CFIUS and National Security: Challenges for the United States, Opportunities for the European Union

Theodore H. Moran[1]
February 19, 2017 draft

Overview

The legislative mandate of Committee on Foreign Investment in the US (CFIUS) is to protect the United States against national security threats that might emerge from foreign takeovers of US firms.

The regulations that surround the operations of CFIUS grew by accretion following the initial attachment of the Exon-Florio provision to the Omnibus Trade Act of 1988. In 2009 they were comprehensively revised under the Foreign Investment and National Security Act (FINSA) in the face of widespread concern across the political spectrum in Washington that the treatment of foreign acquisitions had become too politicized and erratic to adequately serve US national interests.

This paper argues that since 2009 the assessments of proposed acquisitions by the Committee on Foreign Investment in the United States (CFIUS) have grown steadily more rigorous and predictable, with the aim of separating plausible national security threats from implausible apprehensions on a case-by-case basis, up to the present.

The paper goes on to suggest that the CFIUS experience in evaluating those conditions under which genuine national security threats might emerge when foreigners acquire US firms, and when not, might provide useful lessons and principles for other nations to adopt, in particular the EU and its member states.

The paper opens by examining the tension between appreciation of the substantial benefits to the United States from foreign investment, including foreign investment via acquisition of US companies, on the one hand, and concern about threats to US national security, on the other. The paper then introduces a "Three Threat" framework for identifying genuine national security threats that can be inferred from CFIUS cases, and illustrates the application of this framework to

[1] Theodore H. Moran is Marcus Wallenberg Professor of International Business and Finance, Georgetown University. He is a Nonresident Senior Fellow at the Peterson Institute for International Economics. From 2007-2013, Dr. Moran served as Associate to the US National Intelligence Council (NIC) dealing with CFIUS issues. In 2012 he was invited to design and teach in the USG-sponsored course that certifies the staff members from the CFIUS agencies and CFIUS-related intelligence services. He is a Member of the International Advisory Council of Huawei.

concrete acquisition proposals, leading thereby to approvals in some instances and rejections in others.

This paper points out that CFIUS investigations in the United States take a deliberately narrow look at potential national security threats that precludes more sweeping approaches to approving or denying foreign acquisitions: CFIUS focuses on identifying threats within sectors (such as within the energy industry or within the telecom industry), for example, not precluding entire sectors from foreign acquisitions. CFIUS devotes heightened attention to State-Owned-Enterprises (SOEs) but limits such attention to national security concerns, not possible unfair competition. CFIUS does not participate in designing an industrial policy for the United States, such as preserving national ownership in particular industries or thwarting the extraction of commercial technology by foreigners. CFIUS does not apply a national economic-benefits test to foreign acquisitions, nor does CFIUS base approvals or rejections of specific transactions on reciprocal treatment for US investors in the country of the acquiring firm.

This narrow focus by CFIUS on national security threats is currently being challenged across many fronts, however, by the economic advisers of the Trump administration, by the US-China Commission on Economics and Security, by diverse members of the House and Senate, and by the Council of Advisers on Science and Technology of the former Obama administration. At the direction of Congress, the Government Accountability Office (GAO) is preparing an assessment of recommendations to empower CFIUS with fundamental and significant new mandates (due early 2017). These possible new directives include excluding entire sectors of the US economy from acquisitions by firms of certain national origin (such as Russia or China), designing an industrial policy to keep innovation and manufacturing in the United States while preventing technology transfer to outsiders, blocking acquisitions by SOEs that have access to cheap capital or other special treatment at home, conditioning CFIUS approvals on whether home-countries subsidize exports or dump products in the US market, and tying approval or rejection of individual acquisitions to reciprocity toward US investment in the home economy of the acquiring firm.

This paper evaluates proposals to require CFIUS to pursue new objectives beyond investigating national security threats arising from specific cases, and warns that broadening CFIUS's mandate along such lines opens the door to protectionist moves on the part of other countries, invites retaliation against US investors abroad, and threatens the on-going benefits that derive from freer flows of investment across borders.

This paper argues that maintaining CFIUS's current approach to separating genuine national security threats from implausible apprehensions – on a case-by-case basis -- is best for the United States, and best for the international economic system.

The paper finishes by examining contemporary debates about foreign acquisitions and national security in the European Union.[2] The paper concludes that CFIUS's narrow approach to threat

[2]Guy Chazan. "EU capitals seek stronger right of veto on Chinese takeovers". *Financial Times.* February 14, 2017. Jost Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, Björn Conrad. 2016. *MADE IN CHINA 2025. The making of a high-tech superpower and consequences*

assessment might serve as a framework for individual EU member states and for the EU as a whole.

I. The Setting: Tension between Concrete Benefits from Inward FDI and Politicized Apprehensions about Threats to National Security from Foreign Acquisitions of US Companies

Foreign investors make particularly significant contributions to the US domestic economy. Non-US MNCs in the United States join US MNCs in paying higher wages, offering greater benefits, exhibiting higher productivity, exporting more goods and services, and engaging in greater R&D than purely domestic firms. At the same time, foreign investors put competitive pressure on US firms to upgrade their technologies, management practices, and quality-control procedures, and often offer channels for learning and imitation by US firms. Indeed, the most recent data show that *twelve percent of all productivity gains by firms in the US economy over more than two decades can be traced to spillovers from foreign investors*.[3] Such spillovers originate from foreign investors from BRIC countries – such as China, Russia, and Brazil – as well as from foreign companies headquartered in OECD economies.

For this reason, the US government – as well as US state and local governments – have been eager to welcome foreign investors into their midst. Multinational investors in Europe and Asia exhibit similar superior characteristics in comparison to domestic firms in the host economy.

In the US, as in other developed country markets, approximately eighty percent of foreign investments take place via acquisition of a target firm in the target country, depending upon the industry. This leads to concern that under certain circumstances the foreign take-over of a US firm might pose some kind of national security threat to the US.

The creation of the Committee on Foreign Investment in the US (CFIUS) sprang from a desire to protect the United States against national security threats that might emerge from foreign takeovers of US firms. Originating in reaction to Japanese acquisitions of US companies in the mid-1980s, CFIUS was buffeted by political crosswinds for almost two decades until a regulatory restructuring took place in 2007-2009 with the aim of establishing the legal primacy of the CFIUS process and providing some protection from congressional pressures.

---

for industrial countries. Mercator Institute for China Studies. No. 2, December.

[3]Theodore H. Moran and Lindsay Oldenski. 2013. *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China*. Policy Analyses in International Economics 100. Washington: Peterson Institute for International Economics.

