A Macdonald-Laurier Institute Publication

MLI

True North In Canadian Public Policy

Commentary

June 2013

Standing on Guard Post-Nexen: Chinese State-Owned Enterprise and Canadian National Security

By Roger W. Robinson

Introduction

The Canadian government's ruling on the acquisition of Nexen, one of its larger energy firms, by China National Offshore Oil Corporation (CNOOC) for $15.1 billion in December 2012 marked a new variant of the "net benefit test" used to guide Canadian policy makers. Instead of focusing on CNOOC's financials, technical capabilities, performance, employment opportunities, and other economic and commercial "due diligence" considerations, Canadian leadership instead examined the security-related dimensions of a Chinese state-owned enterprise (SOE) investing in Canada's energy sector. The long review period for this transaction served as a wake-up call for many economic policy professionals, who now better appreciate why national security agencies need to be fully engaged in such review processes. Fortunately, these are likely to be more serious and thoughtful in the future, particularly in the case of larger-scale transactions involving Chinese SOEs.

Canada now faces more Chinese SOEs entering the country, whose eyes are set on the high growth potential of the energy sector and on other resources of global importance. Indeed, Canada is now on the front lines of China's probable new strategic forays, which may have profound consequences. Canada has bountiful hydrocarbon and mineral assets, and it plays a pivotal role in the Arctic, with the many important economic and strategic considerations that loom there if, as expected, the melting ice provides new access and passageways. One early observation that the Canadian government can count on is that China's SOEs will continue their efforts to establish themselves in these strategic areas while portraying themselves as benign, independent, environmentally ethical commercial entities. Regrettably, such claims are dubious at best. The Canadian government should not take them at face value.

The objectives of this paper are to provide a brief retrospective concerning the security-related implications of the Nexen transaction and to recommend appropriate risk assessment criteria for Chinese SOEs. This paper also discusses existing and emerging concerns (both security-oriented and commercial) that warrant greater scrutiny from the Canadian government.

Lessons from the Nexen Acquisition

The Nexen transaction provides a number of lessons learned.

- **The government should not again place the Canadian security services in a position of playing catch-up** on a transaction that enjoys the fulsome support of the Canadian business community and Industry Canada. In this respect, the Prime Minister's Office should be commended for its determination to slow the Nexen transaction so that security-related concerns could be properly integrated into the decision-making process. The experience, however, highlights the need for a careful reconsideration of the effectiveness of the national security-related provisions of the *Investment Canada Act* and its regulations.

- **The definition of an SOE needs to be scrutinized carefully** as China's concept of a private sector enterprise is often detached from reality and, as stated in the definition below, the real question is one of control and influence. The investment policy adjustment that followed Nexen included an important provision regarding any future involvement of Chinese SOEs in the Canadian energy sector. Issued on December 7, 2012, the new provision states "investment by foreign SOEs to acquire control of a Canadian oil sands business, will, going forward, be found to be of net benefit on an exceptional basis only." [i] The *Investment Canada Act* defines an SOE as "an enterprise that is owned, controlled, or influenced directly or indirectly by a foreign government." This definition is especially important when doing business with China, as it should cover nominally "private sector" companies (like the controversial telecom giant Huawei), given the Chinese government's implicit control over the activities of such firms in Canada and elsewhere.

- Despite heightened sensitivities coming out of the Nexen experience, **there is still significant room for greater vigilance and security-minded diligence**. Chinese and other foreign SOEs are still not subject to any restrictions in their non-controlling interests in Canadian entities and "continue to be welcome in the development of Canada's economy." [ii] Moreover, this statement is particular to the oilsands. Accordingly, it is no coincidence that within days of the Prime Minister releasing this policy statement, one of China's oil majors, Petro China, acquired a 49.9 percent interest in an Alberta shale formation from Canada's Encana Corporation for $1.2 billion – skillfully dodging the specific sensitivities and parameters just put in place. [iii] The fact that Beijing is already engaging in such work-arounds is disheartening.

