SEPTEMBER 2019

Emerging Technologies and Managing the Risk of Tech Transfer to China

AUTHOR
James Andrew Lewis

A Report of the CSIS TECHNOLOGY POLICY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2019

Emerging Technologies and Managing the Risk of Tech Transfer to China

AUTHOR
James Andrew Lewis

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible through general support to CSIS. No direct sponsorship has contributed to its publication. The author would like to thank Arthur Nelson, William Crumpler, Evan Burke, Matthew Serrone, and Khristal Thomas, and several commentators who wish to remain anonymous for their contributions to this report.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Contents

Executive Summary

A key American assumption behind globalization was that a growing China would become a friendly market economy. This was overly optimistic. While the nature of the bilateral relationship was undecided for some time after China's opening to the West, the necessity of preserving unchallenged Communist Party of China (CCP) rule has impelled China under President Xi Jinping toward a more nationalistic and confrontational path.

There are deep interconnections between the U.S. and Chinese economies, and China has built its technology base on what it has acquired from the West. China's government and some Chinese companies will use any means, legal or illegal, to acquire technology. The interdependent relationship that China has used to modernize itself (and which brought immense returns to Western companies) cannot continue unchanged, but given the deep interconnections, change must be carefully managed.

New legislation calls for agencies to tighten controls on "emerging and foundational technologies." These are broadly defined as technologies essential to U.S. national security—technologies that are at an early stage of commercial or military development. Current restrictions on technology transfers do not adequately capture emerging and foundational technologies. Many emerging technologies have not yet been evaluated for national security implications nor have they been adopted for control by multilateral regimes.

The fundamental issues are whether to allow China to invest in emerging technologies, whether to allow Chinese individuals to work and study in the United States, and whether to limit trade in advanced technology between the United States and China. There are no black-or-white answers for these questions. This essay argues that new restrictions are needed, but counterintuitively, these should be shaped by recognizing that being open makes the United States stronger than being closed. "Open" means that market forces guide most investments and that the United States limits its use of trade barriers and restrictions on the movement of capital and labor, limited only by the need for restrictions to protect national security.

In designing new restrictions, the most important consideration is maintaining U.S. technological strength. This is more important than restricting Chinese access to technology. These objectives are not mutually exclusive. While broad restrictions on emerging technologies will damage the national interest, tailored approaches can minimize risk to security and innovation. The best lens through which to consider policy

is to ask if policies strengthen the American capacity for innovation, since innovation is the cornerstone of future power.

A Cold War-style bifurcation between the United States and China is not in the U.S. interest and may not even be possible. The United States can mitigate and manage the risk of trade with China using regulation, negotiation, and measures to protect intellectual property. The best approach is an incremental and flexible approach to technology transfer centered on the need to avoid harm to the U.S. economy. New restrictions on emerging technologies must map to innovation processes if they are to do more good than harm.

Significant changes are needed to modernize technology transfer restrictions for emerging technologies, as the Foreign Investment Risk and Review Modernization Act (FIRMMA) modernized restrictions on foreign investment, but these will be politically difficult. Cold War-style technology transfer regulations are problematic. However, the United States can draw on existing regulatory tools to manage risk, including foreign investment restrictions under the CFIUS process, export controls on commercial technologies, and expanded counterintelligence action to reduce illicit access to emerging technology. Specific recommendations include:

- Create new end-user controls focused on the Chinese government and military recipients for emerging technology.
- Work with allies to limit Chinese investments that provide access to or control of emerging technologies.
- Modernize export controls to move away from Cold War-style control performance thresholds.
- Increase FBI funding for counterintelligence activities.
- Keep NSDD-189 protections for fundamental research.
- Do not ban Chinese workers and students. Additional scrutiny is necessary for graduate students in research areas with potential military applications or against "minders"—individuals sent to keep an eye on other Chinese students. While there is some technology leakage, the benefits to the United States far outweigh the costs.
- Avoid an embargo. That is not in our interest and would attract little support from allies.

