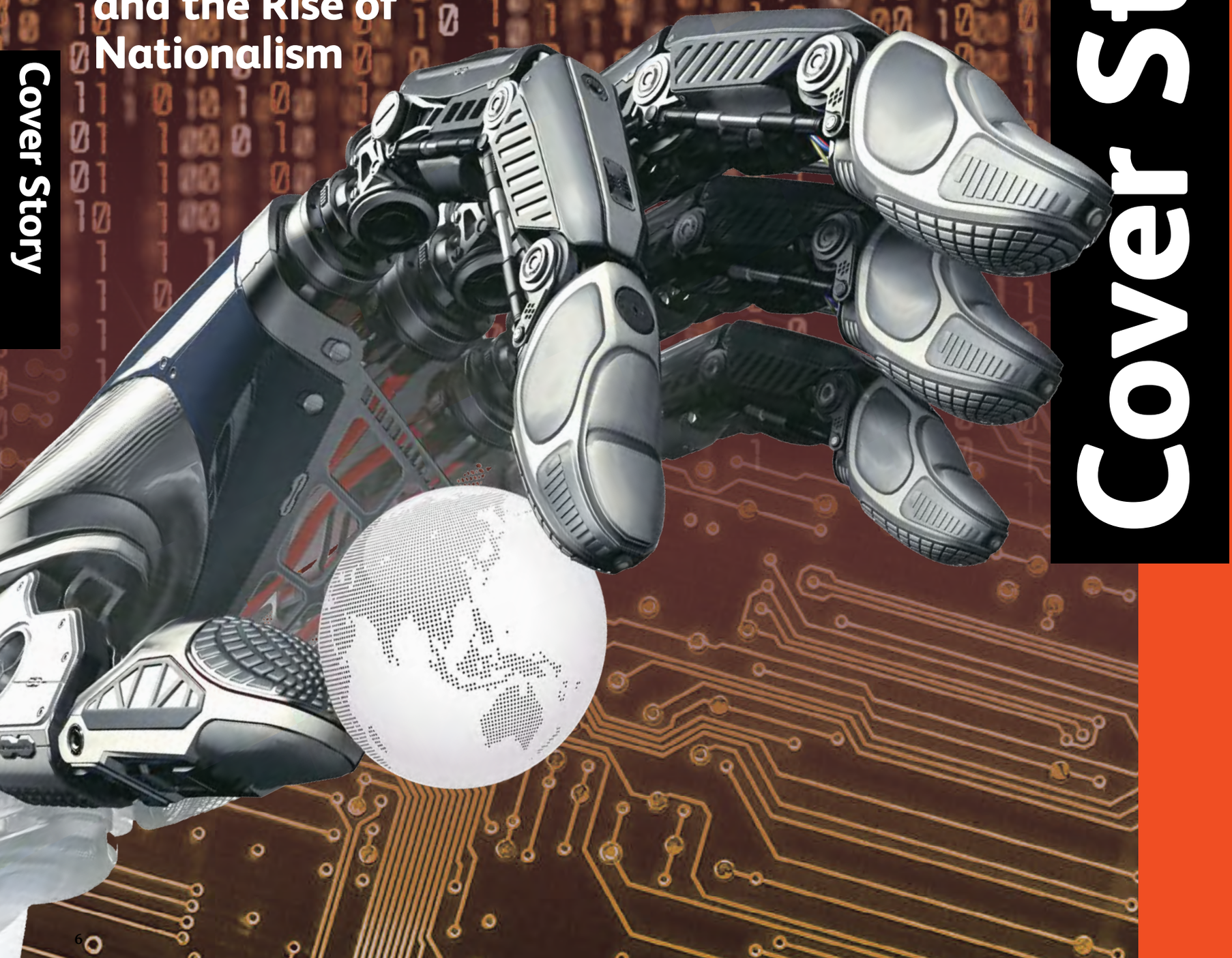
Battle Lines

Technology Rivalry and the Rise of Nationalism



Cover Story

GLOBAL ASIA Vol. 14, No. 1, March 2019

The world is at the advent of a 4th Industrial Revolution. Advances in artificial intelligence, machine learning, Big Data and the so-called Internet of Things, among other things, promise to upend business models around the world and change the way we live in unimaginable ways. But the re-emergence of nationalism as a potent force in geopolitical rivalry threatens the global spread of this new technological transformation. Asia will be an important battleground in this looming 'technology war.'