- **Every major Chinese company is controlled or influenced by the Communist Party.** This must simply be the foundation upon which Canada bases all diligence with regard to Chinese investments in the country and elsewhere that involve strategic or critical assets. On the same day that Canada's new policy guidelines for SOE investments were announced, Prime Minister Harper remarked on the specific factors that would be incorporated into future reviews of acquisition proposals by SOEs. The most important factor, he says, is "… the extent to which the foreign government in question is likely to exercise control or influence over the state-owned enterprise acquiring the Canadian business." [iv]

It is easy to forget, however, that one is dealing with an authoritarian police state in which the Communist Party controls nearly every facet of daily life – especially when it comes to its emissaries abroad, like the SOEs or firms like Huawei masquerading as private Chinese enterprises with a global reach. Indeed, the expression "let's not kid ourselves" comes to mind when Chinese companies seeking business overseas go to great lengths to cast their relationship with the Chinese government (in other words, the Communist Party) as remote, separate, and independent. This was made abundantly clear by the Chairman of CNOOC, Wang Yilin, in May 2012, when he announced to his employees "Large-scale deep-water rigs are our mobile national territory and a strategic weapon." [v]

H1 Security-minded Due Diligence

Scrutinizing the security implications of the investments, mergers, and acquisitions of Chinese companies in Western countries is not new. Chinese SOEs have been scorned for their ties to the Communist Party, the People's Liberation Army (PLA), and their willingness to partner with pariah regimes such as those of Sudan, North Korea, and Iran. Although these stigmas are still present, it is also true that Chinese leaders, including those of their SOEs, have made great efforts to sanitize themselves from these charges. For example, they have adopted the lexicon of industrialized democracies like Canada, and have become more adept at using requisite market and governance buzzwords, such as transparency, disclosure, independent directors, equitable treatment of shareholders, accountability, and free market principles when seeking market acceptance. Some of these concepts are, of course, present in the *Investment Canada Act*.

One of the first major iterations of this sanitization came in the late 1990s when many Chinese SOEs, at the behest of their government owners, embarked on ambitious efforts to disentangle themselves from the PLA. Until then, international observers in the markets and security communities worldwide had a clear understanding of the extensive intermingling of the PLA with SOEs. Within a short time, the narrative became that China's "private sector" had been isolated from the military and security and intelligence services. Any suggestion to the contrary was treated as anti-Chinese rhetoric.

Today, the success of this sanitization is more important than ever, as China's international economic and financial ambitions continue to grow, and foreign markets play prominently in Beijing's long-term economic, diplomatic, and strategic planning. The foreign diversification needs of its sovereign wealth funds, the interests of its corporations in hedging their business portfolios by investing overseas and the flight of capital from China's elite have all contributed to a new urgency for credibility in the independent and purely commercial nature of these entities.

Some attribute the May 2013 Bank of China announcement – the first public announcement of its kind – of the termination of its business with a North Korean bank as evidence of greater concern over the reputations of its leading entities overseas. [vi] Beijing is engaging in similar reputational initiatives around the world, as it allays concerns associated with the activities of its leading corporations and banks to ensure that the prized assets of other countries do not become off limits as a result of SOE complicity in doing the bidding of the State.

Examples of such behaviour are numerous. For example, Sinopec (which already has a large investment footprint in Canada) never explained why the US sanctioned two of its wholly-owned subsidiaries on four occasions for the proliferation of chemical weapons equipment and technology to Iran between 1997 and 2005.[vii] When this and other issues (for example, a $100 billion energy deal signed with Iran in 2007) have been raised, Sinopec differentiates adamantly between the operations of its parent company, Sinopec *Group*, and its independent subsidiaries, such as the publicly traded, NYSE-listed Sinopec *Corp*. One can only hope that market-savvy players who focus on the present do not view these transgressions as merely "ancient history." These unfortunate incidents and others like them have made clear to many in the security community that SOEs are willing to commit serious security-related abuses and obscure the role of the State using corporate shell games.