The most frequently cited case that provoked reform of CFIUS legislation involved Dubai Ports World, in 2006.

In that year a company headquartered in Dubai, called Dubai Ports World, acquired the Peninsular and Oriental Steam Navigation Company (P&O), a British firm.[4] 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. CFIUS reviewed the proposed acquisition carefully, and gave approval to the transaction, subject to the strict mitigation arrangements discussed below.

But public reaction in the US Congress and the press became caught up in the fear that the new parent company (in crude post 9/11 public opinion, an "Arab" parent company) might be lax in allowing dangerous persons or cargo to enter the United States, via these port facilities. A bipartisan group of ten senators, led by Charles Schumer of New York, signed a letter to the Senate leadership insisting that Congress be allowed to review CFIUS's appraisal of the transaction, and vote to approve or disapprove the CFIUS decision. The House Appropriations Committee passed a resolution of disapproval of the acquisition, 62 to 4.

In point of fact, the six American ports to be acquired by DP World would be subject to the same container inspection and immigration regulations as any other US port. Moreover, on top of this, CFIUS had taken the extra precaution of having the Department of Homeland Security negotiate a *"letter of assurances"* with DP World, stipulating that the company would operate all US facilities with management by US nationals, would designate a corporate officer of American citizenship vetted by the FBI to serve as point of contract with DHS on all security matters, to promptly provide any and all information DHS might request, and to assist other US law enforcement agencies on any matters related to port security. So the US ports managed by DP World would be the most carefully inspected ports in America.

Despite CFIUS approval, the political opposition to the proposed take-over was so vociferous, however, that Dubai Ports World announced that it had no choice but to sell off all US port facilities acquired from P&O to a buyer of US nationality.

In reaction to the politicization of this case and the seeming denial of regulatory primacy for the Committee, CFIUS regulations were therefore re-written in 2007 and received final approval in 2009 under the title of the Foreign Investment and National Security Act (FINSA). FINSA ensured the legal preeminence of CFIUS in assessing national security threats that might arise from foreign acquisitions of US companies, regularized CFIUS reporting requirements to the US Congress, and provided a degree of insulation from Congressional pressures.

As in earlier CFIUS regulations, the definition of national security was not explicitly defined, except to point out that foreign acquisition of "critical infrastructure" should be subject to special scrutiny. In addition, foreign acquisitions that involve "control" by a foreign government were

[4]Moran, Theodore H. 2009. *Three Threats: An Analytical Framework for the CFIUS Process.* Policy Analyses in International Economics 89. Washington: Peterson Institute for International Economics. Moran and Oldenski. 2013. *Op. cit.*

required to undergo both the initial 30 day investigation and a subsequent 45 day more detailed examination – "control" was defined very broadly in terms of foreign government influence; "control" was not limited to majority foreign government ownership. FINSA eliminated the safe harbor that had protected transactions cleared by CFIUS from future scrutiny (and potential unwinding), if parties to the transaction intentionally and materially breached any term of a mitigation agreement. FINSA introduced the US intelligence community, through the Director of National Intelligence, as a non-voting member of CFIUS and required an intelligence assessment for all CFIUS cases, while maintaining the confidentiality of information provided to CFIUS as well as CFIUS deliberations and determinations.

II. Separating Genuine National Security Threats from Implausible Apprehensions: A "Three Threat" Framework Inferred from CFIUS Decisions

As noted above, the FINSA redraft of CFIUS regulations in 2009 left the definition of threats to national security open-ended, but an empirical examination of CFIUS cases shows such that the threats can be separated into three distinct types, and the conditions under which each threat becomes plausible can be distinguished from situations in which the harm envisioned is not credible.

The first threat derives from a possible leakage of sensitive technology to a foreign company or government that might deploy or sell such technology so as to be harmful to US national interests. To assess the plausibility of Threat I is a two-step process. Step one is to calculate the damage that could be done if the technology were deployed against US interests. Step two is to calculate how readily available such technology is in international markets to see if it made sense to refuse the transfer to foreign hands. If alternative sources of the technology held by the acquired firm are widespread, national security will not be served by blocking the transaction.

The second threat springs from the ability of the foreign acquisitor, acting independently or under instructions from the home government, to delay, deny, or place conditions upon provision of output from the newly acquired producer. To assess the plausibility of this Threat II manipulation of access also requires a two-step analytic process. The first step is a calculation of how "crucial" or "critical" the process or product is—crucial or critical is defined as the cost of delay or doing without. The second step is a calculation of how concentrated the international industry is, how abundant are near-substitutes to the processes or products of the company that is being acquired, and how high are switching costs. If the goods and services of the company being acquired are widely available and switching costs are low, there is no plausible threat to US national security.

The third threat derives from the potential that acquisition of a US company might allow a foreign company or its government to penetrate the US company's systems so as to monitor, conduct surveillance, or place destructive malware within those systems. If alternative suppliers of the goods and services from the company to be acquired are readily available, any user who feared penetration could simply switch to another provider. This Threat III is particularly prominent in assessing foreign acquisitions involving critical infrastructure. Figuring out how to

cope with this threat in a world of globalized supply chains—especially globalized supply chains in the information technology (IT) sector—creates difficult quandaries for CFIUS.

It is important to specify that *only if* the US firm to be acquired controls access to a critical good or service that does not have substitutes in the international market, *or if* the US firm to be acquired gives over a sensitive semi-unique technology that could be deployed at great cost against US interests, *or if* the target US firm could be used for penetration or surveillance in ways damaging to the United States without the ability of US users to switch to other more secure alternatives, *or if* (as a special case of Threat III) the target US firm has properties close to US military installations so as to allow surveillance, might a credible threat to national security be present.

III. Assessment of Possible National Security Threats in CFIUS Cases

The principles upon which CFIUS bases its decisions are not laid out in CFIUS legislation, nor are they articulated by the Committee. They can be identified, however, by examining specific CFIUS cases in which the proposed foreign acquisition was approved or denied.

Illustrations of Threat I (Leakage of Sensitive Technology) in CFIUS Assessment:

The Philips Lumileds Case

In 2015 the Dutch electronics company Philips proposed a $3.3 billion deal to sell 80 percent of its Lumileds division to GO Scale Capital, which is made up of GSR Ventures, Oak Investment Partners, Asia Pacific Resource Development, plus the Nanchang Industrial Group of China. At first glance, the sale might appear to involve nothing more the transfer of a standard commercial lighting device affiliate to Chinese control. But closer investigation revealed that Philips was experimenting with cutting-edge equipment that utilized a substance called gallium nitride (GaN), which is important for advanced radar and anti-ballistic missile systems. CFIUS claimed jurisdiction over the proposed acquisition due to the large Philips presence in the US market, and refused permission for the acquisition.