ESSAYS BY

Regulators Join Tech Rivalry with National-Security Blocks on Cross-Border Investment

By Vinod K. Aggarwal & Andrew W. Reddie

Fueled by a perception that China is becoming a strategic rival rather than a partner in the liberal global order, there are growing concerns about Chinese investments in strategic sectors abroad, not just in the US but also in Europe and elsewhere. Investments in key emerging technologies are attracting particular attention.

Vinod K. Aggarwal and Andrew W. Reddie lay out the wide-ranging regulatory frameworks being put into place to submit foreign direct investment to greater scrutiny on national-security grounds. They are a new battleground in the war for technological supremacy.

MUCH HAS BEEN MADE of negotiations between the United States and China amid their "trade war" over the past two years. Concerns by the US government about the role of Chinese companies — especially Huawei — in the buildout of next-generation 5G telecom networks around the world has provided the most recent episode in what has been described as a Cold War over technology involving Beijing and Washington. In part due to bilateral discussions between Washington and other capitals around the world, Huawei has been blocked from providing a tender for the buildout of Australia's 5G network, with Canada and Germany currently considering legislation to limit Huawei's role. In the US, existing rules ban the government's use of equipment from Huawei and ZTE, and President Donald Trump's administration is considering a total ban on the use of Chinese equipment on US networks. With the focus of analysts on these trade issues, however, the critical changes in how countries are approaching foreign direct investment (FDI) have fallen by the wayside.

From Washington to Berlin and Brussels to Beijing, governments are increasingly turning to new and enhanced regulations in the name of national security to review and block cross-border mergers and acquisitions (M&A) — changing global patterns of FDI. The consequences of these new merger and investment regimes for regulators, governments and companies, however, remain under-explored. Given the new contours of inter-state competition and the role of emerging technologies in this competition, understanding these patterns is essential.

In 2018, the US passed legislation to expand the oversight procedures of the existing Committee on Foreign Investment in the United States (CFIUS) to include even minority stakes in American companies — including those from venture-capital and private-equity firms. China, too, passed a new law to address concerns about forced technology transfer in 2019, but still has significant oversight of foreign investment through its 2015 National Security Act, focusing on cybersecurity and critical technology. Germany has also become sharply concerned about Chinese FDI, in particular, and passed an amendment to its existing rules in December 2018 that lowers the threshold to review FDI deals from 25 percent to 10 percent. Germany's minister of economics has also proposed both German-French co-operation on industrial policy in key industries and supported an EU-wide framework agreement on national security reviews by member states.

This essay analyzes the evolution of M&A rules driven by concerns over national security. We provide a brief history of CFIUS to examine its performance before noting its perceived limitations that led the US Congress to pass the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018. We then examine similar international efforts to address cross-border investment and discuss the potential consequences of these developments. Finally, we focus on the importance of three key issues: the problem of national security becoming an open-ended excuse for protectionism, how to address early-stage investments in emerging technologies, and whether active government participation in a host of industries will achieve its intended goal.

THE EVOLUTION OF CFIUS

To understand the significance of new legislation and its potential effects on FDI, it is worth revisiting the history and evolution of CFIUS in the United States. Here we outline its evolution since its inception by Executive Order in 1975. Specifically, we point to the various amendments and to the processes that have been proposed and implemented to address concerns regarding the role of foreign investments in the economy and the interaction between domestic markets and national security.

Upon its creation, CFIUS was focused primarily on information and data collection — although it remained unclear what its role ought to be. It wasn't until the 1980s that Japanese acquisitions in defense-related sectors including steel, manufacturing, and semiconductors, along with the 1988 Exon-Florio Amendment outlining how CFIUS should review foreign investments, resulted in the presidential authority to block mergers, acquisitions, or takeovers. The standard for making this decision included "credible evidence" that the foreign investment under investigation would impair national security. The amendment also played a role in outlining the voluntary notification of acquisitions to CFIUS and made clear that these declarations would be confidential.

