EABER
EAST ASIAN BUREAU OF ECONOMIC RESEARCH

EABER WORKING PAPER SERIES

PAPER NO. 85

TOWARD A MULTILATERAL FRAMEWORK FOR IDENTIFYING NATIONAL SECURITY THREATS POSED BY FOREIGN ACQUISITIONS: WITH SPECIAL REFERENCE TO CHINESE ACQUISITIONS IN THE UNITED STATES, CANADA, AND AUSTRALIA

THEODORE H. MORAN
MARCUS WALLENBERG PROFESSOR OF INTERNATIONAL BUSINESS AND FINANCE GEORGETOWN UNIVERSITY

EABER SECRETARIAT
CRAWFORD SCHOOL OF PUBLIC POLICY
ANU COLLEGE OF ASIA AND THE PACIFIC
THE AUSTRALIAN NATIONAL UNIVERSITY
CANBERRA ACT 0200 AUSTRALIA

Toward a Multilateral Framework for Identifying National Security Threats Posed by Foreign Acquisitions: With Special Reference to Chinese Acquisitions in the United States, Canada, and Australia

Theodore H. Moran

Marcus Wallenberg Professor of International Business and Finance

Georgetown University

37th & O Streets NW, Washington, DC 20057

202-687-5854

ibd@georgetown.edu

Non-Resident Senior Fellow, Peterson Institute for International Economics

ABSTRACT

This paper presents a framework for differentiating between foreign acquisitions of companies that might plausibly pose a national security threat to the home country of the target acquisition and those that do not. [1] This framework originally derives from the experience of the United States. The framework is then shown to be relevant and useful for foreign acquisitions in Canada and Australia. In each case, Chinese acquisitions of US, Canadian, or Australian firms are highlighted. The paper concludes by arguing that this framework can serve as an effective non-discriminatory basis for separating genuine from implausible national security threats from foreign acquisitions across OECD states, to include all countries around the world.

Keywords: Multinational Firms and International Business, Globalization and Finance, Policies to Deal with the Impacts of Globalization, Regulation and Business Law.

JEL Codes: F23, F65, F68, K23.

[1] The analysis here draws on Moran and Oldenski (2013) and Moran (2009). In the interest of full disclosure, it should be noted that Theodore Moran serves on the International Advisory Council of Huawei Technology Company.

TABLE OF CONTENTS

Abstract **2**

1. Separating Genuine from Implausible National Security Threats: A 'Three Threats' Framework Derived from US Experience **5**

1.1. Threat I: Denial or Manipulation of Access 8

1.2. Threat II: Leakage of Sensitive Technology or Know-How 12

1.3. Threat III: Infiltration, Espionage, and Disruption 14

2. Applying the Three Threats Prism to Proposed Chinese Acquisitions in the United States 16

2.1. Lenovo-IBM 16

2.2. CNOOC-Unocal 16

2.3. Huawei and Vulnerabilities in IT Systems 20

2.4. A Special Look at Protecting National Security – and Commercial Integrity – in an Era of Global Supply Chains 23

3. Applying the Three Threats Prism to Proposed Chinese Acquisitions in Canada 26

3.1. National Security versus Economic 'Net Benefit' Tests 27

3.2. The Important Case of Chinese Investment in Rare Earths 28

3.3. Conflict of National Interests among Allies as well as Potential Adversaries 30

4. Applying the Three Threats Prism to Possible Chinese Acquisitions in Australia 32

5. Toward a Multilateral Non-Discriminatory Framework for Separating Plausible from Implausible National Security Threats Posed by Foreign Acquisitions **39**

OECD-Wide (or World-Wide) Decision-Tree..... 41

REFERENCES..... 44

1. Separating Genuine from Implausible National Security Threats: a 'Three Threats' Framework Derived from US Experience

Foreign direct investment that takes place via acquisition of an already existing company in the home economy has long been a subject of particular sensitivity around the world, with frequent allegations that the outcome might negatively affect the national security of the home country. Within OECD states, approximately 80% (or more) of all FDI takes place via acquisition of an already-existing firm, rather than as greenfield investment.

How might 'national security threats' be defined, and how can realistic threats be separated from allegations of threat that are implausible? A look at US experience where policymakers have grappled with the notion of what constitutes a national security threat for more than 20 years offers a useful analytical framework for other nations as well.

The Committee on Foreign Investment in the United States (CFIUS) is the inter-agency committee established to review potential foreign acquisitions of US companies to determine whether such acquisitions might threaten the national security of the United States. The CFIUS derives its authority from section 721 of the *Defense Production Act of 1950*,[2] and the Exon-

[2] 'The authority of the President to suspend or prohibit certain transactions was initially provided by the addition of section 721 to the Defense Production Act of 1950 by a 1988 amendment commonly known as the Exon-Florio amendment. The Foreign Investment and National Security Act of 2007 (FINSA), which became effective October 24, 2007, substantially revised section 721. Section 721 of the Defense Production Act of 1950 is codified at 50 U.S.C. App. 2170.' (http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-legislation.aspx).

Florio provision of the *Omnibus Trade Act of 1988* as amended.[3] The most recent amendment to the *Defense Production Act of 1950* is the *Foreign Investment and National Security Act of 2007* (FINSA),[4] and the subsequent FINSA regulations (2008).[5] Notification of a proposed transaction to the CFIUS is voluntary. Once notification is received, the Committee has 30 days to assess the national security implications of the transaction, and – if necessary – has an additional investigation period of 45 days.

The CFIUS is chaired by the Treasury Department, and its members include the Justice Department, State Department, Homeland Security Department, Department of Defense, and Department of Commerce, among other agencies. The Director of National Intelligence provides security assessments to the Committee, but does not have a voting role.

The CFIUS has a mandate to identify and address national security risk posed by a proposed foreign acquisition. CFIUS guidance states that national security considerations may be presented because the US firm that is the target of acquisition: has government contracts; has operations relevant to defense industries; or deals in advanced technologies or goods and services that are controlled for export. CFIUS guidance also states that national security considerations may be presented because of the track record of the company seeking to acquire control of the US business, and/or that of the government where that company is located (including if there is government ownership of that company).

---

[3] An Act to Enhance the Competitiveness of American Industry, and for Other Purposes, HR 4848 100th Congress (1988).

[4] Foreign Investment and National Security Act of 2007, HR 556 110th Congress (2007), Public Law No: 110-49.

[5] Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, Final Rule, 31 CFR Part 800. Federal Register / Vol. 73, No. 226 / (2008).

If the CFIUS finds that the proposed acquisition does not present any national security risks or that other laws adequately and appropriately address the risks, then the CFIUS will so advise the parties to the acquisition. If the CFIUS finds that the proposed acquisition presents national security risks and that other laws do not provide adequate authority to address the risks, then the CFIUS may enter into an agreement with, or impose conditions on, parties to the acquisition to mitigate such risks or may refer the case to the President for action. The President is the only officer with the authority to suspend or prohibit mergers, acquisitions, and takeovers.

The legislation and regulations referred to above, that together confer authority for the US process of reviewing foreign investment, do not spell out the specific nature of national security threats. But the cases that have dominated US analytical focus since the initial insertion of the Exon-Florio provision into the *Omnibus Trade Act of 1988* show that potential threats to national security that might result from foreign acquisition of a home company fall into three distinct categories. Since 2012, this 'Three Threats' framework has been the basis for the US government training program that staff members of the CFIUS committee must take to be certified by their home agencies to deal with CFIUS cases.

The first category of threat ('Threat I') is that the proposed acquisition would make the home country dependent upon a foreign-controlled supplier of goods or services crucial to the functioning of the home economy (including, but not exclusively, the functioning of the defense industrial base) who might delay, deny, or place conditions upon provision of those goods or services.

The second category of threat ('Threat II') is that the proposed acquisition would allow transfer of technology or other expertise to a foreign-controlled entity that might be deployed by the entity or its national government in a manner harmful to home country national interests.

The third category of threat ('Threat III') is that the proposed acquisition would allow for the insertion of some potential capability for infiltration, surveillance, or sabotage – via a human agent, or non-human agent – into the provision of goods or services crucial to the functioning of the home economy (including, but not exclusively, the functioning of the defense industrial base).