Using these tools, the United States can mitigate risk while maintaining the openness that is a hallmark of the American economy. In doing this, however, the United States must balance two goals. The first is to decrease the flow of technology to China when it harms American interests. The second is to ensure this is done in ways that minimize or avoid damage to the U.S. economy and its ability to innovate. The third is to build partnerships with other friendly nations to press China to change its behavior and observe international norms and practices. An alliance strategy delivering a joint request on technology transfer to China is crucial for success.

What was tolerable when China was a developing economy is no longer acceptable, particularly now that it is the second-largest economy in the world and a military competitor. Until Chinese policy changes, these tools let the United States manage technology transfer risk. However, these measures are defensive. The most important

response to China is to strengthen America's own innovative capabilities. In the Cold War, under Eisenhower, America created research and education programs that let it to outperform the Soviets. The impetus for this was a single incident, the launch of Sputnik, which was heralded as evidence that the state-centric model for science and industry was inherently superior to market democracies. Sputnik sailing overhead energized American innovation. This time, however, there may be no Sputnik, nor can the United States afford to wait for one.

The Risk of Technology Transfer

The United States faces a messy reconstruction of the global order it created in the 1990s. A key assumption for this American globalism was that a growing China would become a friendly market economy. This has proven to be wrong. China under Xi Jinping has taken a very different direction. The behavior of the Chinese state raises serious concerns about China's intentions and makes the status quo untenable until this behavior changes.

The United States has never faced a rival like China before, and there are deep interconnections between the two economies. China built its technology base in part through acquisitions, licit and illicit, from the West. While China has made immense progress, it still depends on Western technologies. The interdependent relationship that China has used to modernize itself, and which brought immense returns to Western companies, has to change to protect the interests of the United States, but given the deep interconnections, the form and degree of this change must be carefully designed.

The powerful narrative of Chinese economic growth driven by IP theft shapes discussion in Washington and has led Congress to legislate new restrictions in the Foreign Investment Risk Review Modernization Act (FIRRMA) and the accompanying Export Control Reform Act (ECRA). As the United States moves to implement FIRRMA and ECRA, the fundamental issues are whether to allow China to invest in the United States, whether to allow Chinese citizens to work and study in the United States, and whether to limit trade in advanced technology between the United States and China.

The guiding principle for policy is to act only if the result is to strengthen America's capacity for innovation. Innovation is the cornerstone of future power. In some cases, this means that the best policies for dealing with technology transfer to China will be counterintuitive unless the United States recognizes that the primary goal is not to keep China from acquiring technology but to ensure that the United States retains its ability to innovate.

Innovation has become one of those Washington catchphrases, but hard economic and military truths underpin it. The nation that is best at innovation—creating new technologies—will grow faster and be better equipped to defend itself. To gain this advantage, policies that accelerate research and ease connection to the global innovation system best serve the United States. This includes the integrated "innovation ecosystem" between the United States and China, from which both have benefitted. The challenge for policy is to now impose a degree of separation.

This is not a Cold War; the world is not divided into two hostile camps with little economic interaction between them. Whether it becomes necessary to pursue greater bifurcation depends on the course of the bilateral relationship, but for now it is not in America's interest. For the near term, interconnections must remain. One implication of this, however, is that Cold War-style technology transfer regulations will also be ineffective.

While the nature of the bilateral relationship was not set for some time after China's opening to the West, the necessities of preserving unchallenged CCP rule have impelled China under Xi Jinping toward a more nationalistic and confrontational path. But China currently remains dependent on the West for advanced technology. This will not last forever, and in any case, China's government and some Chinese companies will use any means to acquire advanced technology.