The Byrd Amendment later required CFIUS to investigate mergers, acquisitions or takeovers in which: 1) the acquirer is controlled by or acting on behalf of a foreign government; and 2) the acquisition results in control of a person engaged in interstate commerce in the US that could affect the country's national security.[1] It is worth pointing out that there would be later disagreement concerning the degree to which these reviews were discretionary or mandatory — particularly in the case of Dubai Ports World in 2006, concerning the management contracts for six US ports and its potential sale to DP World — a state-owned firm in the United Arab Emirates (UAE). These contracts were already foreign-owned by the British firm P&O, but when

1 Public Law 102-484, Oct. 23, 1992.

P&O was acquired by DP World, Congress voted to block the deal. DP World would eventually sell P&O's management contracts for the six US ports to AIG, a US firm.

The DP World episode led to changes in the CFIUS process via the Foreign Investment and National Security Act of 2007 (FINSA). FINSA added "critical industries" and "homeland security" as broad categories of economic activity subject to CFIUS review; set out to define the standards for investigation; and gave CFIUS statutory authority. FINSA also sought to better define the circumstances in which an investigation would be appropriate, pointing to a threshold of 10 percent of voting securities as a standard for "controllability" as well as judgments by CFIUS members concerning board seats. The act also made clear that passive investment vehicles — investment funds, banks and insurance companies — carrying out their normal business do not constitute grounds for investigation.

From its inception to the present, five acquisitions have been blocked through the CFIUS process. President George H.W. Bush directed China National Aero-Technology Import and Export Corporation (CATIC) to divest its acquisition of MAMCO Manufacturing in 1990. More recently, President Barack Obama directed the Chinese-owned Ralls Corporation to divest from an Oregon wind farm project and blocked a Chinese company, Fujian Grand Chip Investment Fund, from acquiring Aixtron, a German semiconductor firm with US assets. In 2017, President Trump blocked the US$1.3 billion acquisition of Lattice Semiconductor Corp. of Portland, Oregon, by a Chinese investment firm, Canyon Bridge Capital Partners, as well as the acquisition of semiconductor chip maker Qualcomm by Singapore-based Broadcom for US$117 billion.

Looking at the five acquisitions that US presidents have decided to block, however, doesn't tell the whole story — given the selection effects concerning those investigations that run their course. Indeed, several mergers and acquisitions have been abandoned or reconstituted — including the DP World case noted above — to avoid being blocked through the CFIUS process.

NEW DEVELOPMENTS IN US FOREIGN-INVESTMENT RULES

As noted, the CFIUS process has been predominantly focused on controlling stakes taken by foreign companies in US companies or multinational companies with contracts related to US critical infrastructure. These "traditional" pathways of regulation, however, turn a blind eye to how a number of countries engage with American companies, particularly those in the technology sector working on emerging technologies — including artificial intelligence, quantum computers and next-generation space systems. The role of Chinese investment funds as well as Chinese funding for traditional venture-capital firms in the US has been well documented — though largely absent from the public discourse, which instead has focused on procurement guidelines — specifically related to Huawei and ZTE — and US-China trade concerns.

The 2018 FIRRMA legislation puts these issues back on the agenda. It expands the types of foreign activity in the US market that are subject to oversight. Specifically, FIRRMA lowers the threshold for investigating foreign investment to include any foreign "non-passive" investment in companies involved in critical technology. The technologies discussed during the floor debate concerning the passage of FIRRMA in the House of Representatives included artificial intelligence, robotics, augmented and virtual reality, new biotechnologies, new financial technologies, and advanced materials. According to Croley et al., FIRRMA changes the jurisdictional framework by extending CFIUS review to "any investment that relates to a US business owning or maintaining "critical infrastructure;" a business involved in the development, design or production of "critical technology;" or a business collecting or maintaining "sensitive personal data" of US citizens, in the event that the investor acquires (in connection with the investment) "any material nonpublic technical information;" is granted membership or observer rights on any board of the business; or has "any involvement" in the decision-making of the business." [2] Importantly, this means that transactions that do not lead to foreign control of a company are still subject to disclosure, review and investigation.

