SPECIAL REPORT

ASPI

November 2014

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

China’s cyberpower

International and domestic priorities

James A Lewis
Simon Hansen

Introduction

Since Xi Jinping took over the leadership of the Chinese Communist Party in 2012 and assumed the presidency of his nation, the cybersphere has become an even more important strategic domain. Xi has stressed that cyberpower should be a national priority for China if the country’s to reach its economic, societal and military potential.

And that causes much concern among Western states already concerned about China’s activities in the cybersphere. The information officers of large Western corporations have long voiced their worries, and our governments have intervened to prevent the commercial involvement of Chinese companies in our networks. Barack Obama even insisted that his first discussions with Xi were to cover Washington’s concerns about Beijing’s cyber espionage.

This two-part publication explores two aspects of China’s cyberpower.

James Lewis assesses whether China is waging an economic war in cyberspace—a gradual ‘death by a thousand cuts’ campaign to ‘hollow out’ the Western economy—as is claimed by many American commentators. Lewis finds the claim to be an oversimplification: Chinese companies are in commercial competition, including with each other, and that—rather than a Chinese Government plan to bring the US to its knees—explains their commercial cyberspying. The global economy is far too interconnected for a destructive strategy to affect only other countries. The blowback would be unbearable for China. The upshot: never attribute to malice what’s adequately explained by avarice.

Simon Hansen examines China’s internal mechanisms for delivering and protecting cyberpower. New structures and strategies are emerging under Xi’s presidency, with their own lexicon and nuances. Hansen shows that a great part of China’s efforts are about domestic political and economic concerns, even while Beijing flexes its muscles in the international debate about regulation and the internet.

These papers are essential reading for those who want to understand China’s activities and intentions in cyberspace.

Tobias Feakin
Director of ASPI’s International Cyber Policy Centre

Top Chinese leaders attend the third Plenary Session of the 18th CPC Central Committee in Beijing, China, 12 November 2013.© Lan Hongguang/Xinhua Press/Corbis

Economic warfare and cyberspace

James A Lewis

Many observers assign a high degree of planned malevolence to China's behaviour in cyberspace. This may reflect the intensity of China's espionage or the discrepancy between China's protestations of innocence and its practices. Some Western analysts ascribe China's practices to a centrally guided strategy to 'hollow out' Western economies—a slow campaign of economic warfare intended to cause 'death by a thousand cuts'.

One analyst put it as follows on Australian television:

> We're living through the literally biggest theft in all of human history—the massive theft of intellectual property emanating from China that's been measured in some terms as much as $1 trillion [NB: This trillion dollar figure was discredited shortly after its release]. So in many ways it's not as sexy as a cyber-Pearl Harbour, but it could be just as consequential in terms of a death by a thousand cuts scenario—death by a thousand cuts that are both economic and security cuts.[1]

Similar charges have been made about China's intent to manipulate global finances or energy markets as an economic weapon pointed at the West.[2]

Analysts face difficult challenges in describing a new era of international conflict in which the use of conventional armed forces isn't the preferred tool for interstate conflict. The risk of a conventional military clash among great powers is low because of the serious consequences that would follow, yet competition and low-level conflict among international rivals, contrary to millennial expectations, hasn't diminished.[3] In this environment, it's reasonable to ask what other tools for the exercise of state power are available and whether they're being used.

Economic warfare is one such tool. Economic warfare involves a deliberate strategy to restrict or manipulate trade, financial markets and access to technology to harm an opponent.[4] We need to consider three questions:

- Is there any evidence that an economic warfare strategy explains China's behaviour?
- Would a Chinese economic warfare strategy actually work?
- Does economic warfare still make sense as a tool of national power?

On the first question, there's no evidence that China is engaged in economic warfare. On the larger questions about the utility of economic warfare, its utility in a wealthier, more developed and greatly interconnected world is reduced but not entirely eliminated.[5]

Accompanying the charges of economic warfare and death by a thousand cuts is a picture of Chinese strategists that attributes deep cunning and infinite patience to them, sometimes expressed in the saying 'Americans play checkers and Chinese play chess.' These themes have a long and unfortunate history in Western literature about China and should be discarded. In considering economic warfare as an explanation of Chinese behaviour, it appears that these charges reflect Western fears more than Chinese intent, and that less convoluted and conspiratorial concepts better explain Chinese behaviour.

Assessing Chinese behaviour

Public sources and discussions with Chinese officials suggest that China's cyber doctrine has three elements: control of networks and data to preserve political stability, espionage to build China's economy and technological capabilities, and disruptive acts aimed at damaging an opponent's military command and control and weapons systems, all of which are dependent on software and networks. More 'strategic' uses, such as striking civilian infrastructure in the opponent's homeland, appear to be a lower priority and considered as an adjunct to nuclear strikes as part of China's strategic deterrence. No discussion has ever hinted at death by 1,000 cuts, and Chinese officials seem more concerned about the American and Chinese economies' interdependence. For example, one Chinese scholar from a government-affiliated think tank said that China would never destabilise US financial markets because there's too much Chinese money tied up in them.

While Chinese firms may wish to gain market share at the expense of Western competitors and seek to avoid the risk and expense of R&D, their motives are commercial, not strategic. The People's Liberation Army intends to steal advanced military technology, but in order to modernise China's military and provide it with advantage in battle, not to eliminate Western defence firms. The army's doctrine calls for weakening an opponent's economy during conflict, but doesn't talk about peacetime use.[6] Even this idea of damaging an opponent's productive capabilities during conflict may only reflect Chinese endorsement of outdated Western doctrine. The goal is to strengthen China, not to weaken opponents.

Quantitative measures of cyber incidents from a number of sources show that Chinese actors are the most active in using cyber techniques for economic espionage.[7] This has been true for more than a decade—a troubling phenomenon that's one of the major sources of global concerns about cybersecurity (although American and Russian activities also contribute to those concerns). China's intention is to use cyber espionage to acquire technology to catch up with and surpass the West both economically and militarily. China's still a net importer of advanced technology, and its leaders would like to change that. While it sets long-term strategic economic goals, they have a domestic focus. It has followed a consistent military strategy for two decades, but the focus has been inwards, on restoring China's greatness, rather than on destroying opponents.

Since the opening to the West under Deng, there's been a broad national effort to extract concessions and technology from Western companies in exchange for access to markets, cheap labour, an accommodating regulatory environment and (at least in the past) subsidies. The actions of Chinese hackers are consistent with the larger national effort to increase China's national power and prestige. And the prevailing notion, first expressed by Deng, that to grow rich is glorious, means that they're also competing for private gain, often against each other. China's leaders, although challenged by the tumultuous politics that economic growth has created, clearly expect China's growing economic power to increase its influence in international affairs, but that's not the same as the emotionally laden term 'warfare'.

China's economic growth creates immense stresses that the central Chinese Communist Party organs aren't well equipped to manage. Nor have Chinese efforts in international relations shown evidence of deep cunning or even a clear understanding of Asian regional dynamics. China's a captive of its own rhetoric when it comes to foreign affairs. A simpler and more compelling explanation of Chinese behaviour focused on China's desire for gain rather than a desire to harm its opponents better explains its cyber activities than speculation about a centrally directed campaign of economic warfare against the US and its allies. Deng Xiaoping's statement, 'to be rich is glorious', is a more powerful explanation for Chinese behaviour than economic warfare.

An imperfect tool

If economic warfare and death by a thousand cuts are inaccurate descriptions of Chinese intent, that inaccuracy has serious implications for policy, the most important being that we don't want to misrepresent the ambitions of the leadership in Beijing. But does it matter if the effect of Chinese actions is the same as if there were a Chinese grand strategy to undermine the US? The charges that Chinese espionage is hollowing out the American economy are close relatives of earlier charges that globalisation and offshoring were hollowing out American manufacturing, and the descendants of earlier charges levied against Japan in the heyday of its growth. Fears about globalisation and Japanese predominance both proved to be inaccurate, and a careful disaggregation of causes is necessary to determine how much 'hollowing' is the result of Chinese actions.

First, if hollowing out is indeed China's strategy, it doesn't seem to be working very well. The US share of global GDP was between 20% and 25% in the 1950s; 60 years later, its share is roughly the same. China's share of global income has grown, but that's because European national incomes have failed to grow, leading to a reduced European share of global income, not because China is hollowing out the US. Since China's opening to the West, US national income has almost doubled, from $8.8 trillion to over $16 trillion (in constant 2012 dollars), and the ability of American firms to take advantage of China as a market and as a low-cost supplier helps to explain this.

This is a conundrum from the globalisation debate. Is it a bad outcome if the US manufactures less but is wealthier as a result? There are distributional effects, as high-paying manufacturing jobs disappear, and discomfort with a dependence on a global supply chain rather than a national industrial base, but the strategic effect is limited. China could cut off sales of some manufactured goods, but that would have no immediate effect on military capabilities and a long-term effect only if there were no other sources of supply or none could be created. China could refuse to lend, but at worst that would create a period of painful readjustment without military effect. None of these tactics provides a crippling blow and all could backfire by creating economic damage to China (the effect of restricting sales is to create foreign competitors). China depends on global markets for growth, and many commentators have pointed out its symbiotic economic relationship with the US, making economic warfare as likely to damage China as the US.

We could argue that income may not be the best measure, however, and that the growth of Chinese industrial and scientific capabilities at the expense of the US better measures the potential for harm. This charge unhelpfully mixes factors that explain changes in the distribution of manufacturing and research. The most important factor is the effect of the lower cost of communications and transportation on economic and scientific activity—those who invest in research can now think on a global scale. China remains a net importer of advanced technology, despite impressive strides. By any measure, the US still possesses an impressive scientific and technological base, even if it's in decline, but that decline is more likely the result of US decisions on domestic issues such as taxation, education policies, cultural change and R&D spending, not Chinese hostility.

That the charges of economic warfare echo concerns about the effects of globalisation on the US economy and chauvinistic alarm over the rise of China is one reason to question them. These are complex and emotive subjects in which the logic of economic analysis runs contrary to public perception. Another explanation for China hollowing out the US manufacturing sector is that the US is benefiting from a comparative advantage in trade. In any case, an increase in manufacturing in China is better explained by China's development policies, its leaders' pursuit of modernisation and the desire of its entrepreneurs to gain wealth, rather than a deliberate policy to damage the US.[8] These economic and development motives explain Chinese behaviour better than economic warfare.

