitable in cyberspace', as opposed to the much anticipated disorder characterised by 'duelling sovereignties' and 'balkanization' of the internet.

There is room however to question some assumptions that Forsyth and Pope appear to make. The first is explicit. They say that 'cyberspace is a fringe environment where accepted norms of behaviour lag just enough to permit acts that would be deemed acceptable in other areas' (ibid., pp. 121-122). This suggestion can be contrasted with those by philosophers of the information age who believe, along with the Chinese leaders, that information power changes everything and represents a new era in history that might just bring new rules in international relations. The second assumption that Forsyth and Pope seem to make is that international order in cyber space will not see the same sort of shocks and redefinition that international order experienced before the information age. What for example

[5] Coined by Masuda (1980) in his wonderfully accurate predictive work published in Japan, the term 'information utilities' is used here as a catch-all term for this group of powerful global corporations.

might be the cyber age equivalent of the Arab oil embargo of 1973, the rise of Islamic State, or the Global Financial Crisis (GFC) of 2008. In fact, a case can be made that the contours of such events, especially the GFC, were aggravated by the cyber age. Thus we need to recall that international order in cyber space will still be marked by power contests and power challenges even if the general trend is toward a dampening of conflict and toward convergence of interest.

The thrust of these observations about the unique characteristics of state power in the cyber age is that for a country like China to maximise gains, it must enjoy good relations not only with great powers (other states) but also with powerful corporations (e.g. Google, Apple) and with the distributed authority and power of both its own netizens and foreign netizens who may be influential on key issues or with selected key actors.

Mapping China's Cyber Power: A Provisional Template

There has been little effort to link up the theoretical findings of scholars on power in general or in the information age and the problem of estimating or forecasting the outcomes in relational power for China when it seeks to exercise power in the cyber domain.

My book, *Cyber Policy in China* (2014), used a values-based framework to estimate the power of China's leaders relative to other actors in cyber space affairs against the background of their ambition to become an advanced information society. It found firstly that China was not making the progress that its leaders wanted in accumulating the elements of cyber power. Secondly, it found that China was not consistently pursuing the relationship settings nor creating the right environmental factors at home (innovation system and innovator class) to reach its goals. Thirdly, it found that internationally, China was subject more to the power of other actors than vice versa. In an article later that same year addressing asymmetries in cyber power between China and the United States, I argued that China was showing signs of tension because of its continuing inability to make a dent in the cyber military superiority of the United States (Austin, 2014).

Two recent works are worthy of note because they tackle the question of China's cyber power more directly, although they are both relatively short given the huge scope of the topic. Their approach is based more on an analysis of the real world practices (a logic of the situation analysis) than on any highly developed political science concepts.

Inkster (2016) concluded that China is trying to increase its power in cyber space but that effort will be shaped by the continuing power of the Western countries in the ICT sector and the global flow of information. The worst outcome might be a world divided into two camps of cyber power, but that is not likely because China would try to avoid such an extreme scenario. In a very apt metaphor, Inkster wrote that China 'has in effect embarked on a global experiment in which some liberal democracies serve as the control group'. He reserved his judgement slightly suggesting that 'it will be some time before any safe conclusions can be reached about this experiment' (p. 150). So the cut and thrust of international power and politics is for Inkster still very much alive, even if the medium term outcomes of a cooperative China seated in a stable international order of cyber space look fairly certain. Inskter's study gives an excellent overview of the way in which China has in the recent past sought to participate in that cut and thrust to exercise its cyber power. He used examples like the attempt to change the legislative and regulatory foundations of the ICT sector in China to promote its indigenization, the attempt by China to tightly control political opposition that may emerge through internet-based communications, and its efforts to acquire cyber military capability.

Munish Sharma in a useful study on China's cyber power from the Indian Institute of Defence and Strategic Studies, notes the 7-point formula of Zhang (2012), and observes immediately after that even if a country has the attributes of cyber power, 'the intention to leverage the capability in order to support its political goals establishes it as a cyber power' (Sharma, 2016, p. 47). Sharma's analysis describes in quite broad terms the way in which Chinese leaders have set about accumulating the attributes of cyber power. He leaves the reader with the clear view that China's leaders are highly committed to becoming a cyber power, that the country is firmly on that path, and that China's leader's understand 'leverage' (the set of relationships) as the prime driver, not perceptions of power resources.