The United States can mitigate and manage the risk of trade with China using regulation, negotiation, and measures to protect intellectual property, including an increased emphasis on counterespionage. This will require an incremental and flexible approach to technology transfer. Blanket denials do not serve U.S. interests. New restrictions must map to the processes of innovation. The United States must accept that access to some advanced technologies is inherently unpreventable and, at times, in the national interest. Significant administrative changes are needed to modernize technology transfer restrictions for this new conflict (as FIRMMA modernized restrictions on foreign investment), but these will be politically difficult.

Three policy actions emerge from these conclusions: continued screening of Chinese investment; adoption of "end user"-based controls for most emerging technologies (similar to what is used in the CFIUS process); and an increased effort at countering Chinese espionage in the United States. These three tools will let the United States reduce illicit access by China to advanced technology.

In using these tools, however, the United States must balance two goals: (1) decrease the flow of technology to China when it harms American interests; and (2) ensure this is done in ways that minimize or avoid damage to the U.S. economy and its ability to innovate. The second goal should take precedence, as there is risk that if the tools of technology transfer restraints are misapplied, they will do as much harm to the United States as to China.

How We Got Here

Deng Xiaoping opened China's economy to the West 40 years ago. When Deng took power, he was shocked by the disarray Maoism had created and how far China lagged behind other economies. Deng created policies and programs for trade, education, research, and investment, as well as espionage, to remedy this. The acquisition of Western technology by means both licit and illicit has been part of China's economic and security policies since that time.

This met with little objection from the West. American, European, and Japanese companies saw immense economic opportunity. While the United States tried to win multilateral support for technology transfer restrictions on China during the creation of the Wassenaar Arrangement, it found no support among its allies. As a senior European trade official put it during these talks, "China is our market." Until recently, many Western companies opposed

the extension of restrictions on technology transfers and believed that market forces and China's progress toward becoming a market economy would remedy this.

These hopes proved to be wrong. China's behavior ultimately did not change; if anything it became more aggressive under Xi Jinping. U.S. tolerance for Chinese trade practices and illicit technology acquisitions has ended, and this change included a change in attitudes among American companies. Once they defended China, but that is no longer the case.

China's domestic political dilemma is the primary cause of the technology transfer problem. The issue, as many people realize, is that the CCP fears that it needs economic growth to preserve domestic stability, and that economic growth requires continuing unfair trade practices and economic espionage.

Transnational Innovation

The intertwining of the United States and Chinese technological bases is part of a larger change in research and innovation. These are no longer national activities as they were before 1990. In the 1950s, technological innovation came from large central labs. This has changed, and the current innovation "pipeline" in the United States can be described as a blend of university research, venture capital investment, corporate research, and entrepreneurial start-ups that draw upon talent and capital from around the world. Research combined with business experience is what creates new products, services, and companies.

Technology and innovation do not follow the political map nor is it in the U.S. interest to pursue a reliance on national supply chains or "indigenous innovation." There is already considerable research that shows that the best outcomes are provided by transnational innovation and research ecosystems. Technology is no longer created in discrete national systems, and imposing regulations designed for such national systems would do more harm than good.

Advanced technologies are now created in a transnational research and innovation ecosystem. The end of the Cold War removed political obstacles to trade and communication, and the use of new technologies like the internet created a deeply connected global economy. The effects of globalization on innovation include an increase in the international mobility of labor, especially highly skilled labor, and the spread of technological capabilities and information among many countries. Trade and the explosion in high-speed networks and connectivity have accelerated the global diffusion of scientific, technical, and industrial information and multiplied the pathways to develop emerging technologies.[1] Researchers and companies increasingly rely on a globally mobile workforce and on the exchange of ideas and investments across borders.

The emerging technologies that will shape national power in the future come from sources located in Europe, Japan, and North America. These innovations are not "specially designed" for military applications and must be modified to provide military utility. This means they are not munitions or "dual-use" goods in the conventional sense any more

1. National Science Board, *Science & Engineering Indicators 2018* (Alexandria, VA: National Science Foundation, January 2018), https://nsf.gov/statistics/2018/nsb20181/.

than cloth or steel, which can be used for military purposes but do not fall within the scope of controlled goods because most transfers do not pose a national security risk.