China's attempt to restrict rare earth exports, which some Chinese officials first ascribed to a plan to force Western companies to move manufacturing to China and then, after criticism, to environmental motives, wasn't a happy experience or a successful exercise of national power. It spurred the development of alternative sources of supply, led to a World Trade Organization case that China lost and damaged China's reputation, all without noticeable strategic effect.[9]

Financial warfare seems equally improbable and ineffective. For example, one account posited the following in 2011:

> China has been buying up US government debt and is now its biggest holder. If China were to dump this debt, it would totally screw with the economy. China could, hypothetically, win any number of foreign policy objectives by making it impossible for you to pay your mortgage.[10]

A cynic might note that when the US deregulated Wall Street, it did a fine job of making it difficult for people to pay their mortgages without the need for Chinese assistance or hostility. Damage to US global influence came more from a loss of trust in the American model and US leadership than from Chinese plots.

China's purchases of US bonds, which offer a combination of good returns and security not available in quantity elsewhere, are more persuasively explained by economic motives. In one recent incident, increased Chinese purchases of US bonds were driven by China's trade goals (to lower the value of its currency). According to the *Wall Street Journal*, the purchases had 'salutary effects on both sides of the Pacific … [T]hey hold down US interest rates, making houses more affordable and generally easing financial conditions in the US economy.'[11]

Countries can manipulate currency values for trade advantage. China's routinely accused of this, with reason, but the effect of the manipulation on trade balances may be overstated. This isn't the occasion for a discussion of monetary policy, but precedents could be found in the Asian financial crisis and the more recent Eurozone crisis, where bad monetary and fiscal policies allowed international monetary flows to destabilise national economies. The notion might be that a country could intentionally seek to use monetary policy to damage an opponent's economy, but that would require larger resources than any one nation possesses and a degree of covertness hard to maintain in the tightly knit financial community, where investment flows are scrutinized and tracked.

Currency manipulation as a tool of state power is of dubious utility, given its cost, uncertain effect and potential for backfiring. In the period between World Wars I and II, European nations attempted to leverage the gold standard, war debts and exchange rates to coerce other nations. Those efforts didn't work very well. The lesson that 'beggar thy neighbour' ended up beggaring all clarifies the risks and limited utility of economic warfare.

To explain China's actions, we can choose between a complex and convoluted strategy to inflict harm or a simple desire to gain economic benefit. The debt weapon appears to be imaginary, and exchange rate manipulation is better explained as an economic tool to promote exports rather than as a weapon. For financial and industrial activities, economic policy explains behaviour better than military strategy.

The goals of China's leaders are to keep the Communist Party in power (an increasingly difficult task in a country where very few people are communists), to catch up with and surpass the West in technology and wealth, and to assert China's central position in regional and global affairs. The state of China's economy probably precludes risky financial manoeuvres from consideration by China's leaders. China's own financial situation is parlous, given its local debts and problems with domestic consumption levels. Dumping debt to damage the US would destabilise the global economy and risk an economic conflagration that could consume the Communist Party, given the importance of strong economic growth in China for its continued rule. If we assume that China wants to dump its debt to damage the US, we must also assume that party leaders have an amazing and hitherto undisplayed tolerance for risk.

How useful is economic warfare in a global economy?

Moving beyond the specific case of China, the utility of economic warfare in an integrated global economy is open to question. The use of economic power to punish an opponent is constrained by interconnections and interdependencies. The term 'economic warfare' appeared with the onset of mass industrial warfare, when nations enlisted all elements of society for the fight. Economic warfare was easier to wage in a less-connected world, when national economies weren't as dependent on other nations. Before the 'globalisation' of the 1990s, nationally based industries were the main suppliers of goods in most countries, and national financial and monetary systems were less integrated with global markets. Classic economic warfare policies that restricted an opponent's access to raw materials, technology or money were more effective in that earlier time.

As economies become more connected, however, the ability to restrict access or manipulate markets is greatly diminished. In an interdependent economic environment, economic warfare, particularly as a covert, peacetime activity, will not work.[12] The US wrestles with this problem every time it uses unilateral sanctions, when the effect is more symbolic than harmful. Countries still engage in competition using trade and monetary policies, but those activities have become more difficult to conceal (or to use successfully) in an interdependent global economy that is governed by international agreements and is vastly more transparent than in the past. Sanctions are a tool of coercion and political influence, but they're not covert and they primarily affect the companies of one's own nation. Export controls are a tool of economic warfare, but they involve self-restraint intended to damage an opponent.

Economic warfare is a descendant of the scorched-earth tactics used by ancient armies, and of naval blockades that cut off trade and supplies of food or arms. More refined tactics appeared in the industrial era in the form of efforts to deny raw material needed for war production. That strategy made sense in a time when global trade was less extensive and less interconnected, and when European imperialism could make the home country's industries dependent on resources from remote territories. As national economies have become more integrated and global supply chains more extensive, the ability to restrict access to economic resources has diminished. Countries use embargoes and sanctions as means of coercion, but if there's one thing the US has learned it's that unilateral economic sanctions or embargoes do more to indicate displeasure than to inflict harm. Economic warfare works best when there is broad multilateral support.

Death by a thousand cuts from cyber espionage depends on several dubious economic assumptions, which also cast doubt on the general concept of economic warfare. The most important assumption is that, while the effects of cyber espionage or financial manipulation are marginal, they have a multiplier effect, creating greater damage than the actual dollar value of the losses would indicate. The multiplier effect is the philosopher's stone of modern economics, where an increase in spending leads to a proportionally larger increase in wealth and employment. If we regard the theft of intellectual property by cyber espionage as a form of disinvestment, advocates of economic warfare argue that there could be a similar multiplier effect. This argument collapses under the weight of improbabilities and conjectures about effect—if this scenario was true, China would be covertly competing against the US Federal Reserve Bank to manipulate the American economy using a much smaller pool of resources. Another assumption is that it's possible to restrict access to money, technology or raw materials in a global market where trade and finance are fungible and there are many alternative sources of supply. Economic warfare may be important for its political symbolism (such as sanctions against Russia for its attacks on Ukraine), and a useful indicator of political will, but with declining effect in a global economy.

For China, in any case, this raises the question of intent, and there's no compelling evidence that China's intent is to use espionage and financial manipulation for economic warfare leading to death by a thousand cuts. All economies have various degrees and kinds of inefficiencies that reduce income. Cyber espionage can be considered another investment inefficiency, produced by external causes. To say that America grows more slowly or is less wealthy as a result of cyber espionage is true, but for that to have strategic consequences requires dramatic assumptions about effect that are unsupported by evidence. There's clearly harm to national income and from the loss of military technology, and individual companies can be badly damaged, but that's not the same as fatal harm. The most important implication of cyber espionage isn't that China has a strategy of economic warfare, but that it has scant regard for internal rules and norms in the pursuit of its own self-interest.

Beijing's control over economic espionage

The degree and nature of control of the Chinese leadership over economic espionage is worth considering as part of an assessment of economic warfare. That Chinese leaders see cyber espionage as a source of advantage is obvious. The degree of order or direction they impose on it less obvious. The nature of Chinese espionage activities is a subject of serious debate. Earlier ideas about it, such as the 'thousand grains of sand' explanation (referring to the use of vast numbers of Chinese international visitors and students to collect intelligence), now seem inadequate to explain Chinese activities.[13] At this time, it seems safest to say that the Chinese state uses espionage against economic and technological targets, but that not all Chinese economic and technological espionage is state directed. We need to assess the extent to which Beijing permits Chinese actors to spy on foreign targets within generally understood political parameters, rather than guiding them.

The market for stolen commercial data in China mixes profit-seeking, strategy, *guanxi* (personal networks of influence) and corruption, but not in equal measure. An initial estimate is that there are four channels:

- officially sanctioned and directed cyber espionage
- People's Liberation Army groups and contractors who opportunistically find commercial data as they look for military technology and then sell it, or who have relations with local companies and support them
- companies doing the hacking themselves or hiring contract hackers to go after commercial targets
- independent hackers (although independent operators can be rapidly co-opted by the security services).

Cyber espionage is driven by self-interest and profit motives (and Chinese companies are also targets of cyber espionage by their domestic competitors), and is so far best seen as a mass of private activity that's subject to only limited central direction.

One way to think about intent is to ask whether President Xi could stop cyber espionage. His predecessors encouraged economic espionage and illicit technology acquisition by a broad range of official and private actors in China for military technology. This was very often targeted, but much was opportunistic and driven by the self-interest of a range of actors. Deng sanctioned illicit technology acquisition; Jiang sanctioned cyber espionage, but unleashed forces that any Chinese leader would find very difficult to control, given how important many Chinese think it is for their economic growth and given the close links of commercial cyber espionage to the nexus of corruption and political power at the centre of the Chinese state.

Until recently, the US has been unwilling to move forcefully against China over economic espionage. Some of this is explained by the reluctance of US companies to hurt relations with a country that possesses both a major market and a known inclination for retaliation against foreign firms that displease it. Trade officials reflect this unwillingness to engage on cyber espionage, and in any case existing trade law and processes are not well suited to dealing with industrial espionage activities so extensive as to challenge the structure of trade agreements. Nor do important allies support cyber espionage countermeasures. For example, Germany is much more dependent on the Chinese market and is unwilling to support action against espionage.[14] This unwillingness to engage China may involve miscalculation and underestimation by the US, Germany and others of the harm espionage does to their own economies, but even if there were significant pressure it would need to be sustained for a considerable period, given the political difficulties any Chinese leader would face in asserting control over cyber espionage.

If the Chinese leadership doesn't fully direct or control economic espionage, that has implications for Western policymakers as they attempt to constrain espionage.[15] A counterfactual argument would be to ask whether, if Xi directed Chinese intelligence agencies to stop spying, would all spying end? Xi may not see the necessity of enduring the pain that a dispute with regional military commands and economically powerful actors over cyber espionage would entail. Nor is there yet any reason to abandon the policy of technology acquisition from the West. The idea that someday it will be in China's interest to protect intellectual property assumes that Beijing has the ability to enforce such a policy and that it would apply it to foreign firms. Absent external pressure, there's no reason for China to stop, and it's possible that Western governments may not be willing to exert the degree of pressure required to change Chinese behaviour.

Given China's history, its commitment to the Western system of state relations is ambivalent. In combination with its desire to acquire Western technology to catch up to the West, this creates political conditions favourable for economic espionage. The incentive structure in China and the nexus among business, government and corruption encourages economic espionage and limits Beijing's control. China's inability and unwillingness to observe its international trade commitments is a serious problem, but it isn't warfare. Some of it has to do with the weakness of the rule of law in China and some has to do with Chinese official attitudes to Western norms, the legitimacy of which the Chinese question on a number of historical grounds (a mixed inheritance of Leninism and discontent with European imperialism). China is in the Western economic system, but not of it.