In the US context, the pressures that led to the passage of the Exon-Florio provision in 1988 arose from a broad concern about the possible decline of US high tech industries. This concern was aggravated by aggressive competition from Japan, not unlike some contemporary apprehensions about China.

1.1.Threat I: Denial or Manipulation of Access

The case that provided the most proximate impetus behind the passage of the Exon-Florio provision was the proposed sale of Fairchild Semiconductor by Schlumberger of France to Fujitsu in 1987 with concern that the sale would give Japan control over a company that served as a major supplier of chips to the US military. Fujitsu withdrew its bid for Fairchild, however, before extensive analysis was done about whether foreign 'control' and excessive 'dependence' were valid apprehensions.

The criticism of the proposed acquisition rested on the premise that the target firm was in an industry *'crucial'* to the US economy – and to US defense – with 'crucial' being given the common-sense definition of conveying a large negative impact if the economy had to do without the goods and services in question. In the Fairchild Semiconductor case, there was no careful

analysis of the conditions under which supply could be manipulated or whether such manipulation would have any practical impact.

This changed in 1989 with the battle over Nikon's proposal to acquire the US company Perkin Elmer's 'stepper' division. Steppers are advanced lithography equipment used to imprint circuit patterns on silicon wafers in the semiconductor industry. At the time of the proposed acquisition, Nikon controlled roughly half of the global market for optical lithography and Canon controlled another fifth. If the acquisition were allowed to proceed, US producers would be highly constrained with regard to where they could purchase machinery to etch micro-circuits on semiconductors. It was alleged that the sale would effectively place quasi-monopoly power in the hands of the new owner, and – by extension – the new owner's home government. The novel insight from the Perkin Elmer case was that term 'crucial' – namely, the cost of doing without – had to be joined with a parallel consideration. For there to be a credible likelihood that:

- a good or service can be withheld at great cost to the economy; or
- suppliers (or their home governments) can place conditions upon the provision of the good or service;

the industry must be tightly concentrated, the number of close substitutes limited, and the switching costs high. Under such conditions, home country national security might credibly be placed at risk.

Of particular note, the risk to national security in a highly concentrated industry does not require that the home government of the foreign acquirer be an 'enemy' of the nation where the proposed acquisition might take place, nor that the home government have an ownership stake in the company proposing to make the acquisition. Even though the US-Japan foreign policy

relationship was broadly cooperative, the concern about the Japanese government instructing US subsidiaries of home-country companies to behave in ways inimical to US national interests was not without foundation. In a case not involving any acquisition whatsoever, MITI (the Japanese Ministry of Trade and Industry), under pressure from Socialist members of the Diet, did force Dexel, the American subsidiary of Kyocera, to withhold advanced ceramic technology from the US Tomahawk cruise missile program (House of Representatives 1991, 179). This issue of national security concerns even when the countries of origin of the companies involved are allies will be revisited in the section on acquisition cases in Canada.

The relevance of this growing insight about concentration, substitutes and switching costs becomes apparent if one jumps ahead in time. In the case of a Russian oligarch's proposal to acquire Oregon Steel, it became even clearer and more widely recognized that the fact a proposed acquisition will take place in an industry identified as 'crucial' is not a sufficient justification to block the acquisition. In this case policy analysts sometimes replaced 'crucial' with 'critical', with the same implication of a high cost if supply were manipulated.

Would the acquisition of Oregon Steel in 2006 by Russian company, Evraz, pose a national security threat to the United States bearing in mind the company's close ties to Roman Abramovich, a Russian billionaire who enjoys intimate relations with the Kremlin? For a foreign acquisition such as this to pose a threat that the home economy might become dangerously dependent upon the foreign supplier, national security strategists have to evaluate *both whether:*

- the good or service provided by the target firm is crucial to the functioning of a country's economy, including but not limited to its military services; *and*

- there is a credible likelihood that the good or service can be withheld (or that the suppliers, or their home governments, could place conditions upon provision of the good or service).

The first evaluation clearly raises concerns: steel is a major component of more than 4000 kinds of military equipment, from warships, tanks, and artillery, to components and subassemblies of a myriad of defense systems. Uninterrupted access to steel is likewise crucial for the everyday functioning of the US civilian economy.

But the second evaluation dispels those concerns: in the international steel industry, the top four exporting countries account for no more than 40% of the global steel trade. Alternative sources of supply are widely dispersed, with nine countries besides Russia (*viz.* Japan, Ukraine, Germany, Belgium-Luxembourg, France, South Korea, Brazil, Italy, and Turkey) that export more than 10 million metric tons annually. There are 20 additional suppliers that export more than five million metric tons annually. It is difficult to imagine a scenario in which the Russian government or the Russian oligarch could manipulate output from Oregon steel in a way that was more than a minor inconvenience to buyers in the United States.

At the end of the day, the steel industry remains vital to US national economic and security interests. But the multiplication of sources of supply around the world means that there is no realistic likelihood that an external supplier – or group of suppliers – could withhold steel from US purchasers, or place conditions upon US purchasers or upon the US government in order to take delivery. The globalization of steel production allows US users to take advantage of the most efficient and lowest cost sources of supply without a nagging worry that somehow the United States is becoming 'too dependent' on foreigners.

1.2.Threat II: Leakage of Sensitive Technology or Know-How

In almost all proposed acquisitions, it would be odd if the takeover did not offer the foreign parent corporation some production or managerial expertise that it did not formerly possess, thereby providing the home government of the foreign parent with an opportunity to command that the newfound expertise be deployed in ways desired by the home government. It would be equally odd if the additional production or managerial expertise did not, in some marginal way, strengthen the national defense capabilities – including the military capabilities – of the new home government.

So this second test interacts with the first – how broadly available is the additional production or managerial expertise involved, and how big a difference would the acquisition make to the new home government? The prototypical illustration of potentially worrisome technology transfer can be found in the landmark case of the proposed acquisition of the US-based LTV missile business by Thomson-CSF of France in 1992 (Moran 1992).

The LTV corporation found itself in bankruptcy due to under-funded pension obligations associated with the parent company's steel-making operations. To raise cash, a Federal bankruptcy court in New York considered proposals from Martin Marietta, Lockheed, and Thomson-CSF of France to purchase LTV's missile division, and approved sale to the latter. Some of LTV's missile division capabilities were sufficiently close to those of multiple alternative suppliers that Thomson-CSF could obtain them elsewhere with relative ease. However, three product lines – the MLRS multiple rocket launcher, the ATACM longer range rocket launcher, and the LOSAT anti-tank missile – had few or no comparable substitutes. Moreover, one product line – the ERINT anti-tactical missile interceptor – included highly classified technology that was at least a generation ahead of rival systems and virtually unique at

the time. It is not clear from public sources exactly which LTV missile division products and services were formally included in the US export-control regime of the time.

Thomson-CSF was 58% owned by the French government, and in any case had a long history of following French government directives in the most intimate fashion. The potential for sovereign conflict over the disposition and timing of Thomson-CSF sales should the LTV missile division become part of the group was substantial. Prior Thomson-CSF sales to Libya and Iraq had already provoked considerable controversy: a Thomson-built Crotale missile had shot down the sole US plane lost in the 1986 US bombing raid on Tripoli, and Thomson radar had offered Iraq advance warning of air attack in the first Gulf War.

The Department of Defense (DOD) initially informed Congress that the Pentagon would insist upon a Special Security Agreement (SSA), or blind trust, to perform the security work on LTV programs, an arrangement at first opposed by Thomson-CSF but ultimately accepted. The CFIUS ultimately rejected the proposed acquisition when Thomson and the Pentagon failed to reach agreement on how to ensure that sensitive US technology did not seep through in any way to the new French parent.

Thus the methodology for determining whether a foreign acquisition threatens to provide a channel for some unacceptable ‘leakage’ of technology or other know-how follows the same path as already outlined. The key lies in calculating the concentration or dispersion of the particular capabilities possessed by the entity that is to be acquired. When the entity presides over some unique or very tightly-held capabilities that might be deployed in ways that could damage the national security interests of the home country, the threat is genuine.