Thus we can accept that there is a body of theory supporting closer attention to dynamic aspects of the exercise of power, and several works on China's cyber power affirming the centrality of the set of dynamic relations. How then might we extend the descriptive and broad analysis of China's cyber power that we have seen in the works mentioned here into the realm of how we should perceive the exercise of that power in the daily cut and thrust of policy, using the lens of the traditions of political science.

To assist in this deeper exploration of China's relational power in cyber space affairs, we can take something of a lead from two recent works on China's power in general. Both Shambaugh (2013) and Christensen (2015) rightly assume and assert limits to China's power of one kind or another. Reading both books makes it fairly plain that the prospect of China's hegemony is not one to stake much money on. The pair of books offer two different aspects of China's relational power. Shambaugh looks closely at China's power resources and organization in the context of a reinvigorated global diplomacy (China looking outwards). He concludes that China is far from possessing the necessary tools to be a global power (Shambaugh, 2013, p. 11). Christensen looks at how the US can influence China's policies, though his departure point is sources of power. The essence of the book is an analysis of the exercise of power in the particular international context of the 21st century. He concludes that this context 'reduces the likelihood that China will be both willing and able to drive the United States out of the Asian region' (Christensen, 2015, p. 8). Thus in these two books, we see China as both a power maker and a power taker, in line with the analogy from economics that one can be a price maker or a price taker (Austin, 2016).

The two books mentioned above also reveal a third vector of China's power: its ability to spoil (disrupt) the application of power by other states without necessarily being able to bend them to China's will or being bet to the will of other states. The concept of states as spoiler powers in cyber space, rather than dominators, is brilliantly captured in *The Hacked World Order* by Adam Segal (2016). Equally, if a state can be a disruptor it can also be a facilitator, where its acts of acquiescence and cooperation do not represent a clear exercise of power by it, but where the mere fact that China is not opposing or disrupting gives enhanced impact to the exercise of power by other states or groups of states.

Thus, in principle, we can identify four co-existing vectors of China's cyber power as a state: maker, taker, spoiler, and acquiescent (facilitator). We might also elaborate on this analytical framework by classifying observed elements as constituting an exercise of hard power and soft power, drawing on Nye's concept of the latter. The importance of recognising the soft power consideration is its normative character. Since, by definition, soft power does not involve coercion and hard power does, the more a state relies on soft power, the more peaceful (and acceptable) its international relations are. In most circumstances, we cannot begrudge any state its exercise of soft power, no matter how much, since peacefulness is the primary benchmark by which we assess the international behaviour of all states.

In addition, we cannot perceive China's power in any domain without recognising the domestic domain as at least an equal realm of the exercise of power. We could even go further and suggest that

the domestic realm may be the dominant one as far as politicians are concerned even when they are acting on the international stage.

We would want to know how comprehensively China's influence was felt, what selection of states or other actors were influenced (just one, a few, or many; small powers or great powers) and for how long China was able to sustain that act of influence, i.e. the durability of the exercise of power and breadth of influence.

This would give us a schematic of China's relational power as indicated in Table 1.

Table 1. A Schematic of China's Relational Cyber Power over Time

	External	Internal	Hard	Soft	Durability of Influence	Breadth of influence
Maker: China induces the rest	?	?	?	?	?	?
Maker: China precludes the rest	?	?	?	?	?	?
Maker: China shapes the rest	?	?	?	?	?	?
China as *Spoiler*	?	?	?	?	?	?
China as *Acquiescent*	?	?	?	?	?	?
Taker: China is shaped by the rest	?	?	?	?	?	?
Taker: China is precluded by the rest	?	?	?	?	?	?
Taker: China is induced by the rest	?	?	?	?	?	?

We would also want to know whether China had been more 'cyber powerful' in the political sphere or the military sphere, or even the espionage sphere. We could also construct a separate schematic for sub-sets of 'cyber power', such as 'economic cyber power', 'commercial cyber power', 'scientific cyber power', 'military cyber power', 'cyber espionage power', or 'counter-crime cyber power', to name some of the more obvious.

And finally, for the purposes of this paper, there can be a goal-specific focus to analysing a country's exercise of power. For example, we can ask the question whether China has been able to exercise its cyber power any differently after the Xi announcement of the new 'cyber power' ambition in February 2014 compared with a similar time frame immediately preceding the announcement.