Business and science have become even more international and collaborative. International research and development alliances among corporations have increased eight-fold since the mid-1980s. Most large companies have plants or development centers in many countries. They do this for market access, because of favorable legal and regulatory environments, and to gain access to human talent. This is especially true in China. Multinational research and development provides advantages in both cost and innovation over nationally based systems. This international approach provides competitive advantage in a global marketplace, and layering national regulations on top of this transnational ecosystem will be difficult.

In this environment, there will always be technology leakage, but if properly managed, the gains to the United States outweigh any loss. Recognition of the changed nature of research and technology creation is fundamental for reorienting American tech transfer policy. This means identifying where Chinese participation in American technology development through workforce and investment, provides more benefit than cost. The costs of badly designed restrictions on technology transfers include reduced revenue and market share for U.S. companies, reduced access to highly-skilled foreign individuals, and, in combination, a reduction of innovative capacity. U.S. technological leadership has flourished by embracing openness.

To use artificial intelligence (AI) as an example, the AI innovation ecosystem stretches from the United Kingdom, Canada, and Israel to China, with Silicon Valley at the center. Constraining this global ecosystem will damage American innovation. AI, like many emerging technologies, depends upon collaborative research and an international workforce. The United States needs to weigh any restrictions in light of this. China already has advanced AI capabilities, although somewhat overhyped. AI research depends on open processes; closing this off will slow innovation by American companies and universities.

The source of the U.S. advantage in innovation comes from a blend of science and engineering expertise, openness, and entrepreneurial skills and capital. One sign of its success is that many countries want to copy it. China has tried to substitute government funding for private venture capital, but the United States may have a growing advantage, as China increasingly turns to a reliance on national champions and indigenous innovation, moving away from the open, transnational model that is more successful. The United States can erode its advantage, however, if it constrains transnational flows of people, ideas, and money. Overreaction to China poses considerable risk for American innovation.

Is Globalization Reversible?

The fact that there has been a steady stream of growing interconnections among economies over a period of centuries, despite dramatic interruption from warfare, suggests that globalization is not reversible and probably not in our interest to reverse, since openness is a key U.S. strength. The policy and regulatory tools in this report can help manage the risks and expand the benefits of globalization.

Globalization is the product of broad political, economic, and technological forces that themselves are not easily changed. The end of the rigid demarcation between hostile camps that existed from 1945 to 1990 erased barriers to economic integration, and technological change has reinforced economic integration by providing unprecedented mobility of goods, people, ideas, and now data. While these political demarcations may be returning to some degree, the transnational networks created in the last three decades impose serious penalties for separation: the least globalized economies are usually also the poorest. Globalization can bring problematic social and political consequences, but its benefits for growth and knowledge are unquestionable.

U.S. opponents would like to reverse globalization. They fear the political risk it creates for authoritarian regimes. Their preference is for a system that favors their sovereign political and economic interests while preserving their access to Western markets and technology. While the laissez-faire approach to globalization is unsustainable for the West, and explains much of the populist surge, the United States does not and should not overuse restriction or retreat to Fortress America in our efforts to defend against China.

The Limits of Decoupling

One central problem for American technology policy is how far to "decouple" the U.S. and Chinese economies. It is worth noting that the best outcome for the United States and China would be to avoid decoupling; the two economies are stronger as partners. But China's behavior troubles many nations, not just the United States. When the European Union concluded that China was a "systemic rival," it was a recognition that the unbalanced pattern of the last 20 years, where concessions to China were not reciprocated, is unsustainable.