This is where it becomes necessary to view Chinese SOEs and their "private sector" equivalents through a security-minded lens. The Canadian economic and security community should be asking a different set of questions about such Chinese entities than they would, for example, a Norwegian sovereign wealth fund or even a Malaysian state-owned firm, like Petronas. This is not due to mere speculation or unfounded suspicion, but is based on their behaviour. Among the standard inquiries the Canadian economic and security community should undertake are:

- Is the SOE doing any business in security-sensitive countries such as Iran, Sudan, North Korea, Syria, Venezuela, North Korea, or Pakistan? What is the scope and type of that business?

- Has the SOE solicited or received stolen commercial information/competitive intelligence on Canadian or other Western firms through the cyber warfare/hacking activities of the PLA or other Chinese government-sponsored entities?

- Does the SOE have any business divisions or activities supplying equipment, technologies, services, or commodities to the PLA, any of its affiliates, or the Chinese security/intelligence services? What is the precise nature of any such supplier relationship?

- Do any subsidiaries or affiliates of the SOE have any military/intelligence ties or involvement in the proliferation of weapons of mass destruction or ballistic missiles?

- Are any senior managers or Board members of the SOE or its subsidiaries now or have they previously been affiliated with the PLA or the security/intelligence services of the Chinese government? What are or were the nature of such relationships or former employment?

- Have the SOE or its subsidiaries/affiliates been the subject of any corruption scandals or delisting from equity exchanges in China or abroad? If so, what are the underlying details?

- Has the SOE ever been charged, directly or indirectly, with any World Trade Organization violations or with providing any form of unfair financial or trade subsidies?

- Has the SOE or any of its subsidiaries ever been a member of a consortium of companies that has engaged in controversial, security-related projects domestically or abroad?

- Has the SOE been responsible for despoiling the environment or committing public safety violations in China or abroad?

- Has the SOE been responsible for the employment of forced labor or unsafe workplace conditions in China or abroad?

- Has the SOE employed counterfeit or contaminated goods or materials in its manufacturing processes or broader business services in China or abroad?

The point is that a deeper drill is required to differentiate between which Chinese enterprises are more benign, commercial entities and which have some track record of being used – or indicate the likelihood of being used in the future – to advance the strategic and/or security interests of the Chinese government, to which they are ultimately responsible or beholden. It is also increasingly useful to know the status of these enterprises within China itself, given the increasing severity of pollution and public safety concerns noted above. For example, most if not all the Chinese energy majors have "followed the flag" into countries of security concerns to gain valuable contracts and concessions not available to Western companies due to sanctions, regulations, or the inordinate risk of reputational harm. These companies also serve as beachheads for China's long-term strategic interests in volatile regions such as the Middle East, Africa, and Latin America.

Although these onerous ties have been largely muted of late, the PLA hacking scandal, which took on a public profile in February 2013 with the release of the *New York Times*-sponsored Mandiant report, reignited the connectivity between SOEs (and their equivalents) and the Chinese military and security services. Indeed, the large commercial dimension of Chinese hacking may have played a direct or indirect role in the Nexen transaction and the voluminous Canadian government deliberations surrounding it.

New PLA-SOE Linkage

Although Beijing has worked hard to insulate its SOEs from PLA "taint," occasionally the best-laid plans to obfuscate the truth go awry. Mandiant's report laid the groundwork for a glaring new layer of taint and elevated the financial/reputational risk for a broad array of Chinese SOEs. The report demonstrated yet again that the concerns of the US and Canadian security communities with regard to the connectivity between the Chinese military/intelligence services and SOEs are based on an extensive pattern of behaviour that extends to the present day.