These analytics will be helpful in understanding US cases such as Lenovo's proposal to acquire IBM's PC business, and the proposal by China National Offshore Oil Corporation (CNOOC) to acquire Unocal.

1.3.Threat III: Infiltration, Espionage, and Disruption

The Dubai World Ports (DWP) case brought to the fore an additional concern, namely, that a foreign acquisition might provide a setting in which the new owner: was less than vigilant in preventing hostile forces from infiltrating the operations of the acquired company; or might even be complicit in facilitating surveillance or sabotage. In 2005, DWP – a state-owned company based in the United Arab Emirates – sought to acquire the Peninsular and Oriental Steam Navigation Company (P&O), a British firm. P&O's main assets were terminal facilities owned or leased in various ports around the world, including facilities at six US ports—in Baltimore, Houston, Miami, New Orleans, Newark, and Philadelphia. The CFIUS initially approved the acquisition.

'Threat III' is a separate category for evaluating the potential threat to US national security. The issue is not whether foreign ownership of a given service provider,[6] infrastructure network,[7] or facility[8] might lead to the denial of service delivery by direct order of the new owner or the new owner's home government. Nor is the issue whether sensitive technology or other management capabilities might be transferred to the new owner or the new owner's home government. Rather, the question is whether foreign ownership increases the likelihood that a

[6] E.g., ports administration.

[7] E.g., telecom.

[8] E.g., petrochemical plant.

so-called ‘fifth column’ might be able to penetrate the new foreign-owned structure (Graham and Marchick 2006). Foreign acquisition might afford the new owner’s government a platform for clandestine observation or disruption.

Besides rejection of a proposed acquisition, national authorities (like the CFIUS in the US) may deal with Threat III via remediation of the kind utilized for foreign takeovers. For example, in cases where classified technologies and materials are involved there is often a requirement to set up separate compartmentalized divisions where home country citizenship and special security vetting is mandatory. As part of the process that led to the first CFIUS approval, the Department of Homeland Security (DHS) negotiated a ‘letter of assurances’ with DP World, which stipulated that Dubai Ports would:

- operate all US facilities with US management;
- designate a corporate officer within DP World to serve as a point of contact with DHS on all security matters;
- provide information to DHS whenever requested; and
- assist other US law enforcement agencies on any matter related to port security, including by disclosing information as requested by US agencies (Graham and Marchick 2006, 138).

But public outcry against ownership by Dubai Ports was sufficiently great that this mitigation agreement was dismissed out of hand, and the parent company withdrew its offer.

2. Applying the Three Threats Prism to Proposed Chinese Acquisitions in the United States

How might the 'Three Threats' framework have been applied to proposed Chinese acquisitions in the US, like Lenovo's 2005 purchase of IBM's personal computer business or CNOOC's proposed acquisition of Unocal in the same year?

2.1.Lenovo-IBM

Looking first at Lenovo's proposal to acquire IBM's PC business, could this acquisition have posed a credible national security threat to the home country of the target company (that is, to the US)? Looking at Threat I (denial) and Threat II (leakage of sensitive technology), competition among personal computer producers, for example, is sufficiently intense that basic production technology is considered 'commoditized'. More than a dozen producers compete for 50% of the PC market, with no one showing a predominant edge for any length of time. It is farfetched to think that Lenovo's acquisition of IBM's PC business represented a 'leakage' of sensitive technology, or provided China with military-application or dual-use capabilities that are not readily available elsewhere. Nor could Lenovo manipulate access to PC supplies in any way that would matter. As for Threat III (infiltration, espionage, and disruption), purchasers who feared bugs or surveillance devices within Lenovo PCs could eschew Lenovo and simply purchase any one of numerous alternatives.

2.2.CNOOC-Unocal

Turning next to CNOOC's proposed acquisition of Unocal, the Three Threat assessment tool offered here provides a useful framework for rigorous analysis. Looking solely at the question of whether oil is 'crucial' for the functioning of the home country economy and military, the answer

is clearly yes. Access to oil is critical for the United States, and for the US defense industrial base. For many, this meant case closed![9]

But as shown above, from an analytical point of view the case was far from closed. What about the concentration of alternative suppliers and potential switching costs? What about the potential 'leakage' of sensitive technologies and managerial expertise?

In the year preceding the proposed acquisition (2004), Unocal produced 159,000 barrels of oil per day (70,000 barrels per day in the United States) and 1,510 million cubic feet of gas per day (577 million cubic feet per day in the United States). Thirty three per cent of Unocal's oil and natural gas production was within the United States, while 67% was outside. Unocal had proved reserves of 659 million barrels of oil and 6,658 billion cubic feet of natural gas. Twenty six per cent of these reserves were within the United States, with 64% outside.

Concern was expressed that CNOOC might divert Unocal's energy supplies exclusively to meet Chinese needs. In the extreme, CNOOC might have rerouted Unocal's US production of 70,000 barrels of oil per day and 577 million cubic feet of gas per day back to China. This would have been a highly complicated and expensive undertaking, however, since US pipelines across western states flow west-to-east. Oil from the Gulf of Mexico would have to have been shipped by tanker via the Panama Canal.

The bottom-line question is would this outcome have harmed the United States? As argued above, this diversion would have constituted a 'threat' to US interests – economic, political, or national defense – only if sources of supply were tightly concentrated and switching

[9] Press statements on CNOOC's proposed acquisition of Unocal by Representative Joe Barton (R-Texas) and Representative Duncan Hunter (R-CA).

costs were high. But 21 countries (15 non-OPEC countries) had oil for export in volumes greater than Unocal's entire US production. Six more could have been called upon to make up for a large fraction of Unocal's US output. It is important to reiterate that protection of US interests derives from the dispersed structure and fungible qualities of the international oil industry.

Could US oil from the Gulf of Mexico be used to provision the Chinese People's Liberation Army (PLA)? Certainly, the answer is in the affirmative if the US government did not legally and/or physically block such shipments. But this would penalize the PLA in comparison to provisioning from alternative commercial suppliers nearer to home. If CFIUS strategists could be permitted to enjoy a slyly-mischievous sense of humor, the CFIUS would have *required* that a CNOOC-owned Unocal ship all its North American output back to supply Chinese military forces!

What about the second threat-test? Might the sale of Unocal to CNOOC have represented a leakage – or a loss – of technology that could have damaged the United States? Looking strictly at oil production technology – possible enhancement of Chinese ASW capabilities is considered separately below – the answer is quite to the contrary. If the incorporation of Unocal's technology and managerial expertise into CNOOC would have enhanced the latter's performance in discovering and producing oil, the result would have eased the pressure on world energy markets. That is, the spread of Unocal expertise throughout CNOOC would likely have had a positive (if small) global supply effect. If, as is likely, Unocal engineers and managers would have improved CNOOC performance more than they might improve Chevron performance – Chevron was the alternative bidder for CNOOC – the result would have been a net benefit for US and global energy consumers.

On the demand side, the Chinese thirst for oil is a challenge that the entire world has to cope with. On the supply side, the Chinese drive to develop new energy sources – as argued later in this paper – may be part of the solution, not the problem.

But a complete assessment of CNOOC's proposed acquisition of Unocal requires a second pass through the questions of excessive dependence on the one hand, and potential leakage of technology on the other.

The question of excessive dependence arises because CNOOC's purchase would have included a wholly-owned subsidiary of Unocal, Molycorp, which operates the only rare-earth mine located in the United States at Mountain Pass, California. Molycorp ceased mining production at Mountain Pass in 2003, but the property remained open on a care-and-maintenance basis while reopening production in 2012. As pointed out earlier in this paper, rare-earth supplies have become a matter of concern since 2009 as China has restricted exports and manipulated supply to show its displeasure over foreign policy disputes with Japan. If the CFIUS was to revisit the historical case today, it would want to consider whether Molycorp should have been included in CNOOC's proposed acquisition of Unocal, or whether there should have been a requirement to sell it off separately to an American buyer.