Although neither Philips not CFIUS would comment on why the acquisition was blocked, it became clear that the sale of this affiliate would involve transfer of the sensitive gallium nitride technology to parties that could be accessed by the Chinese government (Threat I). GaN technology can improve military applications such as radar transmitters by magnifying their power while consuming less electricity. The technology is being used to boost performance of systems such as the US THAAD antimissile system to be deployed in South Korea against North Korea's ballistic missile threat, as well as to upgrade U.S. Navy programs to jam enemy radars.

The Aixtron-Fujian Grand Chip Investment Fund Case

The German semiconductor firm Aixtron announced in November 2016 that CFIUS had recommended that their proposed acquisition by Grand Chip Investment GmbH, the German unit of China's Fujian Grand Chip Investment Fund LP, be abandoned because there were no

possible remedies to mitigate the agency's national security concerns. The rejection of the acquisition did not spring from Aixtron's position as a high performance player in the semiconductor industry, however. Instead CFIUS concerns -- once again, as in the Philips Lumileds case -- focused on potential leakage of gallium nitride technology (GaN) since Aixtron, like Philips, is a key supplier of GaN products to NATO defense contractors.

The Lenovo-IBM PC Case

These two semiconductor cases contrast with Lenovo's earlier proposal in 2005 to acquire IBM's personal computer business. The proposed acquisition would make Lenovo the third largest producer of personal computers in the world by volume, with sales to US government and US defense industry users as well as to private sector customers. But by 2005 PC technology had become "commoditized", with multiple choices of products with comparable characteristics available to buyers around the world. As a result, Lenovo's acquisition of IBM's PC business did not represent a "leakage" of sensitive technology, nor provide China with military-application or dual-use capabilities that were not readily available elsewhere. CFIUS approved Lenovo's acquisition without mitigation.

Kuka Medea

Another case involving sensitive technology is the acquisition of German robotics maker Kuka by the Chinese electrical appliance manufacturer Medea. The issue of concern here is not transfer of advanced robotic technology per se, but rather leakage of sensitive production and system-integration know-how. Kuku is a major participant in Northrop Grumman's F-35 assembly operations. Kuku does not simply sell robots to Northrop Grumman; in addition engineers from Kuka's design-production-division and robotics-systems-division have been deeply involved in setting up, maintaining, and upgrading what Northrop calls its "integrated production line". These Kuka engineers work alongside counterparts from other companies responsible for advanced propulsion, stealth characteristics, and IT coordination for the F-35, and help weave all such systems together.

Kuka's announcement that CFIUS had approved the transaction did not indicate whether any mitigation and divestiture would be required. Kuka and Medea expect the acquisition to be completed in the first half of 2017.

<u>Illustrations of Threat II (Denial or Manipulation of Access to a Critical Input) in CFIUS Assessment</u>:

Chinese Acquisition of a Canadian Rare Earths Mining Company Case

In 2015 a Chinese mining company made a non-public proposal to acquire a Canadian mining firm that owned rare-earths properties in Canada, the US, and South Africa. China already controls approximately 90 percent of rate-earth exports that are critical for the aerospace and

automotive industries. The Chinese government has ordered the withholding of rare-earth exports to Japan during periods of time when disputes about islands claimed by both China and Japan have flared up. CFIUS joined its counterpart in Canada in advising the parties (even prior to public announcement of the proposed acquisition) that the deal would not be permitted to go through. This represents a contemporary illustration of concern about Threat II, the threat of denial or manipulation of access to critical inputs for which there are few readily available substitutes.

Russian Acquisition of Oregon Steel Case

This rare-earths case contrasts with the proposal of the Russian company Evraz, owned by the billionaire Roman Abramovich who enjoys close ties with the Kremlin, to acquire Oregon Steel in 2006, a relatively small producer of structural steel products. As indicated earlier, the assessment whether a foreign acquisition poses a serious threat via manipulation of supply is a two step process: first, an evaluation of whether the good or service to be acquired by the foreign firm is crucial to the functioning of the US economy, including but not limited to its military services; and second, an evaluation of whether there are numerous alternative suppliers and whether switching costs are high.

The first evaluation about the criticality of access to steel clearly raises flags: steel is a major component of more than 4000 kinds of military equipment, from warships, tanks, and artillery to components and subassemblies of myriad defense systems. Uninterrupted access to steel is likewise crucial for the every-day 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 percent of the global steel trade. Alternative sources of supply are widely dispersed, with ten countries that export more than 10 million metric tons (Japan, Russia, Ukraine, Germany, Belgium-Luxembourg, France, South Korea, Brazil, Italy, and Turkey). There are twenty additional suppliers that export more than 5 million metric tons. The number of alternative sources of structural steel products available to US buyers is high and switching costs from one to another are low. So while the steel industry remains vital to US national economic and security interests, the ability of Russian-owned Oregon Steel to do damage by withholding supply is very low.

The threat that China would enhance its ability to manipulate supply of rare earths by acquiring new properties in Canada, South Africa, and the US is credible. The threat that Russia might gain a meaningful ability to manipulate supply of structural steel by acquiring Oregon Steel is not.

<u>Illustrations of Threat III (Penetration, Surveillance, and Sabotage) in CFIUS Assessments</u>:

The Huawei-Bain Capital-3Com Case

In 2007 Bain Capital proposed to acquire 3Com, a leading US hardware and software network company based near Boston, for $2.2 billion, with 16.5 percent minority shareholding by Huawei (including the right to appoint three of eleven Board members). Huawei was founded in 1988 by a former Chinese Army officer, Ren Zhengfei. The 3 Com case introduced an apprehension that

has plagued Huawei ever since; namely, that the acquisition might allow Huawei to insert some capability for infiltration, surveillance, or sabotage (via "backdoors" or "trapdoors") into the goods or services provided by the acquired company. CFIUS never ruled on the case, but in the midst of critical outbursts from Congress Bain announced that it was withdrawing the proposal to acquire 3Com in 2008.

The Lenovo-IBM X-86 Servers Case

More recently, in 2014, Threat III preoccupations also emerged in Lenovo's proposed acquisition of IBM's X86 server business. The IBM low-end X86 server was widely used by US businesses, US government agencies (including defense and intelligence agencies), and principal IT trunk carriers like ATT and Verizon. The Threat III concern was that these commonplace X86 servers might become a vehicle for some kind of penetration by Chinese agencies, once Lenovo took over production.