Conclusion

This paper has reviewed some possible approaches to the study of China's use of cyber power and how this relates to predicting outcomes for the country's policy settings and actions. The paper relegates the idea of static assessment of national power (as the sum of assets) well into the background in favour of a rich and complex political science approach to understanding China's relational power. The paper has exposed what seems to be a strong conflict between a nationalistic set of ambitions by China to achieve first tier status in the possession of cyber power resources (industrial, scientific or military) and equally consistent acknowledgement by the country's leaders that China can only maximise its power, including its security, in cyber space affairs through active participation in a continually expanding set of globalised relations.

In looking to satisfy its cyber power ambition, China faces many dilemmas, but there is one over-arching conundrum. It has no way of making the set of other actors (with whom it may occasionally compete for power) hold still. This reality was captured brilliantly in a valedictory speech by the US ambassador to Australia, John Berry, at the National Press Club in Canberra in August 2016. In what

was a clear allusion to China without naming it, Berry declared that the United States 'will remain a rising power for generations to come. Our economy is second to none, as are our universities, our military, and our capacity for research and innovation. For us, the 21st century is only Act 2' (US Embassy & Consulates in Australia, 2016). China may be a rising power but its competitors and rivals for cyber power continue to rise as well.

On the evidence to date, China's ability to exercise cyber power is either so contested or shared with so many powerful actors, that on the few occasions when its leaders have taken a major initiative to flex their muscles in cyber space affairs, they have not made decisive breakthroughs. They have been far more successful at reaping the benefits of cooperation and acquiescence. Based on the evidence present in my 2014 book and subsequent papers, and on the above template for investigating Chinese cyber power more forensically, I feel comfortable concluding that:

(a) China is more likely to a spoiler in cyber space rather than a dominating or dominant power;
(b) that said, the collaborative aspects of the exercise of cyber power by China are likely to outweigh its spoiler effects; and
(c) the country's approach to a nationally framed cyber power is self-defeating.

There are many forces driving these conclusions or outcomes. First, trends in the concentration of the attributes of cyber power do not favour China as an increasing number of states improve their own cyber power. Second, the international system of cyber power constrains China from exercising brute force in this domain in any way that can advance China's goals. Third, the globalised character of cyber power is such that China is unlikely to find a policy formula that will see it occupy any 'commanding heights' of cyber power alongside the United States, Japan and the European Union unless it radically alters course in domestic politics.

Cyber power is essentially an outcome of the political economy of knowledge, and as I have said in the concluding remarks of my 2014 book, 'knowledge has no flag'. The political economy of knowledge is not something that states of any stripe do well, and authoritarian states with nationalistic impulses probably do it more poorly than liberal democracies which are also market economies.

References

Austin, G., 2014. *Cyber Policy in China.* Cambridge, UK: Polity.

Austin, G., 2014. Managing Asymmetries in Chinese and American Cyber Power. *Georgetown Journal of International Affairs. International Engagement in Cyber IV,* pp. 141-51.

Austin, G., 2016. International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In: A. Osula & H. Rõigas, eds. *International Cyber Norms: Legal, Policy & Industry Perspectives.* Tallinn: NATO CCDCOE Publications, pp. 171-201.

Baldwin, D., 2013. Power and International Relations. In: T. Risse & B. A. Simmons, eds. *Handbook of International Relations.* London: Sage, pp. 273-297.

Christensen, T., 2015. *The China Challenge: Shaping the Choices of a Rising Power.* New York NY: W. W. Norton & Co.

Cisco - The Network, 2015. *Cisco Increases Investment in Innovation and Development in China.* [Online]
Available at: https://newsroom.cisco.com/press-release-content?articleId=1660013
[Accessed 05 09 2016].

Floridi, L., 2013. *The ethics of information,* Oxford: Oxford University Press.

Forsyth Jr, J. W. & Pope, B. E., 2014. Structural Causes and Cyber Effect: Why International Order is Inevitable in Cyberspace. *Strategic Studies Quarterly,* Volume Winter 2014, pp. 113-130.

Inkster, N., 2016. *China's Cyber Power.* Kindle ed. London: IISS Adelphi Book 456.

Kissinger, H., 1994. *Diplomacy.* New York NY: Simon & Schuster.

Marks, J., 2015. *U.N. body agrees to U.S. norms in cyberspace.* [Online]
Available at: http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900.html
[Accessed 05 09 2016].