Not a new Cold War

Describing cyber activities by the US and China as a new Cold War in cyberspace is hyperbolic and inaccurate. The relationship between the US and China and the international environment for this relationship are very different from the Cold War, when relations and contacts with the Soviet Union were extremely limited and there was no economic interdependence or interconnection. There have been none of the threats, ideological challenges or proxy conflicts that characterised the Cold War.

The US has sought to avoid a military focus in its cybersecurity efforts. It has cast China's cyber espionage as a commercial matter (Treasury Secretary Lew has told China's President that cyberattacks are 'a very serious threat to our economic interests'). For example, the US indictments of People's Liberation Army officers for cyber espionage focused intentionally on trade and economic crimes[16] to avoid any implication that this was a military contest. China has never used 'force' (defined as acts of violence) against the US in cyberspace; it will use cyberattack against US military forces in any clash, but espionage isn't war—if it were grounds for war, the US would find itself at war with many countries. Both China and the US have implicitly avoided truly damaging attacks or military confrontation in cyberspace, each restricting its activities to espionage. Espionage isn't a crime under international law, and it's not in the US interest to make it so. Dealing with China's cyber espionage requires a sustained effort to construct norms and persuade China to observe them, to create consequences for Chinese actions, and to improve cyber defences in the interim.

This is a much more complex relationship than the Cold War. Managing the trajectory of US–China relations to avoid conflict will be difficult, and Chinese misconceptions about international affairs and American intentions only complicate the task. Similar misconceptions about economic warfare on the US side don't help to manage the relationship. China's best seen as the most assertive and the most potent of a number of new powers that challenge the existing international order and the American role in it. The long-term goal for the US and other Western nations is to bring China into the international 'system' of rules that govern state behaviour, and that means persuading it to get its 'cheating' in trade and in cyberspace under control. Some economic tools, such as sanctions, would be useful in applying pressure to China, but military force has very little utility.

Gigantic, secret conspiracies are a staple of pulp fiction. In practice, they're impossible to sustain on any grand scale. Belief in a Chinese grand strategy of economic warfare against the US assumes that beneath China's almost chaotic and hypercompetitive growth there's some hidden agenda, and that China could develop a secret plan to achieve it and keep the plan secret across four different leaders for more than 25 years.

The frequent references to a Chinese grand strategy reflect an ingenuous effort to explain Chinese actions. They also reflect the deep unease China's growth has created, given the discrepancy between its promises of a peaceful rise and its acts of assertive self-interest. When the Chinese accuse the US of having a grand strategy, it amuses most Americans. The US doesn't have one, but it does have consistent interests and a common approach to problems shaped by its ideology and politics. The same is true for China.

We can impose an artificial order on a complex international problem by ascribing Chinese actions to economic warfare, but the reality, unfortunately, is much more difficult. In struggling to define conflict in an era in which the use of force is more expensive, more dangerous, and therefore less often resorted to by states, the war metaphor can be appealing, but it's not a helpful guide for policy. We could argue that China is simultaneously attempting to build its economy and weaken opponents, but that would involve damaging its major markets and sources of finance.

If our choice in explaining Chinese behaviour is between commercial motives and deliberate geopolitical strategy, the former better explains actions and events.

Notes

[1] Australian Broadcasting Corporation, *The threat of cyberwar*, 5 February 2014, www.abc.net.au/pm/content/2013/s3938870.htm.

[2] *Harmony & chaos: the principles of China's unrestricted warfare*, www.isn.ethz.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=162588&contextid774=162588&contextid775=162582&tabid=1454240802.

[3] An extensive literature examines the changing utility of the use of armed force. Examples are found in the works of Keith Krause, Andrew Bacevitch and Colin Gray, among others.

[4] George Shambaugh defines economic warfare as seeking to weaken an adversary's economy by denying the adversary access to necessary physical, financial and technological resources or by otherwise inhibiting its ability to benefit from trade, financial and technological exchanges with other countries.

[5] A RAND review of Western economic measures against the Soviet Union found similarly disappointing results. Becker, *Economic leverage on the Soviet Union in the 1980s*, www.rand.org/content/dam/rand/pubs/reports/2009/R3127.pdf.

[6] Larry M Wortzel, *The Chinese People's Liberation Army and information warfare*, Strategic Studies Institute, US Army War College, 2014, www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1191.

[7] Ian Steadman, 'Reports find China still largest source of hacking and cyber attacks', *Wired*, 24 April 2013, www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet; Thomas Brewster, 'InfoSec 2013: China is "biggest source of advanced cyber attacks"', *TechWeek Europe*, 23 April 2013, www.techweekeurope.co.uk/news/infosec-2013-china-cyber-attacks-fireeye-verizon-reports-114144.

[8] Marc Levinson, *'Hollowing out' in US manufacturing: analysis and issues for Congress*, Congressional Research Service, 15 April 2013, http://fas.org/sgp/crs/misc/R41712.pdf.

[9] David Stringer, 'China's rare earth toxic time bomb to spur mining boom', *Bloomberg*, 4 June 2014, www.bloomberg.com/news/2014-06-03/china-s-rare-earth-toxic-time-bomb-to-spur-12-billion-of-mines.html; Keith Bradsher, 'China to tighten limits on rare earth exports', *New York Times*, 28 December 2010, www.nytimes.com/2010/12/29/business/global/29rare.html?pagewanted=all.

[10] Helen Rumbelow, 'Pentagon prepares for economic warfare', *The Australian*, 20 August 2011, www.theaustralian.com.au/news/world/pentagon-prepares-for-economic-warfare/story-e6frg6so-1226118380617.

[11] Min Zeng, 'China plays a big role as US Treasury yields fall: record Chinese purchases of treasurys help explain US bond rally', *Wall Street Journal*, 16 July 2014, http://online.wsj.com/articles/china-plays-a-big-role-as-u-s-treasury-yields-fall-1405545034.

[12] Percy W Bidwell, 'Our economic warfare', *Foreign Affairs*, April 1942, www.foreignaffairs.com/articles/70162/percy-w-bidwell/our-economic-warfare.

[13] Peter Mattis, 'The Analytic Challenge of Understanding Chinese Intelligence Services', Central intelligence Agency, *Studies in Intelligence*, September 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf.

[14] An attitude only reinforced by the Snowden revelations. Interviews with German, EC and European officials.

[15] Nigel Inkster, Chinese Intelligence in the Cyber Age, *Survival* (IISS), September 2013, http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-february-march-2013-3db7/55-1-05-inkster-936c.

[16] Interviews with Department of Justice officials.

China's emerging cyberpower: elite discourse and political aspirations

Simon Hansen

Executive summary

On 27 February 2014, President Xi Jinping announced on state-run CCTV that efforts should be made to build China into a 'cyberpower' (*wangluo qiangguo*). China's elites have given particular prominence to cyber issues in recent months, culminating in the establishment of the Internet Security and Informatisation Leading Small Group (ISILSG). How China's leaders conceive of cyberpower and what they choose to make of it has local and global implications, not least for Australia. For such a significant announcement, it's surprising that very little analysis has surfaced.

Perceptions of a 'China cyber threat' abound, and Beijing's declared efforts to build 'cyberpower' have no doubt caused anxiety in strategic circles. In Australia, alleged Chinese cyberespionage activities have garnered high-profile attention. A 2014 Lowy poll found that just over half of all Australians see cyberattacks from other countries as a critical national security threat.[1] The chief goal of this paper is to help Australian and other practitioners of statecraft adapt their own policies to how China thinks about cyberpower.

The establishment of the ISILSG reveals two overarching trends in China's future cyber policymaking: a consolidation of political leadership over cyber issues, and framing the internet as part of China's national strategy. While the effects of the new governance model of the Chinese Communist Party (CCP) are yet to be seen, there's likely to be more coordination of China's complex cyber policy apparatus, and the drafting and implementation of a national cybersecurity strategy.

Analysis of key policy announcements has revealed four basic assumptions held by Beijing about the internet as an instrument of power.

The most convincing theme in China's thinking about cyberpower is that CCP elites are preoccupied with maintaining social stability and the control of public opinion. China's leaders were at first discomforted by the internet—a medium for dissenting views and political risk. Despite the risk of protest fermenting online and materialising offline, the political elites have shown remarkable ingenuity in making the most of the internet, bringing benefits to hundreds of millions of Chinese while shoring up the regime's longevity. Concern about social volatility is evident in China's discourse on cyberpower. At the Third Plenary Session—China's foremost platform for reform—Xi Jinping declared that internet and information security involves both 'national security' and 'social stability'.[2]

The second theme in the discourse is a focus on China's economic growth. Considering that China's rise and the CCP's legitimacy are based on sustained economic development, as it brings individual prosperity and national rejuvenation, it's no surprise that the internet is seen by elites as a tool to aid growth. At the announcement of the ISILSG, Xi Jinping stated that the strategic plan of building cyberpower is towards the goal of building network infrastructure, enhancing indigenous innovation, and developing a comprehensive information economy.[3]

The third theme is that China's international cyber strategy has become increasingly sophisticated. China's approach has traditionally been reactive, focused on countering what China perceives as a prevailing international norm of a 'China cyber threat' (*zhongguo wangluo weixielun*). In order to discredit allegations, officials claim that China, too, is a victim of attacks, while simultaneously counter-accusing other nations, particularly the US, of cyberattacks. More recently, China's strategy has become more proactive, calling for cooperation and advancing its own agenda in international cyberspace discussions. This is promising, as China has signalled that it's open to discussions and potential cooperation. But it's also worrying, as China's agenda for the internet is essentially incompatible with Australia's view.

The fourth theme is that the internet features squarely in China's broader great power ambitions. In an era of rapid transformation, there's no modern-day technological revolution more significant for sustaining China's rise than the internet. Already the internet has diffused power to the country's masses, providing avenues for expression and rising affluence; somewhat paradoxically, it has also concentrated the organisational strength of the state. These trends, if properly managed, will continue to underwrite China's rise. Great powers are technologically advanced powers, and a key priority over the next few decades will be to further develop interconnected information resources that

pave China's path to modernity. 'China Dream', a popular leadership slogan, is the most prominent expression of China's ambition for great power. At the announcement of the ISILSG, Xi Jinping declared that building cyberpower is part of China's 'China Dream' goals.

Four policy implications lead from the themes outlined here. The most pressing need is for Australia to develop a substantive cybersecurity dialogue with China, particularly since Beijing has framed cybersecurity as a top-level strategic issue. There's also a requirement for us to think more deeply about our own 'cyberpower'. The main lesson is that Australia should publish a new Cyber White Paper to outline our international policy in the light of recent developments, to assure other states of our strategy, and to advance our own agenda in cyberspace discussions. There are also other implications, including reconsidering Australia-bound state-owned enterprise investment guidelines and Australia–China cyber relations in the context of the US alliance.