Threat III assessments—involving penetration, surveillance, or placing malware in the goods and services of the acquired firm—pose a conundrum for CFIUS in an era of globalized IT supply chains, like today.[5] The basic building blocks of all IT systems—including servers, routers, data storage and retrieval mechanisms, flash drives, and microchips—have hardware and software components that derive from production sites in China, Taiwan, Russia, Israel, Eastern Europe, Malaysia, the Philippines, and Mexico, all of which are susceptible to surreptitious engineering input placements. It is not logical to think that Threat III penetrations can be eliminated by singling out and discriminating against providers on the basis of the parent company's national origin, such as rejecting Chinese-owned providers while allowing purchases of hardware and software from US or, say, French firms (Lucent-Alcatel) or Swedish firms (Ericsson) whose assembly facilities sit adjacent to the plants of Chinese-owned firms in Shenzhen.

In Lenovo's proposed acquisition of IBM's X86 server business, CFIUS had to face the conundrum of globalized supply chains head on. Most X86s were already produced in China, by Hewlett-Packard and Dell, for example, as well as by IBM, using thousands of Chinese engineers and tens of thousands of Chinese inputs. Since CFIUS approved this acquisition, it must have concluded (recalling, again, that how CFIUS makes its determinations must be inferred since the basis for evaluation is not released to the parties or to the public) that the marginal increase in threat of penetration from transferring ownership of a given set of facilities in China from IBM to Lenovo was insignificant.

<u>Illustrations of a Special Version of Threat III (surveillance via proximity to US military bases or defense installations) in CFIUS Assessments</u>:

The Rawls Case

[5]Theodore H. Moran. 2013. *Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers*. PIIE Policy Brief 13-11 (May). Washington: Peterson Institute for International Economics.

A special version of Threat III (surveillance) lies at the core of the Rawls case. In March 2012, the Ralls Corporation, a Chinese-owned firm, acquired several wind farm projects whose towers overlooked restricted Naval Weapons Systems Training Facility airspace, where the newest generations of drones (unmanned aerial vehicles) are tested, without reporting the transaction to CFIUS. In June, CFIUS contacted Ralls and requested that the firm file a voluntary notification to have its investment retroactively reviewed. After giving the acquisition a preliminary examination, CFIUS asked that Ralls stop operations until a complete investigation could be completed. Based on that investigation, including confidential US Navy inputs, CFIUS recommended that President Obama block the investment by ordering a divestment of the transaction as well as removal of equipment already installed. This was only the second such formal USG prevention of a foreign acquisition.

The Syngenta Case

The Chinese SOE Chem-China proposal to acquire the Swiss agribusiness firm Syngenta in 2016 for a $44 billion raised a similar Threat III (surveillance) concern about proximity to a US military base. Syngenta operates a plant seven miles from Offutt Air Force Base in Nebraska. Offutt AFB operates as the headquarters of the US Strategic Command (USSTRATCOM) with highly protected and encrypted command and control systems; it does not conduct any tests that might be exposed to foreign surveillance via the Syngenta plant site. CFIUS did not even ask that Syngenta divest or close the plant. Meanwhile Senator Charles Grassley of Iowa warned that Chem-China's acquisition of Syngenta might constitute a threat to "food security" via manipulation of supply to US farmers (a Threat II concern). But Syngenta's share of the US market for insecticides and pesticides amounted to not more than 21-23%, and 10-12% of the US market for seeds, and switching costs from one insecticide, pesticide, or seed source to another is not high. CFIUS approved the acquisition without any mitigation whatsoever.

The use of this Three Threat framework shows that the separation of foreign acquisitions that might pose genuine national security threats from those that do not can be done rigorously. The specification of conditions under which threats are plausible, or not, provides comfort, moreover, that *very few* inward acquisitions will pose any credible national security threat to the United States. The overwhelming bulk of foreign acquisitions can be welcomed without hesitation, and their presence will be beneficial to US workers, firms, communities, and consumers.

IV. Contemporary Challenges to CFIUS's Precise Focus on National Security Threats

CFIUS interprets its mandate to investigate foreign acquisitions of US firms with a specific focus on whether such acquisitions might pose a credible national security threat to the United States, or not, case-by-case. This narrow approach is currently under attack across many fronts.

1. *CFIUS Should Preclude Foreign Acquisitions from Certain Countries Across Entire Sectors, Rather than Evaluate National Security Threats Within Sectors*

CFIUS currently focuses on identifying national security threats within sectors, and does not preclude acquisitions from investors headquartered in certain countries (like Russia and China) across entire industry sectors. CFIUS examines sectors that might be considered "critical" – such as energy or semiconductors – and has a mandate to pay careful attention to "critical infrastructure". But CFIUS analysis then closes in to assess what kind of national security threat might become plausible via a specific foreign acquisition of a firm in that sector or via foreign control over a segment of infrastructure. CFIUS does not issue a blanket prohibition against all foreign acquisitions from any specific country in an entire industry sector or infrastructure segment.

Now, a report composed under the direction of former President Obama's Council of Advisers on Science and Technology poses the question of whether the entire US semiconductor industry needs to be better protected, especially if foreign acquisitions enable China to flood the US market so as to threated crucial sectors of the industry.[6] Senators Chuck Grassley and Debbie Stabenow warn that foreign take-overs across US agribusiness should be prevented so as to preserve something called US food security. Members of Congress have repeatedly urged that foreign acquisitions by companies from Russia or China in energy, in infrastructure, in telecommunications, in media (movie studios), and in financial services be rejected.[7]

Besides overarching problems associated with picking winners to be protected as part of a national industrial policy (considered next below), any change in CFIUS's legislative mandate to exclude foreign acquisitions in entire sectors of the US economy opens the door to a political process to which there is no logical end in sight – after semiconductors, agribusiness, infrastructure, energy, media (movie studios) and financial services, which industry sectors might come next? Not only would prevention of foreign acquisitions exclude valuable investor inputs across broad segments of the American economy, but the change in US approach would legitimate reciprocal sector-wide exclusions on the part of other countries, not only Russia and China. For more than four decades the US has worked to widen access for trade and investment across entire industry sectors in foreign markets, under both Republican and Democratic administrations. This change would reverse direction, quite probably undermining much progress that has been made.