In some ways, this decoupling is already underway as a result of private-sector decisions to reduce exposure in China. Companies cite both trade uncertainty and the risks of doing business in China. China's cost advantage has also been eroded, making other developing countries more attractive for investment. But these changes do not address the central U.S. concern on the illicit acquisition of technology by China and its unfair treatment of Western companies.

Many Chinese are unaware of the problem or dismiss it. A self-justifying narrative of China's rightful place and how it is owed for the "Century of Humiliation" combines with an abysmal lack of knowledge about China's international behavior, the product of massive censorship, to leave the Chinese baffled and unhappy that America has turned against them.

Any trade deal reached by the Trump administration will be temporary unless the United States gives up on seeking change from China. The core of the trade dispute is the Chinese failure to protect intellectual property, extend reciprocal treatment to American companies, and refrain from mercantilist policies such as the heavy subsidization of Chinese "champions." It is difficult to see how Xi Jinping could make concessions on these issues, given their centrality to the CCP's political and economic strategies. This makes increased restrictions on technology transfer unavoidable for now.

Is complete decoupling even possible? Only in theory. It would be messy, damaging, and, absent further Chinese transgressions, unlikely to attract much support from other

nations. Few nations have been willing to challenge China, and this suggests that any isolating or containing of China is not feasible. A better approach would be "selective decoupling" that allows continued engagement where it is in the U.S. interest and where risk can be minimized. To identify how to do this, the United States will need to take into account how new technologies are now created.

Assumptions about Emerging Technologies and Military Advantage

The discussion of how emerging technologies affect national security rests on the assumption that our primary strategic opponent, China, depends on U.S. sources for the acquisition of these technologies. This is not true across the board. Looking at the 14 categories of emerging technologies published by the Department of Commerce (DOC), China is a near-peer in four (AI, advanced computing, hypersonics, and surveillance). Overall, China is still dependent on the United States for advanced technologies, but it has been able to develop advanced capabilities in some specialized military areas. This alone suggests that the United States should constrain any desire to overindulge in regulation on the grounds that restricting tech transfer is enough to preserve an advantage.

The United States also risks assuming that unique U.S. technological capabilities will provide the same military and political advantages from restricting access to technology that it did 30 years ago, but we are in a different world (and in a different America), where strategy and leadership may be in short supply. Better technology does not necessarily produce military success. France had better and more tanks than Germany in 1940, but Germany had better leaders and doctrine. America had infinitely better technology than Afghanistan but no coherent strategy. Technology can increase the likelihood of success but only as one factor in combination with other factors, the most important of which are strategy, doctrine, and leadership.

Some of the emerging technologies will reshape warfare. To have military effect, most of these emerging technologies will need significant modification and "weaponization." Even then, emerging technologies must be incorporated into strategy and tactics if they to provide military benefit; having the best technology does not guarantee military success if it is badly used.

Starting in the late 1970s, when it was clear that the United States would not be able to outproduce the Warsaw Pact, the United States made developing advanced military technologies a cornerstone for its security. This was also a key period in the development of investment restrictions, export controls, and counterespionage. We are entering a similar period where defending technological advantage is increasingly important for security. Taking the changes in how the United States innovates, and the expanded role technology plays in building national power, we can identify three sets of tools the United States can use to mitigate the risk of technology transfer to China: foreign investment restrictions, export controls, and expanded counterespionage efforts.

Tool 1: Foreign Investment Restraints

Opening foreign markets for American companies has been a hallmark of U.S. foreign policy for more than a century. Opening the American market to foreign companies has paid dividends for the United States, making it the single largest recipient of foreign investment in the world, creating jobs and expanding research.[2] Recognizing the potential risks of some foreign investments, the United States created a process in 1988 to review acquisitions of U.S. companies by foreign entities for their potential national security implications called the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee composed of economic and security agencies. CFIUS, in combination with export controls, lets the United States manage risks to America's technological advantage.