Introduction

In recent months, concern about strategic competition in cyberspace has heightened. In Washington, there's mounting unease about a China 'hacking threat'; in Beijing, the US has been labelled a 'mincing rascal', guilty of unfettered global surveillance. Tensions flared most recently in May 2014, when the US Department of Justice indicted five People's Liberation Army (PLA) officials for stealing trade secrets. Both nations have directed accusations against each other in sporadic broadsides, and their cybersecurity concerns are likely to be irreconcilable in the short term. This is despite high priority given to cybersecurity cooperation at the Sunnylands summit meeting of presidents Barack Obama and Xi Jinping in June 2013 and on the sidelines of The Hague Nuclear Security Summit in March 2014. In July 2014, the US continued to broach its cybersecurity concerns at the Strategic and Economic Dialogue in Beijing.

International pressure has been matched by China's domestic policy attention. The CCP gave top-tier policy consideration to cybersecurity at the November 2013 Third Plenary Session—China's principal platform for reform—and the March 2014 National People's Congress—the nation's top legislature. China views the control of the internet as a tool of comprehensive national power, as it's critical to social stability and economic development. Strategic thinking about power based on the internet is a relatively new area of statecraft for China, but policy leaders increasingly see the internet not as a domain to tame and censor, but an indispensable part of the party-state's grand political design.

The most potent symbol of China's new thinking on cybersecurity was on 27 February 2014, when Xi Jinping declared himself head of the Internet Security and Informatisation Leading Small Group (ISILSG). During the meeting aired on state-run CCTV, Xi announced that 'efforts should be made to build China into a cyberpower.' His authoritative stamp as leader of this group, along with deputies Premier Li Keqiang and Politburo Standing Committee member Liu Yunshan, suggests that Chinese Communist Party (CCP) elites are consolidating command of a fractured cybersecurity arena. The announcement symbolised Beijing's aspirations, officially declaring cyberpower as part of China's emerging national strategy.

This paper examines the establishment of the ISILSG and other major Chinese policy announcements to identify key themes in China's discourse on cyberpower. Analysis of these policy sources is important, as it reveals basic assumptions held by Beijing about the internet as an instrument of power, giving context to China's behaviour in cyberspace. Equally important, policy statements can be seen in the context of the elites' broader thinking about China's rise, as cyberpower is regarded as part of China's grand strategy. If grand strategy is about aligning a nation's capabilities to achieve its political intentions, then this paper goes some way in analysing China's grand strategy, as it explores how China's leaders conceive of the internet as a tool to achieve their desired outcomes. Most importantly, the chief goal of this paper is to help Australian and other practitioners of statecraft adapt their own policies to how China thinks about cyberpower.

Deciphering what Chinese policy statements are signalling is problematic. While it's clear that cyber issues are being raised on the policy agenda, it's uncertain what China's leaders truly think of cyber capabilities as an instrument of national power to achieve political ends, or even whether that's a topic of discussion in Zhongnanhai. Of course, policy statements could be constructed by political elites to deliberately obscure their intentions. China, being a relative newcomer to strategic thinking about cyber matters—when compared to the US—doesn't gain from displaying strength willingly. Most importantly, public statements don't represent

Chinese thinking on cyberpower in its entirety. Classified and unmentioned activities form a significant part of China's cyberpower, particularly the military applications of cyber capabilities. However, little emphasis is given here to People's Liberation Army (PLA) doctrine, as it has been covered well by other authors, and this paper has a primary interest in analysing recent open-source policy announcements.

This paper first analyses key phrases used by Xi Jinping at the announcement of the ISILSG, outlines two overarching trends in China's strategic approach to cyber policy, and identifies four key themes in China's thinking about cyberpower. It argues, perhaps unsurprisingly, that China's discourse on cyberpower is mainly domestically oriented and focused on maintaining social stability and advancing economic growth. These dual imperatives continue to guide most, if not all, policy formulation in China. In addition to domestic political concerns, there are two other themes in China's broader cyberpower discourse. First, China has become more energised in competing for influence in international cybersecurity debates. Second, China's discourse on cyberpower reflects an emerging trend of self-confidence and national rejuvenation within China as it comes to terms with its power under Xi Jinping's leadership. This paper concludes by outlining four implications for Australian policymakers.

Cyberpower discourse at the ISILSG announcement

States can wield enormous control over information networks not just by controlling physical infrastructure but by using policies that control information through censorship, drive innovation through investment in new technologies, or develop offensive capabilities by establishing military cyber commands. Put simply, the control of information is a constitutive element of state power. To gain a better comprehension of China's thinking about cyberpower, key phrases articulated by Xi Jinping during the announcement of the ISILSG deserve attention.

'Without informatisation, there is no modernisation'(*meiyou xinxihua jiu meiyou xiandaihua*)

In 2006, China's State Council and Central Committee released the national Informatisation Development Strategy 2006–2020, which set out guidelines for China to take advantage of the transformative effects of IT. At the centre of the strategy is the concept of 'informatisation' (*xinxihua*)—the process through which information technologies, particularly the internet, are used to further China's socioeconomic development. While Madame Fu Ying, the chairperson of China's foreign affairs committee, has conceded that the term's difficult to explain ('This is a word we made up; we don't know how to express this'), informatisation is fundamentally the use of IT to support China's modernisation and brace the country's rise to great power status.[4] As the *2013 Informatisation Blue Book* published by the Advisory Committee for State Informatisation notes, it's a 'strategic element in China's modernisation process'.[5]

The concept of informatisation has been previously applied in other areas of Chinese policy—specifically, military affairs and domestic security. In the PLA, informatisation was outlined clearly in Hu Jintao's contribution to military thought, the 2004 'New Historic Missions' (*xinde lishi shiming*) doctrine. These missions, as James Mulvenon argues, 'derived in large measure from Hu Jintao's overall ideological guidance on "scientific development"' (*kexue fazhan guan*), widely considered his signature policy.[6] Recently, China's 2013 white paper on national defence pointed out that changes in the form of war from mechanisation to informatisation are accelerating, and major powers are vigorously developing new and sophisticated technologies to ensure superiority. In late August 2014, while presiding over a meeting with the Political Bureau of the Central Committee, President Xi Jinping spoke about the challenges and opportunities arising from global military innovation and stressed the need to reshape China's military strategy with informatisation at its core.

Informatisation has also featured prominently in China's domestic security authorities, such as the Ministry of Public Security. Peter Mattis explains that the 'process of building up technical surveillance capabilities into police operations is known as "public security informatisation construction" (*gong'an xinxihua jianshe*), and has been a pillar of Ministry of Public Security modernisation since at least 2008.'[7]

The concept's application to cybersecurity is a further evolution of China's thinking about its modernisation of state security functions and the application of information and communications technology. Informatisation can be taken to mean the use of technology to strengthen China's capabilities and increase state power through a comprehensive, interconnected security apparatus, not too dissimilar to Western ideas about the revolution in military affairs, although within China the concept's more readily applied to areas outside the military domain.

'Without internet security, there is no national security' (*meiyou wangluo anquan jiu meiyou guojia anquan*)

In China's discourse on cybersecurity, internet security is complementary to informatisation. Apart from purely technical network security and legal aspects, the concept is more widely understood as the CCP's right to control content.

'Internet security and informatisation are two wings of the same bird and two wheels of the same engine' (*wangluo anquan he xinxihua shi yitizhiyi qudongzhishuanglun*)

Taken together, informatisation and internet security underline the intimate relationship between development and security in China's thinking about cyberpower. This relationship is reasonably clear: as China builds information networks, it needs to also build the capacity to secure them. This connection has featured in other areas of policy discourse. In March 2014, for instance, Xi Jinping borrowed from Greek mythology when he called the development of nuclear energy 'like Prometheus who gave fire to humanity and opened up a bright future for mankind', but that 'bright future is overshadowed by dark clouds, and there is a need for equal emphasis on development and security.'[8] Securing information networks is no small task for China. One commentator, Zhang Hong of the State Information Centre, has recognised the contradiction between development and internet security in China's cyberpower: 'The more the developed the network, the more security issues arise.'[9]

There's also a second level of the development–security relationship in China's thinking. Development is a rationale concerned with overcoming China's perceived 'backwardness' and increasing its security vis-a-vis other states. Informatisation implies a strengthening of China's material base, increasing the power of the state under the ruling elite, and thereby ensuring security. Leaders of other developing nations have expressed this same logic. Alexander Hamilton, one of America's founding fathers, wrote in 1791 that the 'independence and security of a country appear to be materially connected to the prosperity of its manufactures'.[10] At this level, China's development goals are essentially national security imperatives.

'Efforts should be made to build our country into a cyberpower' (*nuli ba zhongguo jiancheng wangluoqiangguo*)

Cyberpower in China's context is the long-term national ability to realise both informatisation and internet security, to modernise China with far-reaching information networks and to securely control those networks. Dual efforts to develop and secure China's internet will allow political elites to use the internet to achieve their objectives and attain national aspirations. Joseph Nye offers a useful definition that's consistent with China's thinking, describing cyberpower as the 'ability to obtain preferred outcomes through the use of interconnected information resources'.[11]

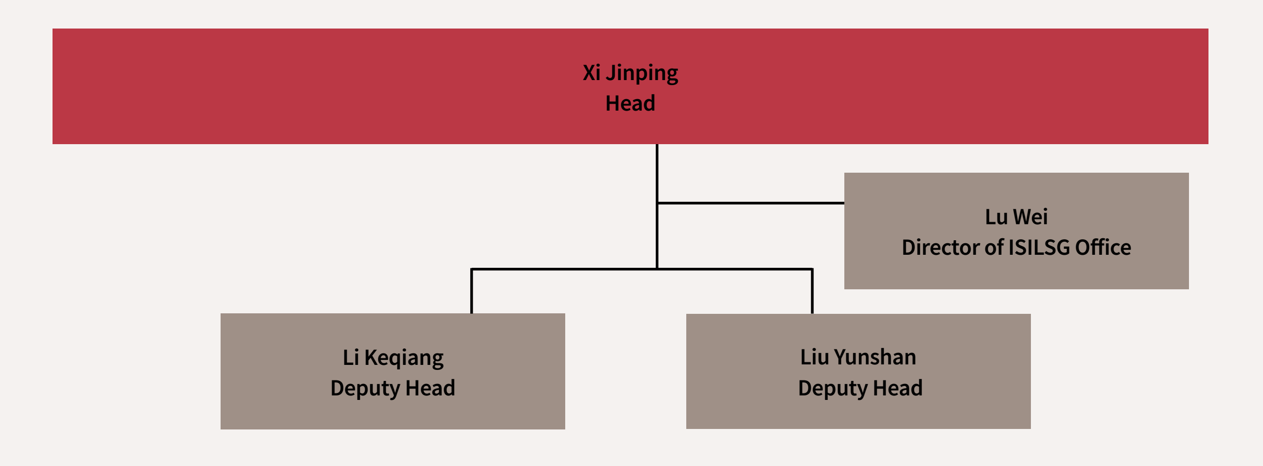
Overarching trends in China's strategic approach to cyber policy

The establishment of the ISILSG, as the symbol of China's emerging cyberpower, reveals two overarching trends in China's thinking: consolidating political leadership over cyber issues, and framing the internet as part of China's national strategy.