2. CFIUS Should Design an Industrial Policy to Ensure US Dominance and Prevent Foreign Commercial Technology-Extraction

---

[6]Executive Office of the President. Council of Advisors on Science and Technology. *REPORT TO THE PRESIDENT: Ensuring Long-Term U.S. Leadership in Semiconductors.* January 2017. Ian Talley. "US Chip Firms Need Protection, Panel Says". *Wall Street Journal*. January 7-8, 2017.

[7]Letter from sixteen Members of Congress to Gene Dodaro, Comptroller General, Government Accountability Office, requesting a GAO Evaluation of CFIUS, September 15, 2016. Letter from forty-six Members of Congress to Assistant Secretary of the Treasury for CFIUS affairs, Marisa Lago, February 16, 2016.

CFIUS already has a legislative mandate to search for broad patterns in the array of individual foreign acquisitions that might in the aggregate threaten US national security threat. But CFIUS does not try to design an industrial policy to ensure US dominance of particular technologies, or to prevent foreign firms from acquiring particular US technologies, or to keep manufacturing facilities within the United States.

Now, as noted above, the US chief science adviser to former President Obama, has called on CFIUS to restrict foreign acquisitions so as to prevent "a loss of leadership in semiconductor innovation and manufacturing".[8] This may parallel concerns of President Trump's approach to foreign acquisitions: the *Wall Street Journal* characterized this as "a rare alignment with the incoming Trump team."[9] If adopted by CFIUS, such an exclusionary approach would fail to recognize the benefits that arise from foreign investment – benefits that include capital, high-paying jobs, R&D expenditures, competitive pressures to upgrade operations, spillovers – in all sectors of the US economy, including the IT sector. The cross-fertilization of R&D across borders within multinational corporations of all nationalities is a particularly strong source of new innovation for the US as well as for other countries.[10]

More broadly, the record of countries that have tried to design an industrial policy to advance certain industries and protect others has proven to be unpromising in the extreme.[11] The costs, distortions, and counterproductive impacts on the national economy are enormous, while the successes are few and far between. The adoption of an industrial policy to ensure US technological domination and protect US manufacturing in certain sectors, furthermore, would enshrine a zero-sum approach toward international economic relations that would invite retaliation and provoke replication on the part of other nations, as noted above.

3. *CFIUS Should Investigate Whether Foreign SOEs Enjoy Unfair Access to Cheap Capital or Other Government Subsidies, and Condition Approvals on Whether Home Countries Subsidize Exports or Dump Products in the US Market*

---

[8]Quote of John Holdren, Chief Science Adviser to President Obama, October, 2016. Ian Talley. "US Gears Up to Restrict Chinese in Chip Industry". *Wall Street Journal*. January 3, 2017.

[9]Ian Talley. "US Gears Up to Restrict Chinese in Chip Industry". *Wall Street Journal*. *op. cit.*

[10]Moran and Oldenski, 2013, *op. cit.* Theodore H. Moran and Lindsay Oldenski. *The Globalization of R&D by US Multinationals: What Are the Effects at Home?* Washington, DC: Peterson Institute for International Economics. Realtime Economic Issues Watch. February 18, 2014.

[11]Marcus Noland and Howard Pack. *Industrial Policy in an Era of Globalization: Lessons From Asia. Washington, DC: Peterson Institute for International Economics.* 2003. Ann Harrison and Andres Rodriguez-Clare. 2010. *Trade, Foreign Investment, and Industrial Policy for Developing Countries*. *Handbook of Development Economics*, Vol. 5: 4039-4214.

CFIUS pays special attention to state-owned-enterprises (SOEs) from a national security threat perspective, but not from a fair-competition perspective. US intelligence agencies (principally the CIA and NSA) prepare an evaluation of capability and intent to subvert US national security for all proposed SOE acquisitions, as well as other acquisitions that might come under foreign government influence. Under FINSA (2009), CFIUS appraisals of foreign acquisitions involving an SOE must go beyond the initial 30-day investigation, to complete a second stage 45-day assessment. But this 75-day examination confines itself to national security threats, and does not pass judgment on whether the acquiring SOE has access to sub-market-rate capital or other subsidized inputs.

Congressional leaders and industry groups regularly urge CFIUS to take into account whether foreign SOEs have unfair access to cheap capital or other home country subsidies when they bid for US companies.[12] An upcoming GAO review (2017) will address the issue of whether CFIUS should base its approvals or rejections of acquisitions of US firms by foreign SOEs on whether the latter receive grants or other favorable treatment from their home governments.

More broadly, the US-China Economic and Security Review Commission's Annual Report to Congress in 2016 included the blanket recommendation that "Congress amend the statute authorizing the Committee on Foreign Investment in the United States to bar Chinese state owned enterprises from acquiring or otherwise gaining effective control of U.S. companies."[13]

The report of the Council of Advisers on Science and Technology of the former Obama administration recommends broadening CFIUS's mandate to condition approval of proposed acquisitions on whether the home county of the acquiring company (e.g. China) floods the US market with products that have received government support, whether SOEs or private firms.[14]

US economic interests would indeed be served by putting pressure on other countries, beginning with China, to ensure that SOEs operate with more transparency, according to market principles, without special subsidies or government support. But the appropriate US agencies to push for such SOE reforms are the US Trade Representative and the Department of Commerce, using mechanisms such as the US-China BIT negotiations – not by having CFIUS approve or disapprove individual transactions one-by-one. At the same time, the US government should make robust use of domestic and multilateral tools to combat subsidies and dumping rather than using CFIUS approvals or disapprovals as a tool for enforcement.

---

[12] Letter from sixteen Members of Congress to Gene Dodaro, Comptroller General, Government Accountability Office, requesting a GAO Evaluation of CFIUS, September 15, 2016. Letter from forty-six Members of Congress to Assistant Secretary of the Treasury for CFIUS affairs, Marisa Lago, February 16, 2016.

[13] US-China Economic and Security Review Commission. 2016. *Annual Report to Congress*.

[14] Executive Office of the President President's Council of Advisors on Science and Technology. *REPORT TO THE PRESIDENT: Ensuring Long-Term U.S. Leadership in Semiconductors.* January 2017. P. 14.