The report gave unprecedented public profile to the PLA's guilt in systematic cyber espionage, theft, and other attacks against the US and, specifically, to the expert hacking activities of PLA Unit 61398. Mandiant traced the PLA's theft of proprietary information from some 150 businesses in the US over six years. This is probably only a fraction of the actual level of cyber crime perpetrated by the Chinese government and PLA. Moreover, Mandiant reported that the Chinese had hacked a wide spectrum of targets, including major US infrastructure hubs (electricity grids, water utilities, air traffic control systems, pipeline control centres, and more), military secrets and technology, commercial intelligence, and "inside" corporate data. [viii]

Although much of what the US government knows about the malevolent behaviour of SOEs and the various dimensions of cyber theft and espionage by the PLA remains classified, public revelations permit certain market-relevant observations and conclusions to be drawn, among them:

- The PLA has likely been illegally collecting competitive intelligence against US, Canadian, and other foreign firms in order to acquire valuable intellectual property and penetrate the key negotiating positions and other private communications of corporate executives (pricing decisions, financing terms, email traffic about a transaction's prospects, and so on.)

- It is reasonable to inquire if Chinese SOEs interested in securing proprietary information on the pending contracts, bids, or other activities of foreign competitors or acquisition targets may have actually hired PLA hackers. (If this were proven, the contracting of PLA "cyber thieves" would make SOEs complicit in such activities and, indeed, instigators, a considerably more egregious offence.)

- Even in instances when the PLA is not financially tied to the SOEs, there is little doubt (without the benefit of classified proof) that it passed on commercial, competitive intelligence through established protocols to prominent SOEs, including many that purport to be "private."

- Where foreign firms have entered into joint venture partnerships with Chinese companies or were acquisition targets, the foreign partner may well have been targeted for cyber theft to accelerate the transfer of technology and intellectual property (with the intention of bringing a "Chinese version" of the product or service to market more expeditiously) or to secure a desirable acquisition, joint venture, or sizable minority shareholding.

If the identities of specific Chinese SOEs that engaged in such activities became publically known, it could cause them serious legal, reputational, and financial complications and costs. Yet, given the findings of Mandiant's investigation, it is likely that such information is available and may emerge in the future. In this scenario, the markets and Western governments could well prove more aggressive in seeking justice and penalties against enterprises, government-controlled or not, that collaborated with the PLA to steal corporate information. Available information would likely include bidding positions, financing terms, internal negotiating strategies of competitors in tenders for major projects/contracts (a number of which might be taxpayer-funded projects), acquisition attempts, supplier contracts, and so forth.

For example, in 2009, Unit 61398 hacked Coca-Cola while the latter was trying to acquire the China Huiyuan Juice Group for $2.4 billion. An FBI investigation revealed that, over the month-long incursions into Coca-Cola's computer networks, the Chinese were able to access – with full remote control – almost any laptop, work station, or other device that had access to the company's Microsoft Windows server. The Huiyuan deal collapsed three days after the hacking was discovered, marking the end of what would have been the largest foreign takeover of a Chinese company. [ix]

Companies that have used stolen technology to compete against foreign firms in their home markets could also find themselves the target of class action lawsuits, shareholder litigation, unwinding procurement contracts or acquisitions, higher borrowing costs, adverse legislative actions, and other negative repercussions. At the same time, governments and corporations forced to grapple with the aftermath of unwinding business arrangements based on criminal activity are likely to incur considerable costs.

In sum, should the connection between PLA corporate espionage and specific Chinese SOEs be verified, public awareness of their continuing linkage – that was supposed to have ended over a decade ago – would likely prove a major setback to the standing of these SOEs in the global markets. It could also prove very challenging for any business partners that made sizable, long-term bets on the services and reputations of these entities. Of course, it would also demonstrate the necessity – and rationale – for heightened government scrutiny of the activities of Chinese SOEs in Canada in the future. That said, it should also not be lost on the Canadian security establishment that these SOEs, regardless of their potential PLA connectivity, carry with them the unfortunate reality that, by definition, they are agents of the state and subject to its will and direction.