Consolidation of domestic cyber policy

China's domestic cyber policy landscape remains splintered. A number of stakeholders compete for influence, including CCP offices, government ministries, the PLA, academia and critical infrastructure operators. The establishment of the ISILSG is an acknowledgement by China's elites of the challenge of cyber governance, and an admission that previous approaches aren't working. The group starts with a fair bit of experience: deputies Li Keqiang and Liu Yunshan have previously drafted major cyber policies in the former, low-profile, Information Security Small Group. The group's office director, Lu Wei, is also the head of the State Internet Information Office (SIIO), China's lead internet regulatory body, (now known as the Cyberspace Administration of China). While the effects of establishing the ISILSG are yet to be seen, there's likely to be more coordination across government in the future.

Figure 1: Internet Security and Informatisation Leading Small Group (ISILSG) (*wangluo anquan he xinxihua lingdao xiaozu*)



Ma Kai Vice Premier State Council	Wang Huning CCP Policy Research Office	Liu Qibao Director Central Propaganda Committee	Fan Changlong Vice Chairman Military Commission	Meng Jianzhu Central Politics and Law Reform Commission
Li Zhanshu Head of the General Office of the CCP	Yang Jing Secretary General State Council	Zhou Xiaochuan Governor of People’s Bank of China	Wang Yi Minister of Foreign Affairs	Fang Fenghui PLA Chief of Staff
Lou Jiwei Minister of Finance	Cai Wu Minister of Culture	Yuan Guiren Minister of Education	Miao Wei Minister of Industry and Information Technology	Guo Shengkun Minister of Public Security
Xu Shaoshi Chairman, Development and Reform Commission	Wang Zhigang Secretary, Ministry of Science and Technology	Cai Fuchao Director, State Administration of Radio, Film and Television		

Note: With the exception of the executive, the members’ names are yet to be released by official channels. Liang Fulong, ‘Zhongyang wangluo anquan he xinxihua lingdao xiaozu chengyuan mingdan 12 zhengfu guo ji jianzhi shen gaizu’, *Guancha*, 28 February 2014, www.guancha.cn/politics/2014_02_28_209672.shtml.

Authoritative commentators in the *People's Daily*, such as Wang Xiujun, Vice-Director of the SIIO, have admitted that China's cybersecurity governance needs unified leadership to avoid overlapping governance responsibilities. This can be achieved by moving away from the existing 'nine-dragon' management of cyber policy to one centralised authority under the ISILSG.[12] In China's policymaking sphere more broadly, there's been a growing trend of political leadership consolidation under the CCP's General Secretary, Xi Jinping (who's also the country's president). The National Security Commission consolidated the leadership of China's vast security agencies in November 2013. Meanwhile, the Central Leading Group on Comprehensively Deepening Reforms is quite possibly the largest ad hoc leadership mechanism in the party's history. Whether the CCP's new governance model will be able to better macro-manage China's diverse challenges remains an open question.

The internet in China's national strategy

The other overarching trend in the establishment of the ISILSG is that the internet's being progressively framed as an integral part of China's national strategy. In recent years, economic instability has challenged the CCP's performance-based legitimacy, and social instability brought about by the internet's ability to disseminate information has made elites hyperaware of China's national problems. In many ways, the internet's seen as both a panacea and a problem, and the ISILSG is likely to be preoccupied with integrating the net into its national strategy as a tool to neutralise dissent and aid economic growth.

The internet also serves a more ambitious aim in China's national strategy: China's rejuvenation as a great and predominant regional power. International relations today have a transformative technological dimension; to compete with other states in an economic–political contest, rising bureaucratic states are required to adopt emerging technologies or invent new ones. Technology will continue to determine the hierarchy of the international society of states, and the expectation that other states will innovate will push nations to do the same, producing a development–security race for superiority. The invisible hand in China's desire for cyberpower is a fear that, without embracing the internet, it will sit stagnant in the ranks of the international order, its once immutable rise will look increasingly shaky, and its vision of great power prestige will be lost.

In the short term, Beijing's likely to announce—at least internally—a national cyber strategy that places cybersecurity squarely as a national strategic issue. Xu Lei, a Hong Kong academic, commented in the *People's Daily* after the announcement of the ISILSG that 'formulating a national cybersecurity strategy has become an urgent task.'[13] In the medium term, there's likely to be further consolidation of party control over online media and internet companies as the elites come to grips with the challenges and opportunities arising from more than a billion Chinese logging on. In the long term, there's likely to be increasing sophistication in using the internet for state responsibilities outside of the areas of national security, such as e-government services.

Social stability—'a clear and bright cyberspace'

China's internet is flourishing. According to the most recent statistical report on internet development in China, there are around 618 million internet users.[14] China has a vibrant online society, for most Chinese the internet is a social portal, and there's been large growth in instant messaging services such as WeChat and online forums such as Weibo. The CCP gains significantly from increasing the nation's access to the internet. Access sparks individual self-confidence and commercial ambitions, and provides a sounding board for officials to identify destabilising oscillations between anti-government protest at one pole and nationalistic impulses at the other.

Here lies the dilemma: the result of increased internet adoption is more dissenting voices, and some defy the party's right to control information. 'The internet is like a magic engine, and it has helped my writing erupt like a geyser,' said Nobel Laureate and dissident Liu Xiaobo.[15] Voices like Liu's—if sufficiently organised—have the potential to challenge the party's legitimacy as the nation undergoes immense change. That's why China's internet is thoroughly managed. It's likened to a birdcage, where there's space to converse and even criticise but freedom is illusory. In 2013, China connected just shy of 150,000 people to the internet *every day*. It's no surprise that policy announcements about cyberpower are married to statements about maintaining social stability.

At the Third Plenary Session of the 18th CCP Central Committee in November 2013, President Xi Jinping described 'The Decision on Several Important Issues of Comprehensively Deepening Reform', declaring that internet and information security involves both 'national security' (*guojia anquan*) and 'social stability' (*shehui wending*), and is China's 'new comprehensive challenge' (*xinde zonghexing tiaozhan*).[16] This was a significant policy development. It was the first time that internet security had been flagged at such a high-level forum. In addition, the issue was flagged as a major priority, positioned eighth on the policy agenda, between corruption and the establishment of the National Security Commission. Internet security is viewed mainly as a social stability issue, affirming the party's political fixation on controlling public opinion.

The leadership's preoccupation with maintaining stability has been exacerbated by the spread of the internet. One instance of social instability was the public uproar following the 2011 Wenzhou train crash, in which 40 people were killed. Because of the online uproar, then Premier Wen Jiabao had no choice but to cave in to public pressure and pledge to unravel the corruption that, in the public's eye, caused the wreck. That the premier was manipulated by online pressure isn't a comforting sign for the political elites. Ironically, Wen would later become the target of online protest against corruption after his own family's financial accounts were leaked.

At the February 2014 announcement of the ISILSG, elite discourse on social stability continued. President Xi Jinping stressed the need to 'promote positive energy' (*chuanbo zhengnengliang*) and make a 'clear and bright cyberspace' (*qinglang de wangluo kongjian*). These phrases are noteworthy: they're an admission by the government that the challenges presented by domestic issues, such as corruption and pollution, do coalesce online, cause palpable instability, and ultimately result in significant political risk—risk that needs to be mitigated by promoting agreeable opinions to support the CCP.

The party's interest in preserving social stability can be seen in its own online activity. Of all the government microblog activity on Weibo, 37% is carried out by the Ministry of Public Security—China's principal internal security authority.[17] Widespread efforts have been made to promote a 'positive energy' culture online. The *wumaodang,* or 'fifty-cent gang', are so called by their critics because, for every favourable online post they write to support the government's line, they're paid the equivalent of 50 cents. The role of Liu Yunshan as deputy of the ISILSG is testament to the elites' view of the internet as a domain for promoting a culture of 'positive energy'. Liu is a cultural thought leader and propaganda lynchpin in the CCP, and his position shows how important the party thinks it is to promote its brand in cyberspace.

In recent months, cybersecurity discourse to maintain social stability has been matched by political action. A growing number of influential voices, such as the 'Big Vs' (popular microbloggers such as Charles Xue), are positioned to sway millions of followers and undermine the party-state's approach to information control. Lu Wei, chief of the SIIO, held a China internet forum for bloggers in August 2013 to bring these disparate voices into the CCP orchestra. At the event he called for Big Vs to take responsibility, abide by seven 'bottom lines' (*qitiao dixian*—essentially an online code of conduct) and shape debates that protect state interests and social order. The control of information to maintain social stability has become more nuanced and effective, moving from public arrests to more sophisticated techniques, such as precluding choices and shaping online debates. One study by a Chinese social media analysis firm shows that the number of posts by influential bloggers dropped 11.2% after the most recent anti-rumour campaign in late 2013.[18] Online, self-discipline is the tacit rule.

In early 2014, efforts to promote social stability through the use of the internet heightened. Starting in April, the SIIO launched the 'Cleanse the web anti-pornography' campaign to remove 'obscene' content.[19] Crackdowns are ostensibly targeted at pornography but serve many purposes, including quelling online rumours—particularly speculation about public officials such as former Politburo Standing Committee member Zhou Yongkang, who's under investigation for corruption. The popular portal Weibo became a noteworthy scalp in the government's online campaign when parent company Sina was fined for 'indecent content' and was stripped of publication licences essential for its operations.[20] As a final insult, Sina was forced to apologise publicly. In August, the power of the SIIO has increased under the so-called 'the WeChat articles', where strict rules are imposed on instant messaging media—such as authenticating your online identity. In coming years this trend will continue, as state regulation perpetually chases the adoption of new media.

The main theme in China's thinking about cyberpower is a concern about social instability. So far, the CCP has prevented the internet being used as a viable tool for meaningful political opposition. Despite the risk of protest fermenting online and materialising offline, political elites have shown remarkable ingenuity in making the most of the internet, bringing benefits to hundreds of millions of Chinese while maintaining stability. There's significant tension for the party between encouraging individual aspirations and simultaneously controlling those tendencies. It's likely that China's thinking about cyberpower will continue to include efforts to balance this central contradiction.