For some, this is a welcome amendment to the CFIUS review process. The US Department of Defense's Defense Innovation Unit (DIU), formerly DIUx, has a series of reports outlining how Chinese investments have contributed to technology transfer across the Pacific — arguing that the existing CFIUS review process has only been partially effective.[3]

There are clearly significant challenges associ-

2 Steven Croley et al., "How FIRRMA Changes the Game for Tech Companies and Investors," Law360, Oct. 10, 2018, www.lw.com/thoughtLeadership/how-firrma-changes-the-game-for-tech-cos-and-investors

3 Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of US Innovation," Defense Innovation Unit Experimental (DIUx), 2018 ed., https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf (accessed on Feb. 28, 2019).

ated with the new legislation. First, the US Treasury Department and other enforcing agencies face a series of decisions concerning which technologies will be subject to heightened scrutiny and control and whether some countries — particularly US allies — are to be exempted from the requirements. Second, companies will have to amend their own procedures and auditing processes regarding foreign investment and resulting voluntary declarations to CFIUS review. Both concerns are suggestive of the difficult balance that policy-makers and companies must strike related to national security considerations while maintaining an open investment environment in the US. But the changes we have seen in new legislation, driven in large part by Chinese foreign investment, are hardly restricted to the US.

In the section below, we turn to international regulations related to FDI to contextualize US legislation and to point to the broader transformation of the regulatory regime driven by emerging technologies and a changing geopolitical landscape.

INTERNATIONAL REGULATIONS ON FDI

Countries have long sought to regulate FDI through unilateral, bilateral, mini-lateral and global arrangements. While not always explicitly focused on national security, such concerns often underlay efforts to restrict the amount and types of investment. In 1971, the Andean Foreign Investment Code sought to influence the terms on which its members contracted for various types of technology, seeking to avoid overpayments to multinational corporations (MNCs). Restrictions on specific sectors also formed a key part of the Code, with explicit exclusions for investment in critical infrastructure such as public services, finance and almost all media.

More recently, the focus of FDI regulations in the name of national security, as with the US case outlined above, has been driven by Chinese investments. In particular, concerns about core industrial sectors, emerging technologies and dual-use technologies have all been drivers of new regulations. In 2009, Canada created a national security review process for FDI based on its Investment Canada Act, focusing on a host of sectors, with an emphasis on defense-related industries and data security. Any transaction could be reviewed under this act, but of 4,500 cases since its creation, only 13 transactions faced review, with provisions for divestment or mitigating actions.[4]

In Europe, the UK has moved forward to strengthen national security reviews of investment, rather than only relying on the existing Competition and Markets Authority (CMA), which is based on a 2002 law that allowed the government to examine mergers based on national security considerations. The new approach, proposed in a July 2018 White Paper, specifies triggering events based on varying levels of shares and assets.[5] While parties to a transaction are encouraged to voluntarily submit their proposed acquisition to the government, the government also can initiate a review of transactions on its own. In terms of likely impact, the White Paper predicts that approximately 200 cases will be subject to review on a yearly basis, with about 50 requiring some mitigating action on the part of the parties in light of national security concerns. In response to this proposed approach, which is likely to be instituted by 2020, venture-capital (VC) firms, law firms, pension funds and others have expressed concern about the possible uptick in cases that will fall under national security review. Under the 2002 law, only nine cases were subject to government intervention.[6]

In continental Europe, France has regulated and blocked FDI since 1966. Its 2004 law expanded the sectors that would be subject to review from weapons to include infrastructure investments such as electricity, gas, oil and water. Pending approval of the French Senate, the PACTE Law first proposed in June 2018 will expand its sectoral overview to AI, data, space, cybersecurity, dual-use goods, robotics and the like. The bill gives the government the right to suspend voting rights and dividend distributions, appoint a trustee in the company to oversee French interests, and sell French assets. Moreover, both acquiring and target companies can seek a review by the Ministry of Economy for their opinion of the investment.

Germany has for the most part been very welcoming with respect to FDI, with few restrictions for national security. Very recently, this has begun to change dramatically. Since 2004, the German Ministry for Economic Affairs and Energy (BMWi) has had the power to review M&A activity in security related industries including military equipment and IT products used for encryption. This review was extended in 2009 to include any M&A activity by non-European investors if a foreign entity acquired more than 25 percent of voting rights. In 2017, in the aftermath of concerns about a 2016 acquisition effort by a Chinese company of a German industrial robotics company and a proposed chip company acquisition, the scope of review was expanded to include critical infrastructure, cloud computing, telematics and some key software. The 25 percent threshold was lowered to 10 percent for sector-specific acquisitions that might impinge on national security, and the scope was expanded to include the media in December 2018.

