

Submission to the Senate Economics Reference Committee into the Foreign Investment Review Framework

Peter Jennings, executive director, Australian Strategic Policy Institute

March 2016

As part of its inquiry into the foreign investment review framework, the Senate Economics References Committee is considering 'the planned lease by the New South Wales Government of TransGrid.'

While supporting foreign direct investment in general, I have significant reservations about the security risks associated with leasing remaining parts of NSW's electricity transmission and distribution infrastructure to a Chinese State Owned Entity (SOE), namely State Grid, one of the world's largest electricity utilities and a potential tenderer for the remaining privatisations of the poles and wires.

SOE's and the Communist Party of China

The relationship between SOE's and the Communist Party of China (CPC) is kept deliberately ambiguous but it is clear that SOE's are ultimately under the direction of the Party. The Central Organisation Department of the CPC has ultimate power to place and remove top level management in the SOE's. While the CPC has stepped back from the day-to-day management of SOE business, these entities are ultimately instruments of the CPC.¹

In the case of State Grid the current chairman, Mr Liu Zhenya, was from 2007 to 2017 an alternate member of the 17th CPC Central Committee and has had a career in the CPC structure in Shandong Province.² Mr Zhenya's 'corporate message' on the English language version of the State Grid web site says that the company's 'most fundamental, important and urgent social responsibility is to thoroughly implement the spirit of the Third Plenary Session' of the CPC, and therefore 'contribute to the Chinese Dream of great rejuvenation.'³

To specialists on China, links between Party and business are a commonplace. Linda Jakobson writes: 'Each enterprise in China — everyone, for that matter, in an authoritarian one-party state — is expected to bear in mind the party-state's interests.'⁴ However this Committee has taken evidence from Australian officials who seem to be unaware or unconcerned about the nature of links between the CPC and SOEs. In providing evidence to the Committee on 15 December 2015, Mr Duncan Lewis said that:

'You will always have an intersection between commercial and government interests. Other governments around the world obviously pursue their interests, and they do it from time to

¹ There is a vast amount of research on the CPC and Chinese business but see, Richard McGregor, *The Party: The secret world of China's Communist rulers*. (Penguin, 2012 revised edition): '...from the moment Beijing decided to restructure state enterprises and sell parts of them offshore, the Party had deliberately downplayed its role in their operations, hiding it from its own people, and the rest of the world as well.' (P. 47.)

² See http://www.chinavivae.com/biography/Liu_Zhenya/full.

³ See <http://www.sgcc.com.cn/ywlm/aboutus/message.shtml>

⁴ Linda Jakobson, 'Darwin port row shows Australia doesn't understand China' *The Australian* 19 November, 2015. <http://www.theaustralian.com.au/opinion/darwin-port-row-shows-australia-doesnt-understand-chinese-society/news-story/9ec885e0131c6a3afd5e156a28da9f9b>.

time through their commercial entities, through entities that are national entities in their own country. There is nothing remarkable about that. That is the way of the world.’⁵

Given the commonplace nature of links between the CPC and Chinese business, Mr Donnelly of the Treasury told the Committee on 15 December 2015 that:

‘Clearly that cannot be a defining factor in determining that that particular company is a foreign government investor, otherwise just about every company coming out of China would be defined as such, so we need to look past that and try and work out whether there are any other indicators of control.’⁶

Applying that framework to State Grid, it is difficult to know what other indicators of state control are needed to demonstrate the deepest level of connection between the CPC and SOEs.

US concerns about critical infrastructure

The United States is increasingly concerned about the vulnerability of its own electricity infrastructure to, as Leon Panetta described it a ‘Pearl Harbour’ style attack from malicious cyber attackers. The head of the United States National Security Agency, Admiral Michael Rodgers briefed the House Intelligence Committee in November 2014 that China and ‘probably one or two other’ countries had the capacity to shut down key elements of the US power grid through a cyber attack.

We have seen instances where we are observing intrusions into industrial control systems. What concerns us is that access, that capability, can be used by nation-states, groups or individuals to take down that capability. ... We clearly are seeing instances where nation-states, groups and individuals are aggressively looking at acquiring that capability. What we think we are seeing is reconnaissance by many of those actors in an attempt to insure they understand our systems so that they can then, if they choose to, exploit the vulnerabilities within those control systems.