Economic development—innovation, infrastructure and the information economy

The second theme in China's discourse on cyberpower is the CCP's preoccupation with economic growth. China's national power is mainly a result of its rapid economic growth over the past few decades, as the country continues to convert its vast resources into growing influence. For China's elites, the most obvious intention is to continue this growth trajectory, as it brings influence over domestic constituents and clout in the international system. This intention has been reflected in China's cyberpower discourse.

In his work report at the National People's Congress in March 2014, Li Keqiang outlined the ability of the internet to increase domestic consumption, transform the economy (particularly the banking sector) and drive innovation-led economic growth. Similarly, at the establishment of the ISILSG in February 2014, *Xinhua* gave this analysis:

> The strategic plan of building cyberpower is towards the goal of building network infrastructure, enhancing independent innovation, developing a comprehensive information economy.[21]

Taken together, the policy focus on infrastructure, innovation and the information economy illustrates the importance that China's elites attach to sustaining economic development in their thinking about cyberpower. The most politically endorsed priority is innovation—the ability to turn ideas into economic growth, and the vital sign of a nation's soft and competitive power.

Innovation has become Xi Jinping's and Li Keqiang's watchword for promoting China's economic growth, and it's a critical component of cyberpower. At a high-level meeting, Xi told leading scientists and engineers that 'science and technology are the foundation of national strength and prosperity, and innovation is the soul of national advancement.'[22] He also commented that 'we should follow the strategy of innovation as an impetus for development.' Li has made parallel statements, saying that 'China will strive to make innovation a driving force of the country's economic upgrading.'[23]

For the rest of the world, the most worrying consequence of CCP attention to innovation is China's alleged widespread 'cybertheft' campaign. In the quest to boost international competitiveness and reduce gaps in science and technology research, China is alleged to have engaged in widespread economic cyberespionage. Reports by cybersecurity companies Mandiant (*APT 1*) in 2013 and Crowdstrike (*Panda Putter*) in 2014, and an indictment by the US Department of Justice in May 2014, accuse PLA officials of stealing intellectual property from US companies. Stolen data was then supposedly given to Chinese companies for their own advantage, increasing the international competitiveness of China's national enterprises and moving China's economy up the value chain.

Indigenous innovation, particularly in the technology sector, has garnered significant political support. Xi Jinping has commented, in techno-nationalist fashion, that 'to build cyberpower, China needs its own technology, excellent technology.'[24]

There are three major political drivers behind China's push for innovation. The first is outlined in the State Council's 12th Five-Year Plan on National Emerging Industries of Strategic Importance: high-tech industry will contribute a significantly higher proportion of national GDP by 2020. Essentially, new technologies will continue China's economic growth trajectory.

The second driver of indigenous innovation is deep suspicion within China about reliance on foreign companies' IT. China's currently reviewing companies such as IBM, which sell high-end servers to China's government agencies, as a supply-chain threat. In some cases, suspicion is warranted, as allegations emerge about US intelligence agencies installing backdoor surveillance tools in technology companies' products, such as Cisco Systems' routers and Microsoft's Windows 8 operating system. Political demands are growing to free China's critical IT systems from foreign-made technology and replace them with indigenous products.

The third driver of indigenous innovation is great-power competition. China has recently moved to exclude foreign companies as a backlash against American accusations about China's cyberespionage activities. International firms have now become trapped in US–China diplomatic disputes. The SIIO has threatened to block foreign companies from selling technology products if those products fail to pass a new 'cybersecurity vetting system'. Meanwhile, the Chief Engineer at the Ministry of Industry and Information Technology, Zhang Feng, has spoken publicly about developing an indigenous Linux operating system to compete against Windows—a measure supported by Fang Binxing, the 'Father of the Great Firewall'.[25] The *China Youth Daily*, a state-run newspaper, has accused Cisco of 'carrying on intimately with the US government and military, exploiting its market advantage in the Chinese information networks'.[26] China is arguably using political fallout to boost its national companies in direct competition with foreigners. This campaign could foreshadow a new and worrying era in US–China relations and international trade policy.

Investment in IT infrastructure is just as important in China's thinking about cyberpower. Concerns about the consequences of an investment binge are outweighed by the perceived benefits. Researchers at the University of Texas and the Chinese Academy of Social Sciences calculated that from 1990 to 1999—the first decade of China's telecommunications boom—connecting phone services to Chinese citizens contributed two percentage points to China's growth rate.[27] While that contribution shrank a decade later to only half a percentage point, China's telecoms are onto the next strategy, building 'Broadband China', which is seen as the next driver of GDP growth. The government plans to invest 2 trillion yuan (A$341 billion) to improve the country's broadband infrastructure by 2020. The aim, according to Shang Bing at the Ministry of Information and Industry, is to take the entire population online. Xi Jinping at the ISILSG affirmed this mission when he called for 'basic, universal network infrastructure' as a critical component of cyberpower. Internet infrastructure is a growth driver. Given the CCP's attention to growth, part of domestic cyber policy will remain fixated on delivering broadband services.

Announcing the ISILSG, Xi Jinping said that the 'strategic plan of building cyberpower proceeds with the comprehensive development of the information economy'. China's information economy is not only new IT industries, but also the use of IT to improve all aspects of the economy. 'Information technology has not only created a powerful information industry, it has transformed China's entire economic model,' said Zhang Hong, director of informatisation research at the State Information Centre.[28] ASPI's International Cyber Policy Centre rightly acknowledges that 'the potential for China's population to engage in the digital economy is enormous.'[29] China's aspirations for a strong information economy, like its aspirations for innovation and infrastructure, can be seen as part of broader concerns about the need for growth and development to underwrite China's rise to great-power status.

Sustained growth has become a difficult proposition, in the light of the structural challenges facing China's economy. China has to move from export-oriented growth to growth in domestic consumption and must try to avoid the middle-income trap faced by developing nations. Chinese elites see innovation, infrastructure and the information economy as a way for the country to avoid those pitfalls, continue its seemingly inexorable economic growth, and ultimately become a cyberpower.

China's international cyber strategy—from counter to control

In their thinking about cyberpower, China's elites have shown serious interest in shaping the international system. China's international cyberpower strategy can be seen as having two distinct stages. Traditionally, its approach has been reactive and focused on countering what it perceives as a prevailing international norm of the 'China cyber threat'. In order to discredit allegations against China as a cyber threat, Chinese officials claim that China *too* is a victim of attacks. A number of semi-authoritative sources have also counter-accused other nations, particularly the US, of cyberattacks and even 'cyber-hegemony'. The second stage is more recent and more aspirational. China's international cyber strategy has become more proactive, calling for cooperation and advancing its own agenda in international cyberspace discussions.

'It is ironic', starts one *Xinhua* article, 'that China, as the largest victim of cybersecurity threats, has suffered groundless accusations over hacking other countries'.[30] When facing foreign accusations, China has historically cast itself as the victim. This goes as far back as the defeat of the Qing dynasty at the hands of the British Empire during the First Opium War, and the first of the unequal treaties, the Treaty of Nanking. When charged with state-sponsored cyberattacks, the Ministry of Foreign Affairs has followed formulaic responses, denying allegations and claiming that it, too, is a victim 'confronted with the grave threat of cyber attack'.[31] At the Bo'ao Forum in April this year, Ministry of Foreign Affairs cyber coordinator Fu Cong raised concerns about a small number of countries monopolising key technologies that enable them to violate others' national sovereignty.[32] China identifies closely with what it perceives as the weaker side of the 'digital divide' between developing and developed nations, which are accused of building the internet to serve their own interests.

China's concerns about being a victim of cyberattacks are in many ways justified. The *2013 Network Security Report* published by China's Computer Network Emergency Response Team claimed that 61,000 computers were controlled through backdoors from outside China, and that 30.2% of those attacks were linked to US servers, although it didn't indicate whether the attacks could be attributed to the US Government.[33]

While there's a genuine concern among China's elites about cyberattacks, playing the victim serves a broader strategic objective. First, China is able to discredit accusations directed against it, because it suffers the same vulnerability. Second, China can justify its own cyberattack activities (which it assures other states don't exist) as more or less acceptable in state-to-state behaviour, because China suffers from attacks that, understandably, require retaliation.

Counter-accusations against foreign states, especially the US, accompany policy statements of victimhood. If identifying as the victim is about undercutting the international 'cyber threat' narrative against China, counter-accusations are used to reframe China's major strategic rival, the US, as the narrative's antagonist. In the aftermath of the Department of Justice indictment against Chinese cyber theft, the Chinese Government published *The United States' global surveillance*. According to the report's foreword:

> The United States' spying operations have exposed its ugly face of pursuing self-interest in complete disregard of moral integrity … flagrantly breached International laws, seriously infringed upon human rights and put global cyber security under threat.[34]

Other voices have been dismissive of the Western conception of the internet as a free and unbridled force. One semi-authoritative commentator has written in *Study Times*, a CCP mouthpiece, that the 'West's so-called internet freedom is actually a form of cyber-hegemony.'[35] Chinese elite browbeating is aimed at influencing international debates about cybersecurity. China has recognised that there's space to turn around cyberspace debates and influence non-aligned countries worried about US global surveillance and the US having a dominant position at the expense of other states. Cybersecurity experts in Chinese state media have recently expressed this attitude by denouncing the US pursuit of hegemony.[36]

China has proven capable of disrupting the existing consensus, claiming victimhood and handing down counter-accusations against other states. However, this is only the ham-fisted end of its international cyber strategy. China's more senior policymakers prefer to focus on leveraging the political space provided by changing international attitudes and a global 'trust deficit' to call for cooperation and advance China's own agenda. In the wake of Edward Snowden's disclosures about US National Security Agency surveillance activities, Beijing has used the incident to expose US activities to audiences at home and sympathetic nations abroad.

The Chinese Academy of Social Sciences—a prominent Chinese think tank—pointed out in the *2014 Blue Book on new media development* that the 'Snowden incident' (*sinuodeng shijian*), or what the Chinese media calls 'PRISM-gate' (*lengjingmen*), affected the global internet community beyond expectations.[37]

China has called for broader cooperation and continues to advance its own message in international policy debates, particularly the idea of internet sovereignty (*wangluo zhuquan*). Internet sovereignty, first outlined by China in the 2010 *The internet in China* white paper, is a concept that upholds the role of the state in cyberspace: 'within China's territory the internet is under the jurisdiction of Chinese sovereignty.'[38] At international forums, China has supported a state-centric concept of internet governance and the establishment of an authoritative internet administration organisation under the UN. China's activism comes at a time when international views on cyberspace are divided, there are organisational shifts underway (the ICANN transition, for instance), and support for an intergovernmental level of internet administration is growing among authoritarian states.