CFIUS assesses the potential risk of an acquisition by looking at where foreign control or access to the company being acquired creates national security risk, the nature of the acquirers, and the sensitivity of any technology involved. This includes a mandatory review by the intelligence community of the acquirer. CFIUS does not have the rigid rules found in other regimes, but one question is whether this approach is scalable to export controls.

A 2017 Department of Defense report described intense Chinese government efforts in Silicon Valley to acquire advanced technology.[3] In response, Congress passed FIRRMA and the accompanying Export Control Act of 2018. FIRRMA closed many gaps in regulation used by China to acquire technology by expanding the scope of CFIUS reviews. FIRRMA was passed in conjunction with an export control reform bill on the assumption that strengthened export controls would reinforce regulatory tools for foreign investment and technology transfer.

FIRRMA included a number of changes that expanded the scope of covered transactions while also streamlining CFIUS processes. These include a pilot program that allows CFIUS to quickly review transactions. CFIUS can restrict foreign investor involvement in the "use, development, acquisition, or release of critical technologies" and impose conditions

2. SelectUSA, "Foreign Direct Investment (FDI): United States," U.S. Department of Commerce, 2019, https://www.selectusa.gov/servlet/servlet.FileDownload?file=015t0000000LKSn.
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 U.S. Innovation* (Silicon Valley: Defence Innovation Unity Experimental, January 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

to mitigate risk.[4] FIRRMA also mandated that the United States develop partnerships and information-sharing mechanisms with other Western nations to coordinate their foreign investment reviews.

Coordination with Allies and Partners

This coordination is essential, as experience shows that China will go from country to country when seeking acquisitions. The experience of Kuka, an advanced German robotics firms acquired by a Chinese company, prompted even Germany's Chancellor Merkel to object. The European Union has moved slowly to ensure that its member states have investment screening mechanisms. Working with the European Union to implement its Investment Screening Regulation, which will go into effect on October 11, 2020, is essential for managing the risk of illicit Chinese acquisition of technology Fewer than half of EU states currently have such screening mechanisms. The regulation does not stablish an EU body like CFIUS. It instead lays out common principles for national screening mechanisms. The United States already works with the European Union and its member states, who share (to a degree) American concerns over Chinese investment, and these common concerns create an opportunity to develop complementary approaches to technology acquisition through investment.[5]

The approach that best serves the national interest would allow continued Chinese investment when it does not provide access to emerging or advanced technologies of security concern. Private Chinese investors are looking for returns on investment. This impels them to invest outside of China. The United States is particularly attractive. However, some Chinese investors, such as those owned or financed by the state, have motives that go beyond financial gain.

FIRMMA chose to rely on regulatory processes to decide when a proposed Chinese investment should be blocked and when it should be allowed. There are still Chinese investors in the United States. Most are attracted by the opportunity for greater returns and from a desire to move money out of China. While Chinese investment in the United States has declined significantly, this reflects domestic Chinese currency controls aimed at stemming a worrisome outflow of money from China, as well as a perception among Chinese investors that they will not gain CFIUS approval, more than actual U.S. policy.

Start-ups

Start-ups—small new innovative firms—pose a more difficult challenge for investment reviews. Their products are not yet, and may never be, commercially viable. These companies do not usually have the resources to fully protect their IP and are often unfamiliar with regulation. The combination of cutting edge and erratic oversight make the transfer of technology to China from startups a major concern not just for the United States but also for Europe.

An anecdote illustrates the problem. A start-up began to develop advanced sensor technology of the kind used in DOD's Project Maven. DOD was interested in the

4. Office of Public Affairs, "Fact Sheet: Interim Regulations for FIRRMA Pilot Program," Department of Treasury, October 10, 2018, https://home.treasury.gov/system/files/206/Fact-Sheet-FIRRMA-Pilot-Program.pdf.
5. "EU foreign investment screening regulation enters into force," European Commission, press release, April 10, 2019, https://europa.eu/rapid/press-release_IP-19-2088_en.htm.

technology, telling the start-up's founders to fill out multiple forms and then await an answer that would arrive some months later. This is not how venture capital works. The same week, a Chinese investor appeared and offered to write a check for 10 million dollars on the spot. In this case, the company turned down the offer, but not all would do so, and this is not the sort of deal that would necessarily trigger a CFIUS review, even if the start-up knew of the requirements.