In addition to these changes in German law, in early February 2019, breaking from longstanding German opposition to industrial policies at the federal level, the Minister of Economics, Peter Altmaier, proposed in a paper the "National Industry Policy 2030." In it, he calls for both a preference for European-wide mergers over outsiders, including looser rules on mergers, and industrial policies including a national investment facility to prevent M&A efforts by non-European companies. In particular, he points to the critical importance of national and European capabilities in AI, autonomous driving, automated production, digitalization and the platform economy. This effort was followed just two weeks later by a joint French-German manifesto on a 21st century industrial policy.[7] The manifesto calls for technology funding from the government in collaboration with the private sector, support for high-risk projects in new technologies, co-operation in R&D in AI, consortia, and better financing in general. Specifically with respect to M&A, without naming countries, it calls for consideration of "state-control of and subsidies for undertakings with the framework of merger control" and reciprocity in public procurement. There is little doubt that the goal of this effort is primarily to address Chinese industrial policy and investments. The manifesto also calls for implementation of an EU-wide screening procedure, to which we now turn.

The EU has long co-ordinated trade policy, but has done little with respect to creating common national security review policies on FDI. Currently, only 14 of the EU's member states have a national-security screening procedure on FDI. But beginning with a European Commission proposal in September 2017 for the development of a framework to screen FDI entering the bloc, the EU's governing institutions moved quickly, with approval by both the European Parliament and member-state governments by July 2018, leading to a proposed agreement on Nov. 20, 2018. Following approval by legislators this year, the framework is likely to come into effect in November 2020. The accord does not call for a single common policy but for information exchange on best practices and allows the commission,

4 "Foreign Investment Control Heats Up: A Global Survey of Existing Regimes and Potential Significant Changes on the Horizon," White Paper, Jones Day, January 2018.

5 *National Security and Investment*, presented to Parliament by the business, energy and industrial strategy minister, July 2018.

6 Ben Martin, "UK plans to tighten takeover rules face resistance from business," Reuters, Nov. 21, 2018, www.reuters.com/article/us-britain-m-a-rules/uk-plans-to-tighten-takeover-rules-face-resistance-from-business-idUSKCN1NQ1Y6

7 German Federal Ministry of Economics and Technology and French Ministry of Economics and Finance, "A Franco-German Manifesto for a European industrial policy fit for the 21st Century," Feb. 19, 2019, www.gouvernement.fr/en/a-franco-german-manifesto-for-a-european-industrial-policy-fit-for-the-21st-century

8 European Commission, "Commission welcomes agreement on foreign investment screening framework," Press Release, Nov. 20, 2019, http://europa.eu/rapid/press-release_IP-18-6467_en.htm

9 See Xingxing Li, "National Security Review in Foreign Investment," *Berkeley Business Law Journal 13*, no. 1, 2015.

10 Vinod K. Aggarwal and Andrew Reddie, "Comparative Industrial Policy and Cybersecurity: The US Case," *Journal of Cyber Policy 3*, no. 3, 2018.

the EU's executive and regulatory arm, to "issue opinions in cases concerning several member states."[8] With respect to scope, the deal covers critical infrastructure and technologies, robotics, AI, cybersecurity, dual-use products, media, and broader infrastructure — similar to the coverage of the new German FDI laws.

In China, the Sino-Foreign Equity Joint Venture Law of 1978 permitted foreign investment, but with a host of strict regulations, management and oversight. In the 1990s, China created the Catalogue to monitor investments by distinguishing between investments that were encouraged, restricted and prohibited, thus providing sectoral restraints on investment. Examples of prohibited investments in the 1990s included the power industry, telecommunications, broadcasting, and military arms, among others, and created conditions on the type of technology that companies could bring in, setting the stage for later national security-oriented legislation. The Catalogue was replaced by a "negative" list, and in 2011, the government created a specific National Security Review process that focuses on M&A activities. Any domestic companies in defense-related industries, such as agriculture, energy, resources, transportation and technology could all be subject to review. The passage of the 2015 PRC National Security Law set the stage for a much more significant national security process on M&A, modeled in part on CFIUS. The first step was the June 2017 Cybersecurity Law, which affected network operators in the critical sectors that were already subject to review, but which put restrictions on data storage and transfer. Under pressure from the Trump administration, the government is on the verge of passing a new foreign investment law that aims to address American concerns on the transfer of proprietary technology and government procurement. But at the same time, the new law contains a national security clause that is very broad, allowing the government to block any investment without a clearly defined procedure.