As for the US-China Commission on Economic and Security recommendation that CFIUS simply reject all Chinese SOE's proposals to acquire US firms, the Annual Report of the Commission (2016) did not provide any analysis whatsoever to support this recommendation. Nor did a near-simultaneous report entitled *Chinese Investment in the United States*, prepared for the US-China Commission by the Rhodium Group, whose authors testified that they did not agree with this Commission recommendation (USCC Chinese Investment in the United States, November, 2016).[15] So it is unclear what line of argument might lie behind this blanket rejection of all SOE acquisitions. Current evidence shows substantial benefits to the US from Chinese investment, including investment by Chinese SOEs.[16]

4. CFIUS Should Demand Reciprocal Treatment before Approving Foreign Acquisitions

CFIUS does not base its approval or rejection of a foreign acquisition on reciprocal treatment of US firms in the market of the foreign acquiring firm. To offer a purely hypothetical example, CFIUS has never indicated that it might condition approval of Lenovo's acquisition of IBM's X86 server business on improved Chinese treatment of Google and Facebook in the Chinese domestic market.

President Donald Trump's economics team has recommended that CFIUS take into consideration reciprocity in international corporate takeovers as part of its recommendation for approval or rejection of each proposed foreign acquisition of a US company. Senator Charles Schumer has similarly proposed that CFIUS approval of Chinese acquisitions be conditioned upon China's willingness to grant US investors access to markets in China.

The US has long been a leader in urging that all countries award most-favored-nation treatment to foreign traders and investors that seek access to their markets. This is a principal reason why the next administration should refrain from charging CFIUS with the duty to design an industrial policy that excludes others from the US economy. Instead the United States should continue to push for reciprocity in treatment of US firms when they operate abroad. But as noted above, international and bilateral negotiations to ensure greater reciprocity should be pursued by a united front of US agencies, led by the White House, the US Trade Representative, and the Department of Congress, not by requiring CFIUS to condition individual approvals or rejections of foreign acquisitions on the degree of reciprocity US firms receive in the acquirer's home market.

For all of these reasons, the United States can best ensure domestic access to the benefits that cross-border investments, including investments via acquisition, bring to the US economy while meeting legitimate concerns about US national security by maintaining CFIUS's precise focus on determining when threats are plausible and when not.

---

[15]Presentation of Thilo Hanneman, US-China Economic and Security Review Commission Hearings. January 26, 2017.

[16]Moran and Oldenski. 2013, *op. cit*. The data do not permit a separate analysis of the impact of Chinese investment via SOEs versus non-SOEs.

But the observation that current CFIUS practices serve US national interests best does not preclude that fundamental changes might nonetheless be adopted by the United States, including changes that do not require new Congressional legislation. The point of vulnerability emerges after CFIUS has sent its recommendation to the President, and the White House decides how to respond.

To date, no US President has ever rejected or added requirements to a transaction that CFIUS has approved; nor has any US President introduced or exercised some broader interpretation of national security than the three-threat perspective embodied in CFIUS assessments

But FINSA regulations do offer the President several avenues to introduce more wide-ranging "national security" considerations as factors to be considered in determining White House acceptance or rejection of the CFIUS determination (see Appendix A of this paper: Section 721 of the Defense Production Act of 1950, 50 U.S.C. App. 2170, as amended by the Foreign Investment and National Security Act of 2007. D.).

Action by the President. Factors to be considered include (*inter alia*):

(5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security;

(7) the potential national security-related effects on United States critical technologies;

(11) such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation.

So, some degree of uncertainty persists about future US behavior as other countries -- such as the members of the European Union -- consider how they might want to try to balance the benefits of inward investment with concerns about potential national security threats from foreign acquisitions.

V. Implications for National Security Screening of Foreign Acquisitions in the European Union

Foreign acquisitions of national firms pose potential national security threats wherever they take place. National authorities in member states of the European Union must rightly be concerned about foreign take-overs just as are their counterparts in the United States.[17] As noted above, high profile cases reviewed by CFIUS in the United States have concerned European-headquartered multinational firms such as Philips, Aixtron, Kuka, and Syngenta (Swiss). A careful appraisal of China's strategic plan to turn the Chinese economy into a manufacturing

[17]Guy Chazan. "EU capitals seek stronger right of veto on Chinese takeovers". *Financial Times.* February 14, 2017.

superpower, "Made in China 2025," by the Mercator Institute for China Studies in Berlin (MERICS), argues that EU "policy makers need a refined set of options to effectively respond to different types of acquisition attempts."[18] The MERICS study recommends that "following the example of the Committee on Foreign Investment in the United States (CFIUS), FDI into Europe should be more comprehensively screened for national security implications."

While confined to foreign acquisitions by companies from China, the comprehensive analysis contained in the MERICs study offers an opportunity to consider the central options for EU member states – and ultimately for the European Union as a whole – to respond to potential national security threats. These options can then be evaluated in light of the preceding discussion of CFIUS procedures – and proposed modifications of CFIUS procedures -- as examined above.

The MERICS study starts from the premise that most foreign direct investments in the EU – including investments from China – create significant benefits in the host economies where they take place, and are unproblematic from a national security perspective. The EU's fundamental posture toward inward investment – including inward investment via acquisition – should therefore be welcoming. Nonetheless, MERICS proposes, EU authorities need to consider a menu of ideas for strengthening how national security screening might take place.

First, MERICS points out, international companies headquartered in China often have deep and opaque ties to the Chinese state. EU authorities must therefore push for more transparency about both Chinese SOEs and ostensibly-private Chinese firms; they must back this with careful confidential investigations; and they must share the results across borders within the EU. The experience of CFIUS in the US provides support for all of these proposals.

Second, notes MERICS, potential threats from foreign acquisitions cannot be limited to cases involving the defense industry but must be expanded to cover the broad expanse of host economies. CFIUS's approach to national security screening in the United States clearly endorses this.

Third, comments MERICS, European authorities must peer beyond individual cases to scrutinize broader national and EU-wide patterns in foreign acquisitions by firms of states like China. The re-write of CFIUS by Congress in 2009 (FINSA) mandated a similar search for possible patterns in acquisitions across a particular industry.

Fourth, suggests MERICS, European decision makers should take into account reciprocal assess for inbound investment on the part of EU firms in the home economy where those investors that acquire EU firms are headquartered. As noted earlier, similar concerns about reciprocity are being debated within the United States, but the recommendation enunciated earlier is that federal level agencies (the White House, Department of Commerce, USTR) should lead negotiations on mutual liberalization without making reciprocity the basis for approval or disapproval of specific acquisitions by CFIUS.