Those control systems are fundamental to how we work most of our infrastructure across this nation. And it’s not just the United States, on a global basis. They are foundational to almost every networked aspect of our life, from our water to our power to our financial segment to the aviation industry just as an example. They’re so foundational to the way ... we operate complex systems ... on a national basis.’⁷

US researches estimate that on ‘about a dozen times in the past decade’ foreign hackers have gained access to US electricity networks because of inadequate cyber security. The numbers of attempted hacks would have been substantially higher. Although there are different views about the difficulty involved in mounting successful attacks on American electricity infrastructure, it appears that the

⁵ Official Committee Hansard, Senate Economics References Committee, *Hearings into the foreign investment review framework*. Tuesday 15 December 2015.

[http://parlinfo.aph.gov.au/parlInfo/download/committees/commsen/07fdc731-1e2b-4fe7-af53-3853ad525f44/toc_pdf/Economics%20References%20Committee 2015 12 15 4077 Official.pdf;fileType=application%2Fpdf#search=%22committees/commsen/07fdc731-1e2b-4fe7-af53-3853ad525f44/0000%22](http://parlinfo.aph.gov.au/parlInfo/download/committees/commsen/07fdc731-1e2b-4fe7-af53-3853ad525f44/toc_pdf/Economics%20References%20Committee%202015%2012%2015%204077%20Official.pdf;fileType=application%2Fpdf#search=%22committees/commsen/07fdc731-1e2b-4fe7-af53-3853ad525f44/0000%22). P. 33.

⁶ *Ibid.* P. 37.

⁷ Admiral Michael Rodgers, Hearing of the House (Select) Intelligence Committee, *Cybersecurity Threats: The Way Forward*. 20 November 2014.

https://www.nsa.gov/public_info/files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.

number of attacks are growing and that a particular vulnerability is the age of the US electricity transmission and distribution network, which wasn't initially designed to address cyber threats.⁸

A US Homeland Security official stated in January 2016 that a suspected Russian cyber attack on the Ukrainian electricity grid may have created the first known power outage as a result of a cyber attack. US authorities have seen an increase in attacks that penetrated industrial control system networks over 2015, and said they are vulnerable because they are exposed to the Internet.⁹

The Committee should note that the NSW 'poles and wires' network is as vulnerable to cyber attack as the US electricity distribution network or the networks of other countries. Moreover there is increasing interest on the part of malicious cyber actors to explore how to damage the critical infrastructure of potential opponents. Australia cannot isolate itself from these international developments.

China is one of the most aggressive users of cyber space for espionage. As is set out in detail in Chinese military doctrine and in President Xi's comments, China sees the role of cyber as a core component of its strategic and defence thinking. China may also see asymmetric advantage in being able to attack United States and allied critical infrastructure. In the United States China is increasingly being identified by senior Government figures as a leading source of aggressive cyber hacking. This has included very detailed analytical work by the Mandiant Group which identified 141 cyber attacks between 2006 and 2013 across many US industry sectors undertaken by a unit of the Chinese People's Liberation Army.¹⁰

Australian authorities have been more reticent about identifying sources of state-based cyber attack although there is acknowledgement that the numbers of attacks 'is undeniable, unrelenting and continues to grow.'¹¹ China has been identified as a source of an attack in many specific instances, including against the Federal Parliament's computer network in 2011, against the Bureau of Meteorology in late 2015 and as having deep interests in hacking Australian government and private sector entities.¹²

⁸ Garance Burke and Jonathan Fahey, 'U.S. Not Prepared To Defend Power Grid From Cyberattacks', *Huffington Post*, 21 December 2015. http://www.huffingtonpost.com/entry/us-not-prepared-to-defend-power-grid-from-cyberattacks_us_56780a3ce4b0b958f657214f.

⁹ Jim Finkle, 'U.S. official sees more cyber attacks on industrial control systems' *Reuters*, 13 January 2016. <http://www.reuters.com/article/us-usa-cybersecurity-infrastructure-idUSKCN0UR2CX20160113>. The US Industrial Control Systems Computer Emergency Response Team (CERT) has confirmed that the power outage was due to external hackers actions on SCADA at three regional power companies. The outage only lasted 6 hours but systems are still being operated manually two months later. ICSCERT is reticent to actually name a state as the actor involved. The sophistication and the coordination involved is one of the notable elements of this incident.