The best response for reducing the risk of technology transfer from start-ups is a combination of increased counterintelligence and enforcement activities, including CFIUS oversight, accompanied by a broader outreach and enforcement effort to make entrepreneurs, their lawyers, and venture capitalists aware of their obligations, particularly for in-country transfers. It is not in the interest of the United States to use heavy-handed regulation of these creative young companies, and the focus of efforts is best placed on tracking Chinese activities.

Security or Trade

One of the constants in discussion of how U.S. reviews of foreign investment should be applied is the need to focus on those that create national security risk and not use CFIUS or technology transfer restrictions for economic or trade goals. This issue came up in the FIRRMA debates (and in the European debates over investment restrictions), and some proposed that the United States add "economic security" to the list of factors that require review.

"Economic security" reflects a fundamental misunderstanding of how technology (not to mention jobs and wealth) are created. This proposed expansion of regulatory scope was rejected in the final bill on the principle that markets do a better job of guiding investment than interagency bodies. China's behavior does blur the lines between security and economic considerations but not enough that the United States should reconsider this emphasis on security in technology transfer. Europe provides many examples of how restricting openness and treating trade as a security issue can lead to stagnation.

CFIUS as a Model

The desire to allow continued Chinese investment was a key factor shaping FIRRMA. FIRRMA shows that Congressional intent was not to impose an embargo on China. FIRRMA allows for continued Chinese investment if it does not provide Chinese investors control of the company or access to technologies. The drafters of FIRRMA hoped to achieve this by identifying "emerging and foundational technologies" to which export controls could be applied. This has turned out to be very difficult because of the changed nature of innovation and the outmoded nature of how the United States controls technology transfer.

The flexibility given to CFIUS has made it the most successful of the new restraints imposed on China. After some initial consideration on whether to create lists of technology or users, FIRRMA provides CFIUS with a broad and expanded remit to decide what should be reviewed and what requires approval. This stands in contrast with the approach still used in the export control regime. CFIUS is also experimenting with a rapid approach process that could be used in other technology transfer control regimes.

Export controls need to be modernized and oriented toward promoting American exports in ways that make them better able to mitigate risk. The United States uses a "positive

list" that describes controlled items using objective performance criteria or other precise descriptions rather than broad and open-ended subjective controls. This reform was adopted in the 1980s to limit controls and allow trade with the Warsaw Pact. The positive list explains, in part, why China has been able to acquire so much U.S. technology. FIRRMA provides a general precedent for restructuring export controls. A CFIUS-like approach can be applied to those emerging technologies where a performance threshold is not identifiable.

Tool 2: Export Controls

Export controls are intended to prevent transfers of weapons or militarily useful goods and services to opponents. The premise of export controls is that one can deny an opponent the industrial and technological resources that would either erode an advantage or confer advantage on the opponent. Export controls find their roots in embargos, on either arms or raw materials, and are a form of partial embargo predicated on the idea that some items can be transferred with little or no risk.

The goal it so deny an opponent the industrial and technological resources that would either erode U.S. advantage or confer advantages on the opponent. Export controls were created in response to military challenges. They originated in the 1930s to prevent "trafficking" in arms, based on the premise that American arms sales to the United Kingdom in World War I had dragged the United States into conflict.

Dual-use technology export controls grow out of a 1940 law that gave the president the authority to "prohibit or curtail" exports in the interests of national security. It was amended in 1949 to focus on the "Communist Bloc (e.g., the Soviet Union, Warsaw Pact members, and China). Export controls were again modified in the final years of the Cold War to allow transfers of goods that did not pose a security risk. Elaborate bureaucratic processes were established to determine the threshold between what can be transferred safely and what should be denied. With the apparent end of strategic conflict in the 1990, these processes fell into a state of disuse and now need to be revitalized and refocused.