Aggressive Financing

There is no question that long-term, subsidized financing represents the tip of the SOEs' competitive spear. This is by no means a new story, but it is now playing out in the more security-relevant sectors of the Canadian and US economies, notably energy, aerospace, telecommunications, and mining. The sales strategy of most SOEs is rather straightforward: offer the client a significantly lower price than that of the competition and/or substantially superior long-term, low-cost financing. When it comes to generous terms, it is useful to recall that CNOOC paid a 61 percent premium to Nexen's shareholders. This should give Canadian policy makers pause to think with respect to the strategic, not just commercial, designs of China's key SOEs. Even the big money involved in these transitions is of no object to Beijing when broader, long-term strategic objectives are at stake. [x]

There are many examples of China capturing or expanding its presence in larger energy and other projects through the subsidized financing door. Indeed, project pricing and financial terms are somewhat artificial and can be "administered" by the SOEs' government keepers where strategic content is involved. For example, both the US and the EU have accused Huawei of receiving illegal subsidies from the Chinese government that allowed the company to sell equipment at artificially low prices. [xi] Although Canada is well aware of this competitive "sweetener" from the Chinese government to SOEs, the non-market, non-commercial aspects of this gambit will become clearer – and more perilous from a security perspective – as competition for the Arctic's assets continues to intensify. Accordingly, Canada should view this financial "tell" of strategic intentions as a prime indicator in the course of the security-related vetting of future SOE investments in the country.

Further Investigation

The Mandiant report and any future revelations regarding corporate espionage could and should serve as the basis for Parliamentary hearings. These hearings should include a careful review of CNOOC's acquisition of Nexen and, for example, seek to answer the question of whether or not CNOOC received sensitive, internal information about Nexen's negotiating position and shareholder disposition, and about the multitude of government deliberations surrounding this controversial deal that the PLA might have obtained. Such a discovery would be all the more explosive if it were ever proven that CNOOC had actually asked and/or compensated PLA hackers for stolen internal Nexen information. Nexen executives should also be officially asked (preferably under oath) if the company was hacked at any time during the CNOOC-related deliberations.

Any such hearings could expand their focus into similar circumstances, even if not on the same scale as this high profile acquisition. For example, Parliamentary hearings should also examine the strategic implications of the PLA hacking into Calgary-based Telvent in September 2012. Telvent manufactures the automated control systems of major utilities: its IT services help manage some 60 percent of all oil and gas pipelines in North America and Latin America. The "digital fingerprints" of the intrusion all pointed to China. Subsequent revelations, like those referenced above, make this allegation all the more likely. China also allegedly hacked companies such as Symantec and McAfee during this time. These intrusions cannot be explained away as examples of the Chinese security community merely testing the cyber waters for some future date. Precisely what commercial information was the PLA stealing? Who are – or were – the recipients of this information? What was it being used for?

Brian Adams, a former Canadian official and expert on Chinese espionage, writes "In essence, it's an electronic war that's going on. And this company [Mandiant] is bringing to our attention that China could shut down the energy resources of any country in the world with this sort of thing going on." [xii] Other experts have also speculated that China is trying to access the computer codes used to control specific pipelines. Such practices are anything but benign, commercial activities, and there is an especially good chance that certain of China's energy majors were "in the loop" on this malevolent, systematic hacking scheme.

In addition to the security dimensions of these sorts of hacks, officials should expand their lines of inquiry to include the business implications and economic and financial costs associated with these intrusions. Canadian corporate entities, for example, should be compelled to share the existence of hacks if their dialogue and working relationships with Chinese companies implicate national security and/or Canada's strategic assets.

Conclusion

Policy makers, administrators, and business executives rarely embrace the layers of complexity involved in dealing with Chinese SOEs and their "private" equivalents. It is far easier and more straightforward to apply established practices and procedures when conducting Canada's net benefit test. The conventional wisdom appears to be that, with a few tweaks to account for Chinese government involvement, SOEs are among the energy majors that search the globe for viable and profitable hydrocarbon sources. Regrettably, it takes considerably more than tweaks to penetrate the mindset and strategic intentions of Chinese leadership and an ascendant PLA within that leadership.