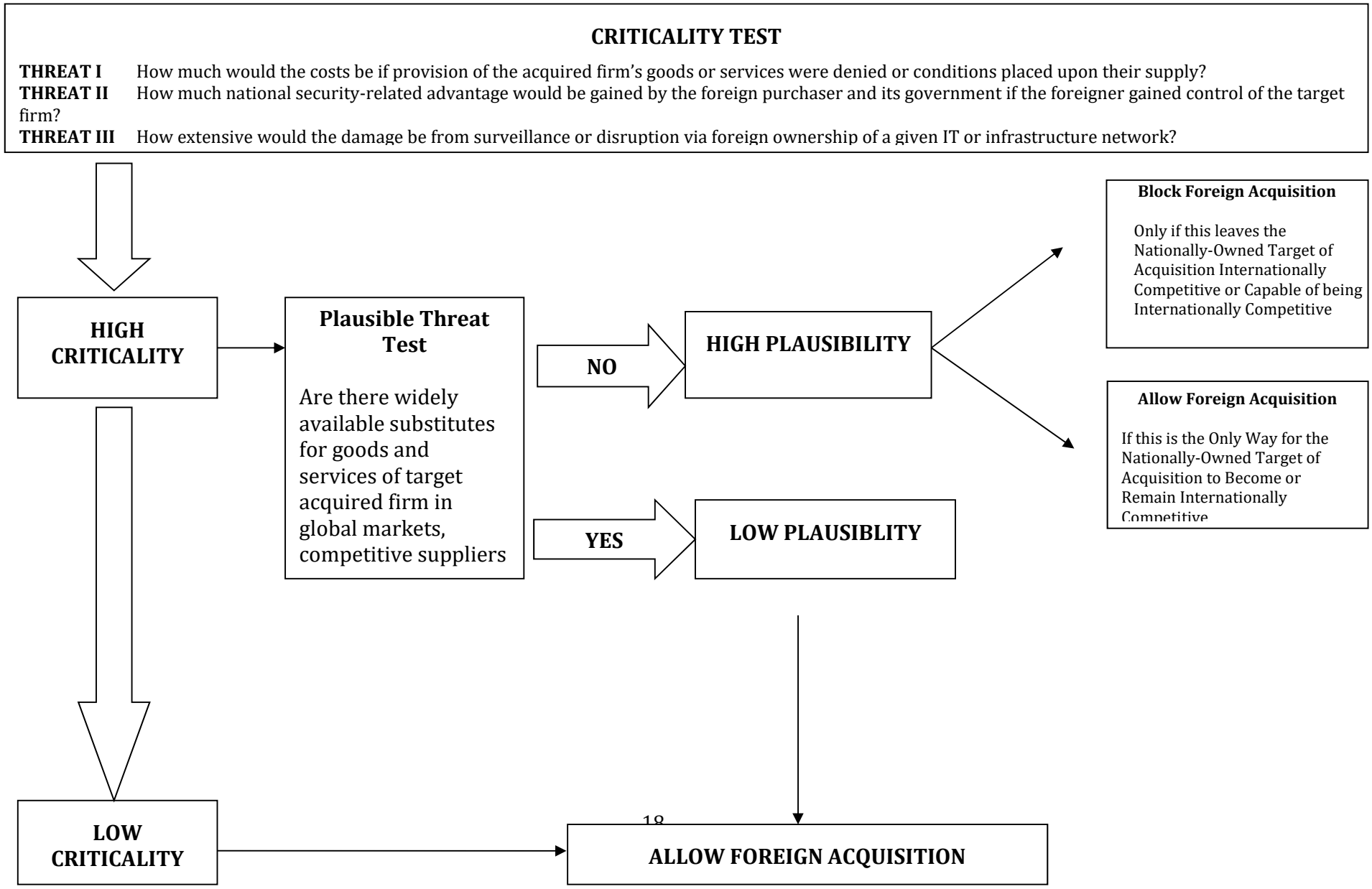
---

[18]Jost Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, Björn Conrad. 2016. *MADE IN CHINA 2025. op. cit*., p. 61.

Fifth – and most problematically – MERICS opens the door to blocking transactions, or attaching conditions to transactions, to prevent technology transfer to firms from specific countries, such as China. The goal, according to MERICS, would be to prevent erosion of technological leadership across entire industrial sectors. One of the three threats that CFIUS investigates most thoroughly is potential transfer of sensitive technology that might be deployed by a foreign company or its home country against the United States. But the idea of designing an industrial policy to ensure technological supremacy for American firms, or to prevent technological sharing with firms of other specific nationalities, would open the door to protectionist policies that would reverse decades of promoting openness for FDI flows across boarders. EU authorities -- like their counterparts in the US -- should eschew such an overarching policy shift, and rely instead on case-by-case decisions about leakage of technology that might threaten national security.

Finally, MERICS recommends that EU authorities might want to "follow the example of the Committee on Foreign Investment in the United States (CFIUS)" as they set about to screen foreign acquisitions more comprehensively for national security implications. As argued above, the example that the EU can follow is clear: the "Three Threats" framework can serve the EU just as it has served the US to promote an appropriate balance between openness to foreign investment and concern about national security.

EU Member (or EU-Wide) Decision-Tree
When Is there a Plausible National Security Rationale to Block a Proposed Foreign Acquisition?



How might the CFIUS three-threat perspective be incorporated into national security screening within the European Union?

Lars-Hendrik Röller and Nicolas Véron have provided suggestions about how to do so.[19] They propose that the CFIUS narrow framework could be adopted via common legislation at the EU level, with implementation carried out via review of individual acquisitions at the national level. They recommend that an internal market directive (Article 95 of the EU Treaty) could establish the overall framework, and dictate a process for national security review by member states, as pertains both to potential threats to that individual state and/or to the EU as a whole.

Röller and Véron argue that new EU legislation should incorporate the following: first, rules of due process, including the maximum duration of the investment review; second, a definition of what is considered 'control' and how it should be assessed; and third, a framework for the negotiation of 'mitigation agreements' or modifications to be made to acquisitions in order to render them compatible with the security objective.

Röller and Véron go on to suggest that such legislation create an EU committee, possibly coordinated by the High Representative for Common Foreign and Security Policy, to ensure mutual information-sharing and coordination, especially in cases of cross-border security spillovers, even though ultimate decision-making would remain with the relevant member state.

Appeals of specific rulings, they note, would be possible through the regular court system, including the European Court of Justice. The European Commission could initiate infringement procedures if a member government's practice is found to be in breach of the Treaties.

IV. In Conclusion

This paper has argued that the narrow case-by-case specific threat assessment approach of CFIUS best serves US and EU interests in combining the benefits of an open approach to inward investment with identification of when national security threats from foreign acquisitions might be plausible. For the US or the EU to introduce broader considerations into approvals or disapprovals of individual cases opens the door to retaliations and protectionist counter-measures on the part of countries throughout the world. This would reverse decades of hard-won progress in opening domestic economies around the globe to greater flows of trade, investment, and technology.