At the World Economic Forum's 2014 Summer Davos in Tianjin, in a panel on 'the future of the internet economy', Lu spoke about the 'need for brakes' on the internet and a model of internet governance that upholds state control. 'Freedom and order are two sisters, and they must live together,' said Lu, implying that policy should keep a tight rein on internet freedom, as it is ultimately subordinate to national security considerations.[39] China's interest in codifying the role of the state in cyberspace has a convincing domestic rationale. The state can control information within its territory and reduce the risk that domestic forces could challenge party rule, all within the bounds of international law.

While China's concept of internet sovereignty predates the Snowden revelations, over the past six months it has made a concerted effort in multilateral forums to promote its agenda. At the UN international workshop on cybersecurity hosted by China in June, Vice Foreign Minister Li Baodong articulated China's cyber sovereignty principle.[40] Late last year, Lu Wei, head of the SIIO, called for nations to 'respect cyber sovereignty, discard hegemony and avoid self-interest'.[41] Other high-level officials made similar statements at the Seoul cyberspace conference in August 2013, the NETmundial in Sao Paulo in May 2014, and at the ICANN50 in London. At the first ASEAN Regional Forum workshop on cybersecurity hosted by China and Malaysia in Beijing, Assistant Foreign Minister Zheng Zeguang called on participants to 'follow the principles of state sovereignty and non-interference in others' internal affairs'.[42]

Currently, China's efforts to counter and control international cyber debates are focused on strengthening domestic political control and redressing perceived weakness in the face of 'US dominance' of internet infrastructure. As one Chinese academic, Lang Ping from the Chinese Academy of Social Sciences, said in the *People's Daily*, 'if you apply Clausewitz' concept of key terrain to cyberspace, it's clear the US has absolute superiority.'[43] It remains to be seen whether Chinese elites will begin to publicly discuss efforts to counter US influence in cyberspace as part of a comprehensive strategic thrust against Washington. That level of elite discourse should ring warning bells about China's long-term ambitions.

The internet and China's place in the world—national rejuvenation and regional pre-eminence

The internet features squarely in China's thinking about its rise as a great power. In an era of rapid transformation, there's no modern-day technological revolution more significant in supporting China's rise. In China's perspective, cyberpower is essential to its broader great-power ambitions. 'China Dream', a popular leadership slogan, is the most prominent expression of the nation's self-confidence as a rising power. Xi Jinping declared soon after his inauguration that the China Dream is 'to achieve the great rejuvenation of the Chinese nation'.[44] The term is contested, but Peking University Professor Wang Yizhou provides a clear outline of the China Dream goal:

> doubling per-capita income by about 2020, bringing China into the club of developed nations as the Party celebrates one hundred years in power; and becoming the number one economic power by the middle of this century, as China celebrates the 100th year anniversary since the establishment of the People's Republic.[45]

Individual prosperity and national glory in the context of sustained GDP growth are the crux of the China Dream, and the CCP has staked its legitimacy on delivering this aspiration for China's citizens.

Chinese commentators view the internet as a means to attain 'China Dream' goals. At the announcement of the ISILSG, Xi Jinping declared that the building of cyberpower is part of China's 'two one hundred year goals', outlined in the China Dream concept.[46] 'To become a cyberpower is to realise the first step of the China Dream,' declared one commentator on ChinaByte, China's first IT website.[47] Chinese Academy of Engineering academic Wu Hequan has also observed recently that 'China's cyberpower is an integral part of the China Dream.'[48]

The elite's attentiveness to the pursuit of a strategy of national rejuvenation under the 'China Dream' is an interesting phenomenon, but not a new one—China has long desired a status that matches its economic strength. That cyberpower has been placed in line with the political pursuits of 'great power' and 'national rejuvenation' suggests that cybersecurity issues will receive the highest level of policy attention. It also suggests that cyberpower will be wielded as part of China's national strategy with more sophistication in the long term, as China continues along its dual tracks of informatisation and internet security.

Finally, it's worth noting that China's determination to become a cyberpower and a great power means that it will pursue that objective in the face of persistent opposition. Cyberpower is a significant strategic issue, as it's critical to China's rise as a respected power. Building cyberpower is a priority national interest, and that can produce surprising results. For instance, Huawei's rejected bid for Australia's National Broadband Network rollout is a sticking point in Australia–China relations, and Trade Minister Andrew Robb has confirmed publicly that it has adversely affected free trade negotiations. National security considerations will always be paramount, even if not justified publicly, but the new Chinese leadership is the first with a truly global consciousness. The new leaders are more optimistic and confident about China's position vis-a-vis other states. While Huawei is privately owned, prejudice against Chinese companies, especially national champions like China Telecom, will damage China's ego and global reputation, hinder its regional influence, and result in real penalties for those involved.

The CCP has taken on the risk of online interconnectivity, using the internet to advance prosperity and build its brand of national pride. However, the contradiction between creating opportunities for the exchange of information and simultaneously controlling it remains. An interconnected, modern China is at the crossroads of two forces: comprehensive state control and incredible social change. It's deeply committed to using information resources for national objectives and, in any case, it can't afford to abandon the internet despite its inherent risk. Engaging China on its concerns and aspirations, and encouraging Beijing to clarify its position, are key priorities for partners—including Australia.

Policy implications for Australia

The development of China's cyber strategy has four obvious policy implications for Australia.

1. Develop a substantive cyber dialogue with China

China has shown remarkable political attention to cyber matters, framing them as a top-level strategic issue. That interest is promising for international engagement, but won't make it any easier to reconcile fundamental differences with other nations. The best option for Australia is to establish a high-level cyber dialogue in Australia–China bilateral relations.

Prime Minister Tony Abbott has canvassed cyber issues with his counterparts, as have previous Australian leaders, but more is needed to develop discussion, especially about cybersecurity concerns and political intentions. The question remains whether Australia can broach a sensitive state issue like cybersecurity with China without prompting stony-faced reticence or, worse, condemnation. The Howard-era approach to human rights discussions with China offers an interesting and useful example. At that time, Canberra favoured dialogue rather than moralising, and distanced itself from China's great power competitor, the US—going so far as to not support US motions at the UN Commission on Human Rights. Most significantly, the Howard government emphasised the importance of economic relations as the context for discussion about sensitive issues. An emphasis on trade and investment ties enabled the two countries to manage their differences on human rights more practically. In a recent ASPI publication, Yuan Jingdong concluded that 'pragmatism, balance and care thus characterised the Howard approaches.'[49]

Tony Abbott has rekindled this approach with a comprehensive 'Team Australia' trade and investment push into Northeast Asia this year. At a luncheon in New York, Abbott said that 'a rich China doesn't mean a billion competitors so much as a billion customers.' And at the Bo'ao Economic Forum, where economic pragmatism ran supreme, Abbott invoked Deng Xiaoping's advice when he said to 'get rich is glorious' and that Australia's objective is to 'win friends rather than find fault'. But the real weight was in Abbott's last sentence: 'Participation in this forum has helped to build

Australia's strategic partnership with China.' The message was clear: economic ties can translate into strategic gains.

Cybersecurity should be at the forefront of this approach: we should propose cyber cooperation on the back of economic partnership, not least because cyber threats—both state and non-state—directly affect most business operations, and especially those involving bilateral trade. In addition, with Australia and China as close economic partners, there's an expectation that basic levels of cybersecurity understanding will underwrite and support that relationship.

Once dialogue is established, such as by including a cyber agenda at 2+2 ministerial meetings, or by way of a separate bilateral cyber dialogue, both parties will be in a confident position to avoid misperceptions and miscalculations, encourage the clarification of international cyber strategies, establish norms of behaviour, and hold each other accountable for actions that are deemed unacceptable according to shared standards. In addition, ministerial meetings would give 'top-cover' impetus for lower, technical-level arrangements.

2. Establish clear international cyber policy

With China's elevation of cyber matters on the policy agenda, it's time for Australia to publish a strategy that takes into account the technological advances and political shifts in the region. Australia's last cybersecurity strategy was released in 2009, and there have been significant developments in cyberspace since then, including fallout from the Snowden affair. A new white paper will need to clarify Australia's cyber policy thinking, particularly as it concerns international strategy.

3. Reconsider state-owned enterprise investment guidelines

The Chinese elite's conception of cyberpower is focused on economic growth; at the same time, China's IT industries are looking for new markets. Australia enjoys a close trade relationship with China that should include stronger investment flows, particularly Australia-bound investment. At the moment, according to leading economist Peter Drysdale, 'the current Australian guidelines are a blunt instrument for dealing with whatever issues were supposed to arise from [state-owned enterprise] investment in Australia'.[50]

The success of China's national companies abroad will lead to commercial and reputational gains for China—and for its investment partners. Australia should reconsider the Foreign Investment Review Board's zero thresholds and other guidelines on state-owned enterprise investment in order to attract Chinese companies to Australia. Reconsidering the guidelines should be seen as a bargaining tool in broader negotiations for the conclusion of the Australia–China Free Trade Agreement. With its internal stability made possible through economic growth, China is likely to act in a more consistent and more responsible way internationally.

4. Australia–China cyber relations and the US alliance

There are signs that China is willing to talk about cybersecurity with other states, even those considered direct competitors. In fact, China asked the US to include cybersecurity in the 2011 Strategic and Economic Dialogue agenda. And, even though US–China cyber relations have soured, we can potentially leverage our good relationships with both China and the US to build confidence between them. Opportunity in this area has been flagged on the Chinese side through ASPI roundtable discussions earlier this year.[51] The US also expects Australia to take a lead role in the region, and cyberspace is a domain with potential for further confrontation.

In one way, closer Australia–China cyber cooperation could be seen as having real strategic value for the US alliance. If the US is at odds with China over the most recent exchange of cyberattacks, or revelations about spying, we could still engage China in discussions and encourage it to behave responsibly in the international arena. Some careful positioning would be required, as we'd have to convincingly present ourselves as an independent voice while not undermining the position of our major ally and intelligence partner. Of course, the problem with this proposal is that China may see closer ties with Australia as directly benefiting Washington at the expense of Beijing. However, it's likely that China's political leaders already think along those lines. Encouraging responsible state behaviour should be the political objective. We have much to gain by improving our cyber relations with China and transferring those advantages to our allies.

Notes

1. Alex Oliver, *Lowy Institute poll 2014*, The Lowy Institute, Sydney, 2 June 2014, www.lowyinstitute.org/publications/lowy-institute-poll-2014.