With regard to the potential leakage of sensitive technology, assertions were made that Unocal seismic technology had dual-use possibilities that might reinforce Chinese anti-submarine warfare capabilities as well as enhance Chinese capacity for oil exploration. To investigate these assertions would involve highly specialized, and perhaps highly classified, expertise. Once again, however, the algorithm to be followed would take the form of what has been laid out above. That is, would the acquisition of Unocal seismic technology confer

capabilities that are closely held, and that are not available for purchase or hire to China from other alternative sources?

2.3.Huawei and Vulnerabilities in IT Systems

In late 2007 international private investment firm, Bain Capital, proposed to acquire 3Com, a leading US hardware and software network company based near Boston. The terms of the proposed acquisition included a US$2.2 billion purchase price and a 16.5% minority shareholding by Huawei, which was to include the right to appoint three of 11 Board members (3Com Corporation 2008). Huawei was founded in 1988 by a former Chinese Army officer, Ren Zhengfei. In 2005, it was reported that Huawei had ties with the Chinese government, in particular the People's Liberation Army (PLA) (Medeiros et al. 2005). The Department of Defense's 2008 *Annual Report to Congress on the Military Power of the People's Republic of China* named Huawei as working with the PLA on techniques of cyber warfare (Department of Defense 2008).[10] That report was a precursor to the Report of the House Intelligence Committee in 2012 (Rogers and Ruppersberger 2012).

At the time of the proposed acquisition, 3Com had already formed a joint venture with Huawei in China referred to as H3C. 3Com's parent subsequently bought out Huawei in order to incorporate the former joint venture into the parent's production chain as a wholly-owned affiliate. For its part, Huawei has larger market penetration in Europe than in the United States, and could make use of a stake in 3Com to provide channels into the US market quite independent of any interest in 3Com products or services.

[10] Datang and Zhongxing were also named in the report.

How might the acquisition by Bain have posed a national security risk to the United States? This case provides particular insight into the interaction between Threats II and III.

The roster of 3Com products suggested that there were as many as nine clusters of goods and services that might be considered crucial to the functioning of the US economy (and the US defense industrial base) – and that might provide important capabilities to the Chinese economy (and the Chinese defense industrial base) – that need therefore to be subjected to the concentration-level and switching-costs tests proposed here, including routers, switches, interface cards, and – most importantly – network security systems.

Addressing Threat I first, could the Bain purchase with the Huawei minority stake lead to circumstances (perhaps during a US-China crisis) in which critical 3Com capabilities were withheld from US users? On its face, it would appear implausible that a minority interest acquired by Huawei Technologies would be enough to allow Chinese interests or ultimately the Chinese government to dictate how 3Com goods and services were offered for sale in the market. A large fraction of 3Com products are assembled in the wholly-owned H3C affiliate and shipped from China. These could be embargoed by the Chinese government – along with other output produced or assembled on the mainland by companies such as Cisco or Ericsson – during a foreign policy/military confrontation. But the Huawei share in 3Com would not per se enhance the options available to the Chinese government one way or another.

Turning to Threat II, would the Bain purchase with the Huawei minority stake allow the 'leakage' of sensitive technology or other capabilities to Chinese users that they would not otherwise have access to? A CFIUS threat assessment would want to discern whether, for each of the nine clusters, alternative suppliers were few enough and switching costs were high enough that the acquisition offered a non-reproducible channel to obtain the technology or other

capabilities. A survey of public sources indicates that most of the router, switch and internet card capabilities of 3Com products are rather widely available commercially for Chinese use. Indeed many of these products involve hardware and software already produced in China. A focus of particular attention at the time, however, was 3Com's prize-winning integrated security and intrusion-protection system called 'Tipping Point', which featured US government and military agencies among its purchasers. The 3Com Tipping Point system is built around an ASIC-based engine that performs thousands of high-speed checks on each data packet the recipient receives through the internet.

How concentrated is the international market for this kind of threat suppression engine? A review of commercial sources suggests that there are at least nine US players in this market – including Cisco Systems, Juniper Networks, Sourcefire, IBM, McAfee, Top Layer Networks, Radware, NFR Security, Reflex Security, DeepNines, Still Secure, and NitroSecurity – plus additional European and Asian firms. While specialized expertise would be required to compare the individual attributes of these alternative security systems, it would appear that Chinese agencies have redundant access to capabilities similar to Tipping Point products. In the event, after some initial reluctance 3Com and Bain announced that they were prepared to spin off the Tipping Point operations.

Turning to Threat III, the 3Com case introduced an apprehension that has plagued Huawei ever since – namely, that the acquisition might allow potential insertion of some capability for infiltration, surveillance, or sabotage (via 'backdoors' or 'trapdoors') into the goods or services provided by the company. There was also a concern that can be seen as a special case of Threat III, *viz.* that the proposed acquisition might provide malevolent third parties with insight into weak points of a system that even purchasers and users (including USG

users) might not be fully aware of and hence cannot adequately guard against. In March 2008, Bain announced that it was withdrawing the proposal to acquire 3Com and hence the CFIUS was spared from having to conduct an in-depth assessment of the transaction of the kind proposed in this paper. Two years later, Hewlett Packard bought 3Com and consumers in the United States began to see products from 3Com's Chinese facilities in the US market, an observation that will receive more detailed analysis later.

In 2010, Huawei purchased the patent portfolio and hired some of the staff of 3Leaf, a near-bankrupt Silicon Valley company whose assets had no other bidder. Only after it discovered that the CFIUS was investigating this acquisition did Huawei file an official notice of the transaction. Two months later, the CFIUS informed Huawei that it would recommend to the President that the company divest itself of all 3Leaf assets. In reaction, Huawei issued an 'Open Letter' defending its reputation and inviting US government agencies to investigate the company. In the end, the company accepted the divestiture and agreed to appoint an officer who was responsible for periodically showing US agencies that the company was in compliance.

2.4. A Special Look at Protecting National Security – and Commercial Integrity – in an Era of Global Supply Chains

Cyber security is becoming one of the leading national security and commercial concerns at the highest levels of government around the world. Allegations that the Chinese government is behind the penetration of public and private IT systems are being made precisely at the moment when United States intelligence agencies are revealed to be placing communications under surveillance across the globe.

Governmental cyber attackers, like rogue hackers, need to find entry points to penetrate the IT systems and data bases of those they target. How might it be possible to protect against hardware and software that offer – perhaps even deliberately – such entry points?

Intelligence agencies and congressional leaders in the United States – like their counterparts in Canada and Australia – have fixed on the idea of prohibiting IT suppliers of certain nationalities (in the case of China, Huawei and ZTE) from participating in national telecommunications networks as means of combatting the threat of cyber penetration. How effective is this approach of discriminating against IT suppliers on the basis of national ownership of the provider likely to be? The answer becomes apparent as one drives through Shenzhen on the way to Huawei or ZTE headquarters. Along the highway are facilities and research campuses of Ericsson, Lucent-Alcatel, Samsung, Cisco, Siemens-Nokia, Motorola, Infosys, and NTT Docomo – in short, facilities operated by all the major IT rivals and competitors of Huawei and ZTE. Most of these companies outsource the manufacture of components, in turn, to India, Israel, and Russia, as well as Taiwan, Malaysia, Thailand, and Mexico. In an era of global IT supply chains, the potential for inserting trapdoors, backdoors, and surveillance mechanisms in hardware or software is ubiquitous.

Is it possible to realistically ensure supply chain integrity? The approach that Huawei has taken provides a possible answer. Its own security assurance program offers to place all source code in escrow to a trusted third party that can verify to buyers or governments that goods and services are ‘clean’. The most advanced instance of such vetting is Huawei’s Cyber Security Evaluation Center at Banbury in the United Kingdom, which is staffed by Huawei employees who are UK nationals with UK government security clearances. The center makes a forensic

audit of Huawei hardware and software according to UK government specifications and provides it to UK intelligence and other agencies, which are expected to share information with counterparts in the United States and elsewhere. Hardware and software – including patches and upgrades – must pass inspection and receive an embedded time/date stamp that a subsequent user can verify to ensure that no changes have been made to the code after leaving Banbury.