Masuda, Y., 1980. *The Information Society as Post-industrial Society.* Fujimara: Institute for the Information Society. First US printing, 1981. Bethesda, MD: World Future Society.

Ministry of Foreign Affairs of the PRC, 2015. *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference.* [Online]
Available at: http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml
[Accessed 05 09 2016].

Nye Jr, J., 2010. *Cyber Power,* Cambridge MA: Harvard University Belfer Center for Science and International Affairs.

Pasick, A., 2015. *It's official—China is blacklisting Apple, Cisco, and other US tech companies.* [Online]
Available at: http://qz.com/351256/its-official-china-is-blacklisting-apple-cisco-and-other-us-tech-companies/
[Accessed 05 09 2016].

People's Daily, 2002. *China Releases World's First National IT Index.* [Online]
Available at: http://www.china.org.cn/english/32193.htm
[Accessed 05 09 2016].

Segal, A., 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York NY: Council on Foreign Relations.

Shambaugh, D., 2013. *China Goes Global: The Partial Power.* Oxford: Oxford University Press.

Sharma, M., 2016. China's Emergence as a Cyber Power. *Journal of Defence Studies,* 10(1), pp. 43-68.

Tao, C. & Yu, M., 2015. Comparative Analysis on the Integration Level of Informatization and Industrialization: Evidence from China. *International Journal of Hybrid Information Technology,* 8(8), pp. 123-132.

US Embassy & Consulates in Australia, 2016. *"The United States and Australia: Infinite Possibilities – the New Normal" – Ambassador Berry's Remarks at the National Press Club of Australia.* [Online]

Available at: https://au.usembassy.gov/united-states-australia-infinite-possibilities-new-normal-ambassador-berrys-remarks-national-press-club-australia/
[Accessed 05 09 2016].
World Bank & PRC Development Research Centre of the State Council, 2013. *China 2030: Building a modern, harmonious, and creative society,* Washington DC: The World Bank.
World Economic Forum, 2016. *Global Information Technology Report 2016.* [Online]
Available at: https://www.weforum.org/reports/the-global-information-technology-report-2016/
[Accessed 05 09 2016].
Xinhua, 2014. *Xi Jinping leads internet security group.* [Online]
Available at: http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm
[Accessed 05 09 2016].
Xinhua, 2015. *China's Military Strategy.* [Online]
Available at: http://news.xinhuanet.com/english/china/2015-05/26/c_134271001.htm
[Accessed 05 09 2016].
Xinhua, 2016a. *Xi sets targets for China's science, technology progress.* [Online]
Available at: http://news.xinhuanet.com/english/2016-05/30/c_135399655.htm
[Accessed 05 09 2016].
Xinhua, 2016b. *President Xi says China faces major science, technology 'bottleneck'.* [Online]
Available at: http://news.xinhuanet.com/english/2016-06/01/c_135402671.htm
[Accessed 5 09 2016].
Xinhua, 2016c. *President Xi's speech on science, technology published.* [Online]
Available at: http://usa.chinadaily.com.cn/china/2016-06/02/content_25595722.htm
[Accessed 5 09 2016].
Yan, X., 2006. The Rise of China and its Power Status. *Chinese Journal of International Politics,* Volume 1, pp. 5-33.
Yuen, S., 2015. Becoming a cyber power: China's cybersecurity upgrade and its consequences. *China Perspectives,* 2015(2), pp. 53-58.
Zhang, L., 2012. A Chinese Perspective on Cyber War. *International Review of the Red Cross,* 94(886), pp. 802-803.
Zhang, L., Xue, L., Li, D. & Fu, Z., 2013. Evaluation of the rural informatization level in four Chinese regions: A methodology based on catastrophe theory. *Mathematical and Computer Modelling,* 58(3-4), pp. 868-876.
Zhang, S., 2016. *China sets goals of informatization.* [Online]
Available at: http://english.cri.cn/12394/2016/07/28/3821s935816.htm
[Accessed 05 09 2016].
Zhang, Y., 2015. *Forecast of the informatization index of China from 2011 to 2015 using the Grey forecasting scale.* Leicester, IEEE International Conference on Grey Systems and Intelligent Services (GSIS).
Zuo, M., 2016. *China aims to become internet superpower by 2050.* [Online]
Available at: http://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020
[Accessed 05 09 2016].

This Page is Intentionally Blank

Lau China Institute
Strand Campus
King's College London
Strand
London WC2R 2LS