In many cases, countries have looked to the US CFIUS process in designing their national security oversight of FDI. For example, China, which has been the subject of recent efforts to block investments in the US (and elsewhere), has modeled some of its efforts on the US approach.[9] This raises issues about the emulation of practices that may eventually create growing conflict as countries aggressively block investments.

WHAT'S NEXT?

We have seen a dramatic trend toward new regulations in the name of national security, driven in large part by growing Chinese investments that affect the inflow of FDI into countries. In our view, we must pay attention to three critical issues.

First, while we agree with the concerns underlying this trend, particularly in areas such as cybersecurity and emerging technologies that are dual-use (with civilian and military purposes), the question remains whether and how these new regulations will change the level of scrutiny concerning international investment.[10] The temptation for protectionist interest groups to frame claims for protection in terms of national security in investment, just as they have in trade, may well prove irresistible. With the passage of FIRRMA legislation in the US, and comparable legislation elsewhere, there is a real danger that national security reviews will be abused. Most of this legislation, while specifying particular industries that are "critical," leaves a large amount of discretion in the various committees and enforcing bodies that are being set up. So far, at least in Western countries, the number of cases of national security reviews being used to block FDI has been remarkably small. But with new legislation on the books, and continued fear of China's outward FDI push, it appears inevitable that the number of cases will grow rapidly. A key question is whether the differing national approaches to national reviews of investment will lead to pressure to create an international regime to regulate what states are doing.

Second, the new emphasis on the regulation of investments by venture capital and private equity firms in the case of FIRRMA raises an important issue regarding how it will carry out its regulatory function. As we have argued, the prior focus of both the US and other countries' regulations on mergers and acquisitions may have been misplaced. If the goal of other states is to transfer key technologies across borders, there are alternative and more efficient vehicles for doing so, including early-stage investment. Over the last 30 years, innovation has been driven by startups backed by seed-stage and follow-up investments by venture capital funds. The new FIRRMA legislation in the US seeks to address this, but it remains an open question whether the opaque origins of investors in many venture capital and private equity firms will prevent technology transfer by foreign countries of critical innovative technologies being developed by Silicon Valley startups. A number of US-based companies, for example, have taken funding from sovereign wealth funds and monies from abroad and in turn channeled that investment into Silicon Valley. In principle, the FIRRMA legislation should lead to these types of transactions being reviewed. In practice, however, investors may argue that they do not have a controlling stake or a board seat and should avoid review. It remains unclear whether the CFIUS process that has hitherto relied on voluntary declarations has the regulatory power to address edge cases in which investors attempt to obfuscate their identity.

Third, it is also worth considering the question of whether efforts undertaken to reduce technology transfer and to mitigate their strategic benefits will have unintended consequences. When government funding vehicles have sought to provide early-stage investment in Silicon Valley companies, they are often last to the party. It is worth considering, then, how the research and development pipelines of companies are likely to be affected by rules designed to increase transparency and scrutinize foreign investment. On its face, increased transparency represents a good idea but it is also likely to increase the reporting requirements placed on (relatively small) companies and impact the speed at which startups grow.

FIRRMA and efforts like it that have been undertaken abroad, while increasingly common, are not a panacea. Understanding their effects and limits represents an important subject of study for companies big and small as well as academics and lawyers.

Vinod K. Aggarwal is Travers Family Senior Faculty Fellow and Professor of Political Science and Director of the Berkeley APEC Study Center (BASC) at the University of California, Berkeley.

Andrew W. Reddie is a BASC Project Director and PhD candidate in the Department of Political Science at the University of California, Berkeley.

For research support, the authors would like to thank Claire Tianyu Qiao and Courtney Kantowski. Aggarwal's work is partially supported by a National Research Foundation of Korea Grant funded by the Korean government (NRF-2017S1A3A2067636).