Complementing this audit of hardware and software is the option that indigenous trusted third party installers – such as Bechtel, CDTI, or TESSCO – can take delivery of goods and services that have been verified as secure and deliver, install, maintain, and manage upgrades/updates for purchasers. If the buyer wishes, therefore, no Huawei individual or entity will touch Huawei goods or services between security audit and installation (or upgrade) with the final user.

Perhaps the vetting process can be improved, but the logical extension of this method for ensuring supply chain integrity is clear. The worldwide community may need an array of independent cyber security assessment cells around the globe that vet the hardware and software of all major IT providers without discrimination, providing results to private clients and governments alike. It is in the interest of IT buyers and suppliers everywhere to devise a system of safeguards and inspections that prevents the compromise of globalized supply chains without disrupting the vital flow of technology.

Singling out foreign producers of IT goods and services on the basis of their nationality and forbidding them from doing business or acquiring companies in the domestic market is ineffective, discriminatory, and unfair. This observation is no less true in Canada and Australia as it is in the United States. The dangers and risks of compromised national security are real. But in a world where supply chains of IT companies of every nationality are thoroughly globalized,

what is needed is a multilateral non-discriminatory system to ensure the integrity of equipment, software, patches, and upgrades from all sources.

3. Applying the Three Threats Prism to Proposed Chinese Acquisitions in Canada

The above framework for separating plausible national security threats from implausible apprehensions and allegations when it comes to foreign acquisitions of a home country firm is proposed here with a view to meeting the needs of all nation states.

From the point of view of an external observer, how might the framework be used in the case of Canada?[11] The first consideration is whether Canada's national interests are best served by an international natural resource supply base that is as diversified and competitive as possible. As discussed later, Australia – and, incidentally, Brazil – occasionally adopts a rhetoric and/or takes policy actions that might be better suited to a quasi-monopsonist resource producer, for example, with regard to exports of coal or iron ore. Does Canada prefer to take a stance as a quasi-monopsonist world supplier of energy or potash, for example, or not? Later, the same question will be posed for the case of Australia.

Secondly, looking more specifically at potential foreign acquisitions of Canadian companies in the extractive sector, the preceding framework would appear to fit Canadian circumstances quite appropriately. While a complete analysis of the evolving structure of the international fertilizer industry is beyond the scope of this paper, the evidence suggests that

[11] This section draws on Moran (2013).

supplies of both potash and phosphates are becoming more concentrated (with the former centered in Canada and the latter centered in Morocco) as US sources diminish. Within this context, BHP-Billiton's hostile bid for Potash Corporation of Saskatchewan would fall into the category of placing external control of a major world source of supply into foreign hands rather than in the category of helping to expand, diversify, and make more competitive the world supplier base. How BHP-Billiton exercised control over output levels, prices, and the destination of sales could become problematic for Canada, even though provincial and national authorities could take steps to try to influence BHP-Billiton's actions post-acquisition. In the extreme, authorities in Ottawa could impose export controls on the acquired company, notwithstanding the controversies such controls would engender.

Popular speculation at the time of the BHP-Billiton bid for Potash Corporation of Saskatchewan suggested that a Chinese or even a Russian firm might be an alternative to BHP. From a national security point of view, neither of these alternative acquirers would be preferable to BHP, since each of these too would represent transferring control of a major world source of supply in an increasingly concentrated industry to an external actor.

3.1. National Security versus Economic 'Net Benefit' Tests

It should be noted that the framework for evaluating the implications of foreign acquisitions introduced here is directed at potential national security threats, and excludes other considerations of 'net benefit' as contained in the *Investment Canada Act*. Thus in the Potash case above, a Chinese or Russian acquirer might offer a higher price to shareholders than BHP-Billiton or might make more generous no-layoff-of-workers commitments. But this would not

alter the calculation in the proposed national security framework – concern about transferring control of a major world source of supply in an increasingly concentrated industry to an external actor would remain. A quick review of the concentrated structure of the international nickel industry suggests that it would have been desirable for China Minmetals' proposed acquisition of Noranda in 2004, which was never completed, to have been subjected to national security examination rather than a simple 'net benefits' assessment.

In contrast to the Potash case, PetroChina's decision to exercise its option to acquire all of the undeveloped MacKay River project from Athabasca would, to the outside observer, appear to be helping to expand and diversify Canada's energy base. The same can be said of Sinopec's acquisition of new drilling lands owned by Calgary-based Day Energy. While both PetroChina and Sinopec embody Chinese state ownership, this does not alter the national security calculus. Nor is the calculus changed by the fact that Chinese companies may be acquiring Canadian firms to obtain access to oil sands production technology for transfer back for use in China's own oil sands, as this would actually help relieve the burden on world energy supplies.

Within the national security perspective offered in this paper, State Owned Enterprises (SOEs) would receive particularly close scrutiny. But there would have to be an acknowledgement that ostensibly independent private investors in a relatively concentrated international industry could equally be subject to home country geopolitical pressures and directives. Ultimately, the overriding question from a national security perspective is the structure of the international industry rather than the ownership structure of the investing entity.

3.2. The Important Case of Chinese Investment in Rare Earths

It is important to note that not all Chinese strategic maneuvers toward natural resource procurement reflect the predominant trend toward making the supplier base more competitive.

Indeed Chinese policies to exercise control over 'rare earth' mining run precisely in the opposite direction.

It is widely recognized that rare earth elements (REE) are crucial for a growing array of civilian and military products. In 2009-2010 China's Ministry of Industry and Information Technology set an export quota of 35,000 tons per year for REE, and issued a potential ban on exports of at least five types of rare earth elements and other steps to control mining. Chinese investors have simultaneously actively sought to acquire equity stakes in new producers of REE, in particular in Australia. Deng Xiaoping is often quoted as pointing out that while the Mideast has oil, China has rare earth elements. In the fall of 2010, Chinese customs authorities refused to issue export licenses for rare earths destined for Japan and perhaps for other countries as well. They subsequently lifted the ban on export licenses. In 2011-2012, Chinese explanations of national policy highlight a desire to consolidate the domestic REE industry to limit environmental damage. Chinese policy actions simultaneously focus on attracting more value-added in processing and using rare earth elements within China. Beyond the economic sphere, Chinese manipulation of REE exports play a role in geopolitical maneuvers vis-à-vis Japan.

Potential acquisitions of Canadian rare earth elements companies might be subjected to the same calculus as Potash. A hypothetical Chinese acquisition of Avalon Rare Metals or Great Western Minerals Group would further consolidate Chinese control over the global REE industry. Indeed Canadian authorities perhaps ought to be concerned about such consolidation even if a proposed Chinese acquisition does not involve a production site on Canadian soil. Again, as a purely hypothetical example, a proposed Chinese acquisition of Great Western Minerals Group's operations at Steenkampskraal in South Africa would qualify to be blocked by Canada on national security grounds.

The above example highlights that national security review along the lines suggested here introduces considerations beyond those that might ordinarily be contained in a standard anti-trust review of a potential acquisition. Canadian authorities would want to be cognizant of Chinese government manipulation of rare earth exports to Japan as part of geo-strategic rivalries in North Asia – and make a judgment about the advisability of permitting a hypothetical Steenkampskraal acquisition in light of Canadian foreign policy considerations – rather than looking solely at anti-competitive grounds in a purely economic sense. In this sense, national security reviews could draw on widely accepted industry concentration measurements, but as suggested earlier, would have to add more subtle considerations of Canadian national interest.

3.3. Conflict of National Interests among Allies as well as Potential Adversaries

The opening section of this paper recalled concerns about Japanese acquisitions of US companies in the 1980s, even as the United States and Japan enjoyed a close international affairs relationship. An examination of recent concerns about foreign acquisitions in Canada shows similar sensitivities with regard to certain proposed US acquisitions. A key case in point is the 2008 proposed purchase of the space technology division of Vancouver-based MacDonald, Dettwiler and Associates (MDA) by Alliant Techsystems Inc. (ATK) of the United States.