For example, it cannot be assumed that the traditional range of commercial and shareholder considerations that drive and temper the activities of Canadian and US firms will also guide SOEs. Moreover, Beijing's view of long-term objectives will likely be at odds with those of the Canadian government and industry. US and Canadian firms probably do not enjoy the substantial benefits of their respective intelligence communities or militaries feeding them sensitive intelligence on their competition, acquisition targets, and so forth that Chinese SOEs receive. This and other differences are stark, not subtle.

Accordingly, when one reads about Minerals and Metals Group, a Chinese SOE in the process of buying 350 kilometres of territory that extends from Izok Lake to the central Arctic coast that purports solely to be pursuing mining interests, it warrants special scrutiny. Now that China has achieved observer status in the Arctic Council, its agenda of issues should prove quite telling, but probably only after a year or more hiatus. During this period, the Chinese are likely to veil their real intentions while they insinuate themselves into the fabric of the Council.

To prepare for these types of contingencies, the Canadian government, Parliament, and the media should return to the Nexen transaction in light of the disturbing revelations of the Mandiant investigation. It is hard to believe that the Nexen "litmus test" – and national debate – concerning China's future prospects in the highly attractive Canadian energy sector did not interest the accomplished PLA hackers of Unit 61398 as they searched for high-value commercial and political intelligence to advantage its SOEs. A thorough and security-minded retrospective regarding this deal would likely yield a number of troubling realities overlooked in the first round of diligence.

The question is whether anyone will care now that the deal is done and off the front page. Hopefully, the political will and courage exists to answer that question in the affirmative. Canada's future positioning in the Arctic and the North American energy picture may depend on such inquiries.

Roger W. Robinson, Jr. is Executive Director of PSSI Washington and Chairman and Co-Founder of the Prague Security Studies Institute. He was formerly Chairman of the Congressional US-China Economic and Security Review Commission and Senior Director of International Economic Affairs at the National Security Council.

Endnotes

[i] Industry Canada. December 7, 2012. "Government of Canada Releases Policy Statement and Revised Guidelines for Investments by State-Owned Enterprises." Ottawa.

[ii] Jeffrey Jones. December 13, 2012. "Encana, PetroChina take $2.2 Billion Stab at Joint Venture." *Reuters*.

[iii] Stephen Harper. December 7, 2012. "Statement by the Prime Minister of Canada on Foreign Investment." Ottawa.

[iv] Brian Spegele. August 29, 2012. "For China Boss, Deep-Water Rigs are a 'Strategic Weapon.'" *Wall Street Journal*.

[v] Lingling Wei. May 7, 2013. "Bank of China Severs Ties with North Korean Bank." *Wall Street Journal*.

[vi] Gary Milhollin. March 10, 2005. "Testimony of Gary Milhollin before the U.S.-China Economic and Security Review Commission." US-China Economic and Security Review Commission.

[vii] Mandiant. 2013. *Exposing One of China's Cyber Espionage Units*. Mandiant Intelligence Center Report. February 18.

[viii] Ben Elgin, Dune Lawrence, and Michael Riley. November 4, 2012. "Coke Gets Hacked and Doesn't Tell Anyone." *Bloomberg*.

[ix] Paul Boothe. 2013. "State-Owned Enterprises and Foreign Investment in Canada." *Ivey Business Journal*. January/February.

[x] Denis Pinchuk. January 23, 2012. "Huawei Denies Using Chinese Subsidies to Grab More Business." *Reuters*.

[xi] The Huffington Post Alberta. September 28, 2012. "Calgary Telvent Security Breach: Customers Warned, Signs Point to Chinese Hackers." *The Huffington Post Alberta.*