2. Xi Jinping, 'Xijinping guanyu quanmian shenhua gaige ruogan zhongda wenti de jueding de shuoming', *The Central People's Government of China*, 15 November 2013, http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm.

3. Xi Jinping, 'Ba woguo cong wangluo daguo jianshe chengwei wangluo qiangguo', *Xinhua,* 27 February 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

4. Fu Ying, *The US and China: a new kind of great power relationship?*, The Brookings Institution, 12 June 2013, www.brookings.edu/~/media/events/2013/6/12%20us%20china%20fu%20ying/20130612_us_china_transcript.pdf.

5. Advisory Committee for State Informatisation, '2013 nian de <zhongguo xinxihua lanpishu>', 18 May 2013, http://www.acsi.gov.cn/content.aspx?newsId=1347&TId=113.

6. James Mulvenon, 'Chairman Hu and the PLA's New Historic Missions', Hoover Institution, *China Leadership Monitor*, no. 27, 1–11, 2009, www.cfr.org/china/hoover-institution-chairman-hu-plas-new-historic-missions/p18412.

7. Peter Mattis, 'Informatization drives expanded scope of public security', The Jamestown Foundation, *China Brief*, 2013, 13(8):1–3, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=40721&tx_ttnews[backPid]=688&no_cache=1#.VFiPyMm0QTQ.

8. Xi Jinping, 'Statement by Xi Jinping President of the People's Republic of China at the Nuclear Security Summit', 24 March 2014, http://sydney.chineseconsulate.org/eng/zgxw/t1140583.htm.

9. Zhang Hong, 'Zhongguo shi niannei jiben wancheng xiang xinxi shehui zhuanxing', *State Information Centre*, 15 July 2014, www.sic.gov.cn/News/249/3058.htm.

10. Edward Carr, *The twenty years crisis 1919–1939*, HarperCollins, 1984, p. 122.

11. Joseph Nye, *The future of power*, Public Affairs, 2011, p. 123.

12. Wang Xiujun, 'Wangluo anquan shi zhongda zhanlue wenti', *Communist Party of China News*, 18 May 2014, http://cpc.people.com.cn/n/2014/0518/c64102-25030795.html.

13. Xu Lei, 'Jiaqiang zhanlue bushu weihu wangluo anquan cheng guoji shehui gongshi he guanli', *Seeking Truth*, 28 February 2014, www.qstheory.cn/llzx/201402/t20140228_325546.htm.

14. China Internet Network Information Center, *Statistical report on internet development in China*, 16 January 2014, www1.cnnic.cn/IDR/ReportDownloads/201404/U020140417607531610855.pdf.

15. Liu Xiaobo, *No enemies, no hatred,* President and Fellows of Harvard College, 2012, p. 204.

16. Xi Jinping, 'Xijinping guanyu quanmian shenhua gaige ruogan zhongda wenti de jueding de shuoming', *The Central People's Government of China*, 15 November 2013, http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm.

17. Chinese Academy of Governance's E-Government Research Center, *2013 China Government micro-blog assessment report*, 8 April 2014.

18. Patrick Boehler, 'Is anti-rumour crackdown silencing voices of online dissent at Weibo?', *South China Morning Post*, 13 September 2013, www.scmp.com/news/china/article/1308860/anti-rumour-crackdown-silencing-voices-online-dissent-weibo.

19. Xinhua, 'Gejie renshi huyu duo guan qi xia, buxie nuli yingzao qinglang mingjing wangluo kongjian', 16 April 2014, http://news.xinhuanet.com/politics/2014-04/16/c_1110271784.htm.

20. Reuters, 'China's Sina fined for indecent content in web porn crackdown', 2 May 2014, www.reuters.com/article/2014/05/02/us-china-internet-sina-idUSBREA410XJ20140502.

21. Xinhua, 'Ba woguo cong wangluo daguo jianshe chengwei wangluo qingguo', 27 February 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

22. Xi Jinping, 'Xi urges independent innovation in science, technology', *Xinhua,* 9 June 2014, http://news.xinhuanet.com/english/china/2014-06/09/c_133394743.htm.

23. Li Keqiang, 'China pledges growth through innovation', *Xinhua,* 27 May 2014, http://news.xinhuanet.com/english/china/2014-05/27/c_133366203.htm.

24. Xi Jinping, 'Wangluo anquan zhanlue yiyi ji xin qushi', *Communist Party of China News*, 9 April 2014, http://theory.people.com.cn/n/2014/0604/c112851-25101944.html.

25. Zhang Feng, 'Shui lai tidai Windows XP gongxinbu xiwang yonghu shiyong guochan caozuo xitong', *CCTV,* 10 May 2014, http://tv.cntv.cn/video/C10616/e3af556308774b45b8c00de665dcbab7.

26. Austin Ramzy, 'China pulls Cisco into dispute on cyberspying', *New York Times*, 27 May 2014, www.nytimes.com/2014/05/28/business/international/china-pulls-cisco-into-dispute-on-cyberspying.html.

27. Michael Ward, Shilin Zheng, 'Mobile telecommunications infrastructure and economic growth: evidence from China', *Social Science Research Network*, August 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2355509.

28. Zhang Hong, 'Zhongguo shi niannei jiben wancheng xiang xinxi shehui zhuanxing', *State Information Centre*, 15 July 2014, www.sic.gov.cn/News/249/3058.htm.

29. Tobias Feakin, Jessica Woodall, Klee Aiken, *Cyber maturity in the Asia–Pacific region 2014*, Australian Strategic Policy Institute, 14 April 2014, www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014.

30. Zhang Hao, 'Drop Cold War mentality on China's cyber security', *Xinhua,* 22 April 2014, http://english.cntv.cn/2014/04/22/ARTI1398148113852301.shtml.

31. Hong Lei, 'Foreign Ministry spokesperson Hong Lei's regular press conference', Ministry of Foreign Affairs, 3 June 2013, www.mfa.gov.cn/ce/ceke/eng/fyrth/t1047004.htm.

32. Fu Cong, 'Guanjian sheshi jishu longduan goucheng wangluo kongjian zhongda tiaozhan', *Sina*, 10 April 2014, http://news.sina.com.cn/o/2014-04-10/192229905735.shtml.

33. National Computer Network Emergency Response Team, 'CNCERT fabu <2013 nian woguo hulianwang wangluo anquan taishi zongshu>', 28 March 2014, www.cert.org.cn/publish/main/12/2014/20140429133057350676875/20140429133057350676875_.html.

34. Internet Media Research Center, 'The United States' global surveillance record', People's Republic of China, 26 May 2014, http://news.xinhuanet.com/english/china/2014-05/27/c_133363178.htm.

35. Qi Jianguo, 'An unprecedented great changing situation: understanding and thoughts on the global strategic situation and our country's national security environment', *Study Times*, 21 January 2013, translation by Center for Naval Analyses China Studies Division, www.cna.org/sites/default/files/research/DQR-2013-U-004445-Final.pdf.

36. Liu Hanzhen, 'Wangluo gongji xianfazhiren mei shi baquan shengqilingren', *Xinhua*, 8 February 2014, http://news.xinhuanet.com/world/2013-02/08/c_124336726.htm.

37. ETnet, 'Wangluo guanhi guojia anquan sinuodeng shijian cheng fen shui ling', 26 June 2014, http://news.etnet.com.cn/topic/33673.htm.

38. Information Office of the State Council, 'The internet in China', People's Republic of China, 8 June 2010, http://www.gov.cn/english/2010-06/08/content_1622956.htm.

39. David Bandurski, 'Lu Wei: the internet must have brakes', *China Media Project*, 11 September 2014, http://cmp.hku.hk/2014/09/11/36011/.

40. Li Baodong, 'Address at the opening ceremony of the International Workshop on Information and Cyber Security', Ministry of Foreign Affairs, 5 June 2014, www.fmprc.gov.cn/mfa_eng/wjbxw/t1162458.shtml.

41. Lu Wei, 'Liberty and order in cyberspace', *Xinhua*, 9 September 2013, http://news.xinhuanet.com/english/china/2013-09/09/c_132705681.htm.

42. Tobias Feakin, 'ARF, and how to change the tune of the cyber debate', *The Strategist*, 14 October 2013, www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/.

43. Lang Ping, 'Wangluo zhuquan: Yige burong huibi de yiti', *People's Daily,* 23 June 2014, http://world.people.com.cn/n/2014/0623/c1002-25183696.html.

44. Xi Jinping, 'Xi pledges great renewal of Chinese nation', *Xinhua*, 29 November 2012, http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.

45. Wang Yizhou, 'China's new foreign policy: transformations and challenges reflected in changing discourse', *The Asan Forum,* 21 March 2014, www.theasanforum.org/chinas-new-foreign-policy-transformations-and-challenges-reflected-in-changing-discourse/.

46. Xi Jinping, 'Zhongyang wangluo anquan he xinxihua lingdao xiaozu chengli: cong wangluo daguo mai xiang wangluo qiangguo', *Xinhua,* 27 February 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538719.htm.

47. ChinaByte, 'Wangluo qiangguo de zhongguo meng xuyao shuju jiami de youli houdun', 4 March 2014, http://sec.chinabyte.com/189/12874689.shtml.

48. Wu Hequan, 'Wangluo qiangguo shi zhongguo meng de yibufen', *People's Daily*, 1 March 2014, http://www.people.com.cn/n/2014/0301/c347407-24501176.html.

49. Yuan Jindong, *A rising power looks down under: Chinese perspectives on Australia*, Australian Strategic Policy Institute, March 2014, https://www.aspi.org.au/publications/a-rising-power-looks-down-under-chinese-perspectives-on-australia/Rising_Power_China.pdf.

50. Peter Drysdale, 'Chinese state-owned enterprise investment', *East Asia Forum*, 25 August 2014, www.eastasiaforum.org/2014/08/25/chinese-state-owned-enterprise-investment-in-australia/.

51. Tobias Feakin, 'China–Australia cyber relations: insights for a cooperative future', *The Strategist*, 2 May 2014, www.aspistrategist.org.au/china-australia-cyber-relations-insights-for-a-cooperative-future/.

Acronyms and abbreviations

CCP	Chinese Communist Party
GDP	gross domestic product
ISILSG	Internet Security and Informatisation Leading Small Group
IT	information technology
PLA	People's Liberation Army
SIIO	State Internet Information Office
UN	United Nations

About the authors

Dr James A Lewis is an ASPI-ICPC International Fellow. He is a senior fellow and director of the Technology and Public Policy Program at CSIS, where he writes on technology, security, and the international economy.

Mr Simon Hansen is an ASPI-ICPC analyst.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
ASPI-ICPC http://cyberpolicy.aspi.org.au

RRP $5.00 ISSN 2200-6648