MDA asserted that the $1.3 billion sale price would enable the company to devote more resources to its faster growing IT businesses, while getting out from under increasingly burdensome ITAR constraints on doing satellite business in the United States. The Canadian Minister of Industry asserted that the sale did not provide net benefits to Canada. This was an economic argument that would have required comparing benefits to Canada from MDA's proposed expansion in the IT sector with losses associated with ATK's possible relocation of space technology operations outside of Canada. There is no evidence that the 'net benefits'

calculation by the Canadian Minister of Industry included the opportunity cost of reduced MDA expansion in the IT sector.

Approaching the case from a national security point of view, the proposed sale would have transferred control of Radarsat-2, a distinctive high resolution satellite with an unusual polar orbit, to ATK. Alliant obligated itself to honor all of MDA's outstanding contracts and agreements with the Canadian government, including existing access protocols to Radarsat-2 for surveillance of the Arctic. But Alliant could not promise that the US government would refrain from imposing controls on sharing of information gleaned from Radarsat-2 if there were a dispute between the United States and Canada about policies toward sovereignty in the Arctic. The United States rejects Canada's claim over the Northwest Passage shipping channel, for example, and could conceivably have refused to permit Canada to use Radarsat-2 surveillance to enforce its claim. Given the unique nature of Radarsat-2's technology and polar orbit, what has been labeled 'Threat I' earlier would come into play in this scenario since Canada would have no other alternative if the US were to behave in this way.

It is difficult for an outsider to assess the depth and significance of a future hypothetical US-Canada dispute over arctic sovereignty, but the logic of rejecting the proposed acquisition for Canadian national security reasons ('Threat I') does not appear inappropriate even though in actual fact the acquisition was rejected on the grounds that it did not deliver a net benefit to Canada.

The brevity of the above review, which illustrates how the national security threat assessment apparatus proposed by this paper might apply to sensitive cases in Canada, should not mislead about the principal value of using such a rigorous framework. The primary value of such a framework is to show that the vast majority of proposed foreign acquisitions do not pose

any plausible threat whatsoever. Application of this framework in Canada should – as elsewhere – help dampen down the politicization of individual cases and lead to swift and confident approval of those acquisitions where genuine national security threats are totally absent.

4. Applying the Three Threats Prism to Possible Chinese Acquisitions in Australia

Like Canada, Australia has been a rich target of Chinese investments and Chinese acquisitions in the natural resource sector. Once again like Canada, a fundamental strategic choice for Australia is whether the country wants to consolidate its power as a quasi-monopolistic supplier of iron ore, coal, and other industrial commodities in international markets or not.

It is not clear to the outsider exactly how Australian market power toward external markets would be dealt with through an interaction between Australia's *Competition and Consumer Act 2010* (Cth) and the *Foreign Acquisitions and Takeovers Act 1975* (Cth). In any case, general Australian concern for maintaining competitive supplier markets at home and abroad could possibly be somewhat alleviated by examining an investigation that has been ongoing at the Peterson Institute for International Economics (PIIE). The PIIE has for some time now been investigating whether Chinese extractive industry investments around the world have been trying to: 'lock up' the world's resource base for China; gain 'preferential access' to available output; and extend 'control' over the world's extractive industries.

The PIIE investigation recognizes that on the demand side, Chinese appetite for vast amounts of energy and minerals puts significant strain on international markets for oil, natural gas, iron ore, coal, copper, nickel, aluminum, and other materials. But on the supply side, Chinese investments around the globe need not have a zero-sum effect. Chinese efforts to

procure raw materials might actually help solve the problems of strong demand. Which outcome Chinese procurement arrangements generate depends upon whether those arrangements:

- basically solidify a concentrated global supplier system and enhance Chinese ownership/control within that concentrated system; or
- expand, diversify, and make more competitive the global supplier system, and use Chinese ownership/control as a lever for such expansion, diversification, and enhanced competition.

To test which outcome predominates, the PIIE investigation divided Chinese deployment of capital used to procure natural resources into four categories. In the first procurement arrangement (henceforth referred to as Category I), Chinese investors take an equity stake in a very large *already established* producer so as to secure an equity share of production on terms comparable to other co-owners. In the second procurement arrangement (Category II), Chinese investors take an equity stake in an *up-and-coming producer* so as to secure an equity share of production on terms comparable to other co-owners. In the third procurement arrangement (Category III), Chinese buyers and/or the Chinese government make a loan to a *very large already-established producer* in return for a purchase agreement to service the loan. In the fourth procurement arrangement (Category IV), Chinese buyers and/or the Chinese government make a loan to finance an *up-and-coming producer* in return for a purchase agreement to service the loan.

These four structures provide the basis for giving an operational definition to 'tying up' supplies. If the procurement arrangement simply solidifies legal claim to a given structure of production (first and third structures), 'tying up' or gaining 'preferential access' to supplies has

zero-sum implications for other consumers. What is noteworthy, however, is that if the procurement arrangement expands and diversifies sources of output more rapidly than growth in world demand (second and fourth structures), the zero-sum implication vanishes as all consumers (including Chinese purchasers) have easier access to a larger and more competitive global resource base.

The PIIE research first examined the 16 largest Chinese natural resource procurement arrangements around the world within these four categories (Moran 2010). The results showed a few instances in which Chinese natural resource companies take an equity stake to create a 'special relationship' with a major producer. But the predominant pattern (13 of 16 projects) is to take equity stakes and/or write long-term procurement contracts with the competitive fringe. A brief review (to check for selection-bias) of four smaller Chinese procurement arrangements undertaken at the same time did not suggest that there is significant misplaced focus in looking at these 16 largest projects. Three projects in Australia, Myanmar, and Canada show the characteristics of Category II. One project in Indonesia, on the other hand, presented more the characteristics of Category I.

More recent research undertaken at the PIIE provides a comprehensive examination of 34 Chinese natural resource investments and procurement arrangements in Latin America (Kotschwar, Moran, and Muir 2012). Twenty five of the 34 Chinese investments and procurement arrangements served to help diversify and make more competitive the portion of the world natural resource base located in Latin America.

These outcomes hold some good news for host countries since they seem to suggest that Chinese investors are more willing to take on new frontier – or even fringe – projects that the major established oil and mining companies might pass by.

The PIIE scorecard of the 16 largest Chinese natural resource investments as of 2010 includes three instructive cases from Australia. First is the CNOOC-North West Shelf Venture LNG Exports project. In October 2002, Australian based North West Shelf Venture and Guangdong Dapeng LNG Company signed a sales and purchase agreement for the supply of more than 3.3 million tons of LNG per year for 25 years from Australia. With this contract as collateral, CNOOC formed a new joint venture – the China LNG Joint Venture – to invest in LNG. CNOOC received a 25% ownership share in this new joint venture, which diluted the existing Northwest Shelf Venture participants[12] who had all signed the original contract with Guangdong Dapeng to 12.5% each. The oil majors (BP, Chevron, and Shell) who together had held 49.5% of the enterprise were reduced, collectively, to no more than a 37.5% stake. LNG exports began in 2006. In PIIE scoring, this qualifies as Category II.

Second is the Chalco-Aurukun Australia Bauxite Project of 2007. In 2004 the Queensland government moved to end its contract with the Canadian 'major', Alcan, which had tied up bauxite reserves at Aurukun for more than a decade but had never entered into development. The Aluminum Corporation of China (Chalco) purchased rights to develop a new $3 billion bauxite project near Aurukun, Queensland, in September 2007. The project includes a bauxite mine at Aurukun, and an alumina refinery and port facilities at Abbot Point near Bowen. Chalco lost the lease to Aurukun in 2011 when it could not complete investment in a smelter, but entered the running again in 2013 as one of several contenders for the project. This qualifies as a Category II project.

[12] Woodside Energy, BHP Billiton, BP Australia, Chevron Australia, Japan Australia, and Shell Australia.