¹⁰ Dan McWhorter, 'Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators' 19 February 2013. <https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html>.

¹¹ Australian Cyber Security Centre, *2015 Threat Report*. P. 2. [https://www.acsc.gov.au/publications/ACSC Threat Report 2015.pdf](https://www.acsc.gov.au/publications/ACSC%20Threat%20Report%202015.pdf).

¹² Christopher Joye, Aaron Patrick, 'Chinese spies may have read all MPs' emails for a year.' *Australian Financial Review* 28 April, 2014. www.afr.com/news/policy/defence/chinese-spies-may-have-read-all-mps-emails-for-a-year-20140427-if7ag#ixzz42Hkcl8uL

NSW's critical infrastructure is a vital enabler of our Defence capabilities

NSW's electrical transmission and distribution system is an element of critical national infrastructure on which significant parts of the Federal Government, Defence and the Intelligence community relies. We cannot afford to be casual about the security of this critical infrastructure.

The lease in November 2015 of 100% of Transgrid to an Australian-led consortium 'NSW Electricity Networks' which included Canadian, Kuwaiti and Abu Dhabi interests will still require putting prudent security measures in place to ensure the transmission of electricity to a range of Defence bases, the Federal Parliament and many Commonwealth departments and agencies. It is a positive security outcome that the NSW Government did not place the lease to bidders that included Chinese SOEs. However it is not clear that security considerations played any role in either the FIRB response to the proposed lease or the NSW Government's decision. The outcome is therefore welcome, but future security assessments need to be more deliberately considered.

The remaining poles and wires privatisation options include leasing 50.5% of Ausgrid, distributing electricity to 1.6 million households and businesses in Sydney, the Central Coast and the Hunter and leasing 50.4% of Endeavour Energy, distributing electricity to 900,000 households and businesses in Sydney, the Blue Mountains, the Southern Highlands and Illawarra region.¹³

Combined, these businesses provide the electricity distribution network for around 6.5 million Australians (based on the Bureau of Statistics count of 2.6 persons per household)¹⁴. By any measure this a network is a component of national infrastructure which, if attacked and disabled would severely impact on Australia's national security. Dealing with the consequences of disruption of electricity supply to Australia's major city, Sydney, and of an industry base that is vital to the effective working of the Australian Defence Force, would potentially damage Australia's capacity to respond to other national security threats at a time that the country might be under attack.

Chinese SOE's should not be considered as appropriate tenderers.

These considerations – about the close link between Chinese SOE's and the CPC; China's increasingly aggressive use of cyber capabilities and the vulnerability of Western critical infrastructure to cyber attack – should lead to a judgement that Chinese SOE's ought not be considered as appropriate partners in NSW's 'poles and wires' infrastructure.

No Australian company would ever be allowed by Chinese authorities to tender for parts of their electricity distribution and transmission. Indeed State Grid was kept as an SOE at a time when Beijing privatised many businesses precisely because power infrastructure was seen to be critical to Chinese security and must be kept in Government hands.

While visiting Beijing as Leader of the Opposition in 2012, Tony Abbott set out his response to the role of Chinese SOE's in seeking Australian investments:

¹³ NSW Legislative Council, Select Committee on the Leasing of Electricity Infrastructure, *Leasing of Electricity Infrastructure* June 2015. Page 4.

[http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/0235f3f94185e7ccca257e5700809547/\\$FILE/Report%20-%20Leasing%20of%20electricity%20infrastructure.pdf](http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/0235f3f94185e7ccca257e5700809547/$FILE/Report%20-%20Leasing%20of%20electricity%20infrastructure.pdf).

¹⁴ Australian Bureau of Statistics, 'Households and Families' as at 2006.

<http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1301.0~2012~Main%20Features~Households%20and%20families~56>.

‘Chinese investment is complicated by the prevalence of state-owned enterprises. It would rarely be in Australia’s national interest to allow a foreign government or its agencies to control an Australian business.’¹⁵

That position reflects a prudent approach to managing the national security implications of investment into critical infrastructure by Chinese SOEs.