Moreover, the preceding analysis in this paper suggests that use of CFIUS's narrow threat-assessment framework need not be limited to the US and the EU. The logic embodied in the CFIUS threat-assessment approach makes it equally applicable to all

[19] Lars-Hendrik Röller and Nicolas Véron. *Safe and Sound: An EU Approach to Sovereign Investment.* Bruegel Policy Brief. Issue 2008/08. November 2008.

OECD countries, to emerging market economies, and – indeed – to China or Russia, as well.

This threat assessment framework could thus become the basis for a worldwide multilateral agreement. American multinationals, European multinationals, UK-Canadian-Australian multinationals, Japanese and South Korean multinationals, and international investors from other nations could continue to operate as usual – in the vast majority of cases -- if governments around the globe adopted mirror-image policies, while enjoying less discrimination and less arbitrary treatment wherever these companies choose to invest.

Appendix A

Section 721 of the Defense Production Act of 1950, 50 U.S.C. App. 2170 (as amended by the Foreign Investment and National Security Act of 2007).

(d) Action by the President

(1) In general, the President may take such action for such time as the President considers appropriate to suspend or prohibit any covered transaction that threatens to impair the national security of the United States.

(2) Announcement by the president. The President shall announce the decision on whether or not to take action pursuant to paragraph (1) not later than 15 days after the date on which an investigation described in subsection (b) is completed.

(3) Enforcement. The President may direct the Attorney General of the United States to seek appropriate relief, including divestment relief, in the district courts of the United States, in order to implement and enforce this subsection.

4) Findings of the president. The President may exercise the authority conferred by paragraph (1), only if the President finds that (A) there is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security; and (B) provisions of law, other than this section and the International Emergency Economic Powers Act, do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President.

5) Factors to be considered. For purposes of determining whether to take action under paragraph (1), the President shall consider, among other factors each of the factors described in subsection (f), as appropriate.

(f) For purposes of this section, the President or the President's designee may, taking into account the requirements of national security, consider

(1) domestic production needed for projected national defense requirements,

(2) the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services,

(3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security,

(4) the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country— (A) identified by the Secretary of State— (i)

under section 6(j) of the Export Administration Act of 1979 [section 2405(j) of this Appendix], as a country that supports terrorism; (ii) under section 6(l) of the Export Administration Act of 1979 [section 2405(l) of this Appendix], as a country of concern regarding missile proliferation; or (iii) under section 6(m) of the Export Administration Act of 1979 [section 2405(m) of this Appendix], as a country of concern regarding the proliferation of chemical and biological weapons; (B) identified by the Secretary of Defense as posing a potential regional military threat to the interests of the United States; or' (C) listed under section 309(c) of the Nuclear Non-Proliferation Act of 1978 [42 U.S.C. 2139a(c)] on the "Nuclear Non-Proliferation-Special Country List" (15 C.F.R. Part 778, Supplement No. 4) or any successor list;

(5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security;

(6) the potential national security-related effects on United States critical infrastructure, including major energy assets;

(7) the potential national security-related effects on United States critical technologies;

(8) whether the covered transaction is a foreign government-controlled transaction, as determined under subsection (b)(1)(B);

(9) as appropriate, and particularly with respect to transactions requiring an investigation under subsection (b)(1)(B), a review of the current assessment of— (A) the adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines, which shall draw on, but not be limited to, the annual report on `Adherence to and Compliance with Arms Control, Nonproliferation and Disarmament Agreements and Commitments' required by section 403 of the Arms Control and Disarmament Act; (B) the relationship of such country with the United States, specifically on its record on cooperating in counter-terrorism efforts, which shall draw on, but not be limited to, the report of the President to Congress under section 7120 of the Intelligence Reform and Terrorism Prevention Act of 2004; and 8 (C) the potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations;

(10) the long-term projection of United States requirements for sources of energy and other critical resources and material; and

(11) such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation.

References

Chazan, Guy. "EU capitals seek stronger right of veto on Chinese takeovers". *Financial Times.* February 14, 2017.

Executive Office of the President. Council of Advisors on Science and Technology. *REPORT TO THE PRESIDENT: Ensuring Long-Term U.S. Leadership in Semiconductors.* January 2017.

Harrison, Ann, and Andres Rodriguez-Clare. 2010. *Trade, Foreign Investment, and Industrial Policy for Developing Countries*. *Handbook of Development Economics*, Vol 5: 4039-4214.

Letter from forty-six Members of Congress to Assistant Secretary of the Treasury for CFIUS affairs, Marisa Lago, February 16, 2016.

Letter from sixteen Members of Congress to Gene Dodaro, Comptroller General, Government Accountability Office, requesting a GAO Evaluation of CFIUS, September 15, 2016.

Moran, Theodore H. 2009. *Three Threats: An Analytical Framework for the CFIUS Process.* Policy Analyses in International Economics 89. Washington: Peterson Institute for International Economics.

Moran, Theodore H. 2013. *Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers*. PIIE Policy Brief 13-11 (May). Washington: Peterson Institute for International Economics.

Moran, Theodore H., and Lindsay Oldenski. 2013. *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China.* Policy Analyses in International Economics 100. Washington: Peterson Institute for International Economics.

Moran, Theodore H. and Lindsay Oldenski. *The Globalization of R&D by US Multinationals: What Are the Effects at Home?* Washington, DC: Peterson Institute for International Economics. Realtime Economic Issues Watch. February 18, 2014.

Noland, Marcus and Howard Pack. *Industrial Policy in an Era of Globalization: Lessons From Asia. Washington, DC: Peterson Institute for International Economics.* 2003.

Talley, Ian. "US Chip Firms Need Protection, Panel Says". *Wall Street Journal*. January 7-8, 2017.

Röller, Lars-Hendrik and Nicolas Véron. *Safe and Sound: An EU Approach to Sovereign Investment.* Bruegel Policy Brief. Issue 2008/08. November 2008.

Rosen, Daniel and Thilo Hanneman. 2016. *Chinese Investment in the United States.* November.

US-China Economic and Security Review Commission. 2016. *Annual Report to Congress*. November.

US-China Economic and Security Review Commission. 2016. *Annual Report to Congress*. Hearings, January 26, 2017.

Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, Björn Conrad. 2016. *MADE IN CHINA 2025. The making of a high-tech superpower and consequences for industrial countries*. Mercator Institute for China Studies. No. 2, December.