Third – and most interesting – is the Chinalco-Rio Tinto proposed deal of 2008-2009, which was ultimately aborted. In February 2008, China's state-owned metals multinational Chinalco acquired 9% of the shares in Australia's Rio Tinto for US$15.5 billion. Rio Tinto is one of the top five international producers (by volume) of aluminum, iron ore, copper, gold, diamonds, and other industrial materials; it is also the second largest supplier of iron ore to world export markets (Rio Tinto PLC 2008). In February 2009, Chinalco and Rio Tinto signed an agreement to increase Chinalco's stake in Rio for US$19.5 billion. The agreement included the purchase of convertible bonds that (if converted) would increase Chinalco's ownership share to 18% of the Rio Tinto Group. Chinalco thereby obtained the right to nominate two new non-executive directors to add to the then 15 Board members of Rio Tinto. Independent non-executive directors comprise a majority of the Rio Tinto Board.

At first glance, the two transactions between Chinalco and Rio Tinto would appear to fit into Category I above, with Chinalco trying to consolidate a special relationship with a 'major' in the natural resource sector (in particular, iron ore and aluminum). But according to Drysdale and Findlay (2009), this Chinese maneuver has to be seen in light of BHP Billiton's hostile bid in 2008 to take over Rio Tinto (378). Chinese steelmakers estimated that a merged corporation comprising both BHP Billiton and Rio Tinto would enjoy a market share of world iron ore output as large as the joint output of all OPEC members in the global oil market. At a meeting in Beijing of Chinese government officials, steelmakers, China's largest coal mining companies, and the China Development Bank, the then President of Chinalco proposed that the company present itself as a 'white knight' in Rio Tinto's attempt to avoid the unwanted takeover (Oster

and Carew 2009, A1).[13] Chinalco's explicit objective was 'to stymie' any super-merger between BHP Billiton and Rio Tinto. Rather than falling into Category I above (industry consolidation), the Chinalco-Rio Tinto deal should probably be assigned to Category II, that of trying to keep a large player functioning in a competitive manner.[14]

As Australia's Foreign Investment Review Board prepared an analysis of the deal in the midst of intensive public controversy, Rio Tinto abruptly decided to reverse course and reject the Chinalco arrangement paying a $195 million break fee (Beverage 2009; Wines 2009, A1). Rio Tinto substituted the agreement with Chinalco for a $15 billion rights issue, backed by the formation of a 50-50 production joint venture with BHP Billiton covering 'the entirety of both companies' current and future Western Australian iron ore assets'.[15] The result was a smaller Chinese equity stake in the Australian mining industry, and a potentially more consolidated industry headquartered in Australia: Chinalco's prior 9% holding in Rio Tinto would be diluted by the rights offering, and the company would not be able to exercise veto power over the proposed consolidation of the two great iron ore producers.[16] So this episode represents a failed Category II strategy on the part of the Chinese.

Thus Chinese investments in Australian natural resources have served, as elsewhere, primarily to help diversify and keep competitive supplies of energy and minerals. This strategy on the part of government-backed Chinese investors and lending agencies will not come as a

---

[13] The larger equity stake allowed Chinalco to exercise veto power over the 'Great Acquisition'.

[14] Days after making the 2009 offer to increase Chinalco's stake in Rio Tinto, Chinalco's President XiaoYaqing was 'promoted' to a new post in China's cabinet.

[15] Available at http://www.riotinto.com. Accessed June 30, 2013.

[16] In the event, the proposed joint venture between Rio Tinto and BHP Billiton did not proceed.

surprise to those who have examined the evolution of the Japanese approach to natural resource procurement. In the early resource struggles of the 1970s the Japanese government entertained the idea of creating the country's own major 'national champion' resource companies, or of engaging in Category I and Category III strategies to secure a 'special relationship' with major resource companies and/or producer governments. From the late 1970s through the 1980s, however, Japanese policies shifted toward Category II and IV strategies and Japanese procurement became a major force in enhancing the competitive structure of global extractive industries and diversifying the geography of production (Wells 1993). Japanese participation in energy and mining projects today consists primarily of minority equity stakes in a large array of extractive projects, backed by purchase contracts for a portion of the output.

As in the case of Canada and the United States, Australia's Foreign Investment Review Board should be wary of any proposed Chinese acquisition of a company that is involved in the development of rare earth projects. Lynas Corporation might one day again be a target, or Arafura Resources, Peak Resources, Hastings Rare Metals, or Victory Metals.[17] Just as Canadian authorities might want to exercise extraterritorial control over a Chinese proposal to take over South African projects owned by Canadian mining companies, Australian authorities would want to monitor any Chinese interest in Lynas Corporation's Malaysian holdings.

Finally, there remains the issue of Threat III concerns (backdoors, trapdoors, surveillance, or espionage portholes) associated with foreign acquisitions of Australian IT firms, or sales of IT hardware and software to Australian IT companies. Australian authorities will

---

[17] Lynas was targeted by CNMC in 2009, but CNMC ultimately withdrew its offer as it saw conditions imposed by the Foreign Investment Review Board as intolerable: see for example http://www.abc.net.au/lateline/business/items/200909/s2695949.htm.

want to investigate measures to vet the supply chains of all companies, rather than trying to solve the challenge of cyber security by banning acquisitions or purchases involving corporations of particular national origin.

5. Toward a Multilateral Non-Discriminatory Framework for Separating Plausible from Implausible National Security Threats Posed by Foreign Acquisitions

Contemporary work at the Peterson Institute suggests that the 'Three Threats' perspective introduced here could be generalized for adoption by all OECD countries and beyond. Looking first at the OECD (of which the United States, Canada, and Australia are of course members), the 'three threats' perspective complements and enhances the goals set forth in the OECD's *Guidelines for Recipient Country Investment Policies Relating to National Security* (2009) of:

- transparency of policies;
- predictability of outcomes;
- measures of general application, which treat similarly situated investors in a similar fashion;
- proportionality of measures; and
- accountability of implementing authorities (Recommendation adopted by the OECD Council on 25 May 2009).

Common use of the decision tree (below) as a tool for threat assessment would improve upon the OECD Guidelines in two ways. First, the guidelines permit that 'essential security concerns are self-judging'. That is, 'OECD investment instruments recognize that each country has a right to determine what is necessary to protect its national security'. The decision-tree below would impose a common discipline for all OECD members to evaluate whether concerns

about a possible national security threat are plausible. Second, the OECD Investment Committee occasionally uses the term 'Strategic Industries' in ways that suggest entire sectors – energy, military suppliers, financial institutions, infrastructure – might be excluded from foreign takeovers. In contrast, the threat assessment tool developed in this paper deliberately discriminates as to when a proposed foreign acquisition within such sectors might pose a threat and when it does not.