Critical security concerns not addressed by NSW requirements

It is important to ensure that the conditions put on the lease arrangements adequately address critical security concerns. Ownership, including the NSW Government continuing to own a substantial element of the poles and wires infrastructure, does not adequately address these issues.

It will be essential to have clear understandings over who will have physical access to the hardware and software of the industrial control systems used by Transgrid, Ausgrid and Endeavour Energy.

Security systems should be in place to:

- Security clear staff with access to sensitive software and hardware control systems;
- Check replacement parts for key technologies;
- Vet alterations to computer programs by appropriate security agencies;
- Place stringent limits on controlling remote access to data and systems; and,
- Control access to billing information.

Appropriate inspection and test mechanisms should be in place making it possible to verify that tampering with a view to potentially damaging operations has not occurred.

A cyber red herring

It has been claimed that, if Australian critical infrastructure is vulnerable to Chinese cyber hacking, then the ownership and control of our infrastructure should make no difference. This is a council of despair, and hardly a basis on which to make sensible judgements about controlling our critical infrastructure. It remains the case that physical access is by far the easiest way to tamper with control systems, as while effective, remote access can take a great deal of time and requires high degree of technical ability. Sensible strategies to manage security around physical and cyber access to the control systems of critical infrastructure will go a very long way to protecting Australian interests.

FIRB decisions unclear

The basis of FIRB decisions in this case are as opaque as the management of Chinese SOEs. The Committee will have noted that the Treasury’s submission to the enquiry continues to defend a process that:

- Involves keeping ‘strict standards of confidentiality in the handling of information provided by applicants’ (Paragraph 1 of Treasury submission);
- Refuses, in the name of maintaining flexibility, to explain the basis on which decisions are made or the processes used to arrive at decisions (paragraph 16-18);

¹⁵ Tony Abbott, ‘Working Harder On A Complex Relationship’ *Address to the Australian Chamber of Commerce in Beijing*. 24 July, 2012. <http://australianpolitics.com/2012/07/24/abbott-auscam-china-speech.html>.

- Maintains that ‘the national interest test is a negative test meaning the presumption is that foreign investment proposals will be allowed to proceed unless found to be contrary to the national interest’ (paragraph 14);
- Says that ‘advice from the relevant national security agencies is relied upon for assessments as to whether an investment raises national security concerns’ (paragraph 53). But the Committee has seen that Defence makes judgements based on the impact of investment proposals on bases and facilities, not on national security grounds.
- Vests in the Treasurer ‘the power to decide in each case whether a particular investment would be contrary to the national interest (paragraph 13).

The Treasury maintains that this process is necessary to maintain community confidence in foreign investment decisions (paragraph 12). It is difficult to see how such an opaque and impenetrable process can create any basis for public confidence in FIRB decisions.

Conclusion

On national security grounds the Committee should advise against the NSW Government making any remaining privatisation decisions for the ‘poles and wires’ critical infrastructure to be leased to consortiums that include Chinese SOEs.

I refer the Committee to the submission made by myself, Anthony Bergin and Paul Barnes on 15 January 2016, in which we make eight recommendations to reform FIRB structures and processes and to better position decision-making on foreign investment proposals that genuinely will receive greater community endorsement. In summary, these recommendations are:

- 1: Establish a statutory basis for the FIRB and separate the Board from the Treasury Department.
- 2: FIRB should report to the National Security Committee of Cabinet, through the Treasurer.
- 3: FIRB must have adequate staffing, including individuals with professional expertise to make policy recommendations on national security matters.
- 4: FIRB must have defined assessment procedures to show that appropriate due-diligence has been performed on assessments.
- 5: A whole of Government Deputy Secretary level management committee is established to support the FIRB’s processes
- 6: Better define critical infrastructure and bring this more sharply into the FIRB’s focus.
- 7: The new FIRB structure should develop a classified paper for Government consideration on managing Chinese foreign direct investment.
- 8: Establish a dialogue on Foreign Investment matters involving the ‘Five eyes’ countries, that is Australia’s closest allies: the US, UK, New Zealand and Canada.