OECD-Wide (or World-Wide) Decision-Tree

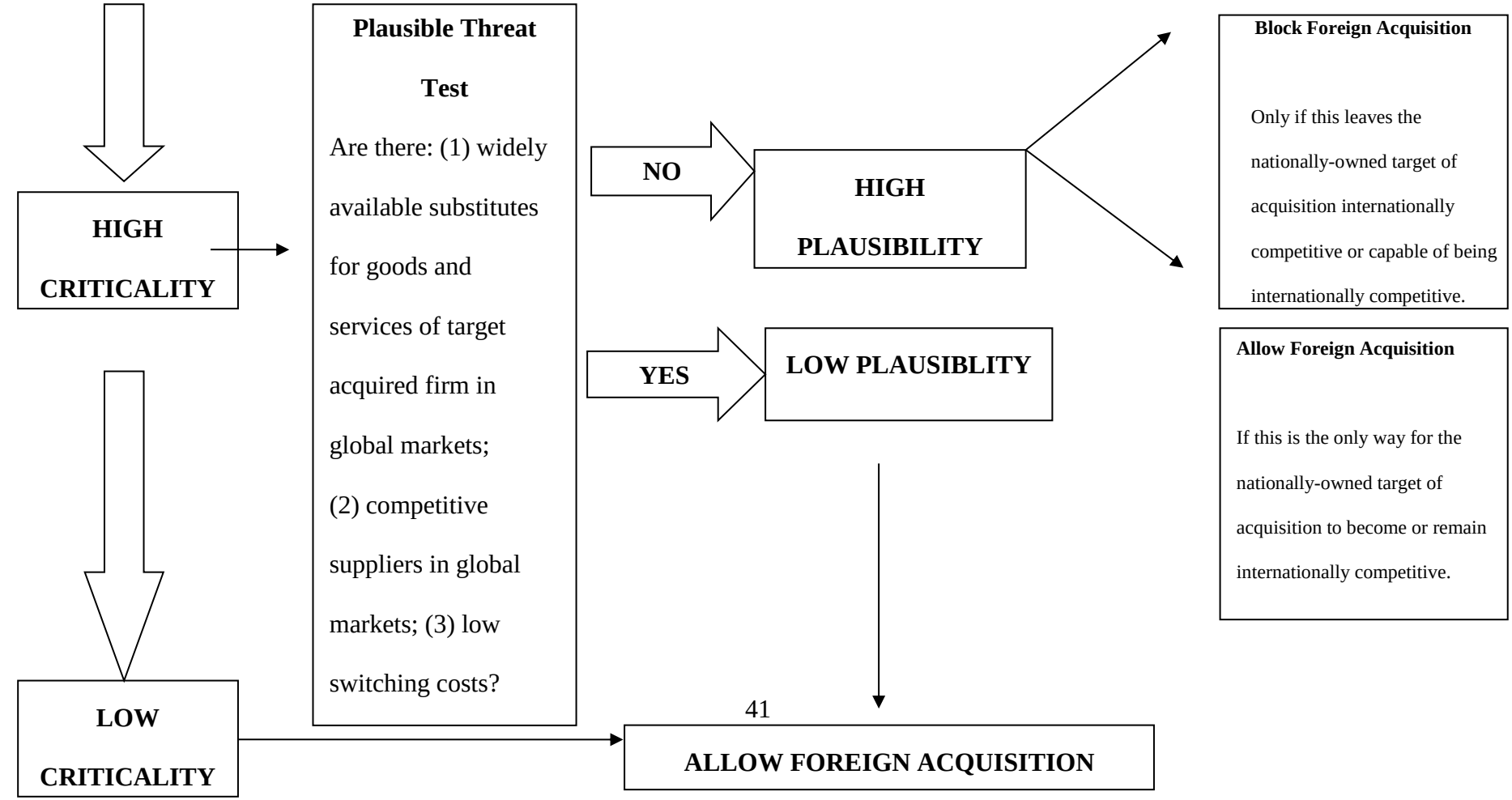
When is there a Plausible National Security Rationale to Block a Proposed Foreign Acquisition?

CRITICALITY TEST

THREAT I How much would the costs be if provision of the target firm's goods or services was denied or conditions were placed upon supply?

THREAT II How much national security-related advantage would be gained by the foreign purchaser and its government if the foreigner gained control of the target firm?

THREAT III How extensive would the damage be from surveillance or disruption via foreign ownership of a given network?



Is there some quantitative standard that might be used to guide an OECD-wide – or worldwide – 'plausible threat test'; that is, to determine whether there are 'widely available substitutes for goods and services of the target acquired firm in global markets, competitive suppliers in global markets, and low switching costs'? The most obvious tool to operationalize the degree of competition among suppliers is to use the long-standing US Department of Justice and Federal Trade Commission (2006) guidelines on mergers and acquisitions. Guidance provided by the similar European Commission's Directorate-General for Competition would be another option (European Union 2008). The goal, however, is not to turn the national security framework into an anti-trust issue. Rather, the goal is to limit national security scrutiny to circumstances in which:

- denial of access to an acquired firm's goods or services would impose high costs;
- unwanted advantage to the foreign purchaser and its government would be large; or
- damage from surveillance or disruption via foreign ownership of a supplier would be unavoidable.

In each case, national security monitors would want to look for consequences that affect the home country in ways much beyond the raising of prices.

This threat assessment framework need not be limited to OECD members. The same logic would make it applicable to all countries, including China or Russia. This threat assessment framework could thus become the basis for a worldwide multilateral approach. US, Canadian, or Australian multinational investors could face mirror-image policies in other countries without undue concern. Indeed acceptance of such a common

framework would help reduce arbitrary or nationalistic discrimination against non-threatening foreign acquisitions.

References

3Com Corporation. 2008. *Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934*. Washington DC: United States Securities and Exchange Commission. January 24.

An Act to Enhance the Competitiveness of American Industry, and for Other Purposes, HR 4848 100th Congress (1988).

Beverage, John. 2009. "Rio Tinto Deal Leaves a List of Winners and Losers." *Herald Sun*, June 6.

Drysdale, Peter, and Christopher Findlay. 2009. "Chinese Foreign Direct Investment in the Australian Resource Sector." In *China's New Place in a World in Crisis*, edited by Ross Garnaut, Ligang Song, and Wing Thye Woo, 349-388. Canberra: ANU E-Press. http://epress.anu.edu.au/titles/china-update-series/china_new_place_citation.

European Union. January 2008. "European Commission's Directorate-General for Competition (EU DG Competition)." European Union. http://ec.europa.eu/comm/competition/general_info/h_en.html.

Foreign Investment and National Security Act of 2007, HR 556 110th Congress, Public Law No: 110-49 (2007).

Graham, Edward M., and David M. Marchick. 2006. *US National Security and Foreign Direct Investment.* Washington DC: Peterson Institute for International Economics.

House of Representatives. 1991. *National Security Takeovers and Technology Preservation: Hearings before the Subcommittee on Commerce, Consumer Protection, and Competitiveness of the Committee on Energy and Commerce*. Washington DC: US Government Printing Office. February 26 and June 12.

Kotschwar, Barbara, Theodore H. Moran, and Julia Muir. 2012. *Chinese Investment in Latin American Resources: the Good, the Bad, and the Ugly.* Working Paper 12-3. Washington DC: Peterson Institute for International Economics.

Medeiros, Evan S., Roger Cliff, Keith Crane, and James C. Mulvenon. 2005. *A New Direction for China's Defense Industry*. Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/monographs/MG334.

Moran, Theodore H. 1992. *Materials Prepared for the Subcommittee on Defense Industry and Technology, Senate Armed Services Committee*. April 30. Unpublished, confidential.

Moran, Theodore H. 2009. *Three Threats: An Analytical Framework for the CFIUS Process.* Policy Analysis in International Economics No. 89. Washington DC: Peterson Institute for International Economics. August.

Moran, Theodore H. 2010. *China's Strategy to Secure Natural Resources: Risks, Dangers, and Opportunities.* Policy Analysis in International Economics No. 92. Washington DC: Peterson Institute for International Economics.

Moran, Theodore H. 2013. *Materials Prepared for the Canadian Council of Chief Executives and the Canadian Security Intelligence Service*. Unpublished, confidential.

Moran, Theodore H., and Lindsay Oldenski. Forthcoming. *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China.* Washington DC: Peterson Institute for International Economics.

Organization for Economic Cooperation and Development (OECD). 2008. *Guidelines for Recipient Country Investment Policies Relating to National Security*. OECD. http://www.oecd.org/daf/inv/investment-policy/41807723.pdf.

Oster, Shai, and Pick Carew. 2009. "China Inc.'s Top Deal Maker Provokes a Backlash Abroad." *Wall Street Journal*, April 16.

Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, Final Rule. 31 CFR Part 800. Federal Register / Vol. 73, No. 226 / (2008).

Rio Tinto PLC. 2008. *Annual Report and Financial Statements*. Rio Tinto. http://www.riotinto.com.

Rogers, Mike, and Dutch Ruppersberger. 2012. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Report by the Permanent Select Committee on Intelligence. US House of Representatives (112th Congress). October 8. http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

US Department of Justice, and Federal Trade Commission. 2006. *Commentary on the Horizontal Merger Guidelines.* Washington: US Government Printing Office. March. www.usdoj.gov/atr/public/guidelines/215247.htm.

Wells, Louis T. Jr. 1993. "Minerals: Eroding Oligopolies." In *Beyond Free Trade: Firms, Governments, and Global Competition*, edited by D.B. Yoffie, 335-384. Boston: Harvard Business School Press.

Wines, Michael. 2009. "Australia, Nourishing China's Economic Engine, Questions Ties." *New York Times*, June 3.