The United States has identified 14 broad categories of emerging technologies. Seven of them involve information technologies. Many of these technologies have been emerging for years (in some cases, for decades). Some of the 14 fit well with the conventional approach to export controls, but some do not, such as AI, data analytics, additive manufacturing, and brain-computer interfaces. Others, such as quantum information technology, require a new approach to export controls for some applications for the United States to reduce risk.

The Ghost of COCOM

In considering the use of export controls against China, the United States must note that this policy tool was created in very different circumstances. The global economy has evolved in ways not envisioned when the United States established its export control programs decades ago. One legacy comes from COCOM, the NATO Coordinating

Committee to review technology transfers to the Communist Bloc. COCOM still shapes U.S. policy and regulation, but today's environment is very different from the Cold War for a number of reasons. First, there was a clear political and economic bifurcation between opponents, with very little commerce between them. Second, innovation and invention rested on national scientific foundations that were largely disconnected from each other. Third, there was a unity of purpose among industrial nations.

None of these still exist. The old bifurcation between West and East is long gone. Technology and invention depend on an interconnected transnational system of research and innovation. And while there is discontent with China's behavior in many nations, it has not reached the point where nations will move quickly to constrain economic relations with China, given the high degree of interdependence and, in some instances, a reluctance to abandon the China market.

Current technology transfer restrictions do not adequately protect many emerging and foundational technologies because the system is too close to its Cold War roots. They rely on identifying categories of technology and performance thresholds to determine which technologies require prior government approval for transfer. These thresholds were conditioned on asking where a transfer would allow the Soviets to close the technological gaps that gave the United States a military advantage. Thresholds were designed to catch cutting-edge technology and keep the opponent a generation or two behind the United States and could be progressively raised to remove a technology from control as it grows older.

End-User Restrictions for Most Emerging Technologies, Thresholds for Others

The primary difficulty lies in establishing control thresholds for some emerging technologies. We cannot describe the military utility of these technologies or, in some instances, even the direction the technology will take. The intent of these thresholds is to allow transfers that are "safe," in that they are considered not to provide military or strategic advantage to an opponent. Emerging technologies can evolve quickly and could make thresholds either obsolete or ineffective. A twentieth-century export control regime will not adequately protect all categories of emerging technologies.

The Wassenaar Arrangement calls on its members to "control" dual-use goods and munitions, continuing the use of Cold War categories of sensitive items. Wassenaar's control lists form the basis for U.S. export control regulations and the regulations of other countries. What control means is a question, however, of "national discretion"—each nation decides what restrictions, if any, it will impose on exports of the controlled item. The United States tends to have the most rigid controls, while other Wassenaar members take a much more relaxed approach, not constraining their exporters in any meaningful way. However, being listed by Wassenaar is a requirement for control by the United States and a few other countries, most notably Japan.

Many emerging technologies are not at the point where they can be designated as defense articles or services nor are all amenable to the traditional DOC approach of setting control thresholds. Perhaps a third of the emerging technologies on the DOC list, including AI,

data analytics, additive manufacturing, and brain computer interfaces, fall in this category. Another third, depending on how thresholds are defined, could be controlled using the traditional approach, but there would be some risks of either overcontrolling or creating loopholes. Some emerging technologies should only be controlled if they are specially designed or modified for military use. A few, such as hypersonic technologies, fit easily into existing control paradigms. Some emerging technologies are or could be covered by existing technology transfer regimes, such as the Missile Technology Control Regime (MTCR) or the other controls on missile technology and biological and chemical weapons. Others, like AI, do not easily fall in the scope of existing regulatory regimes.

A better approach to controlling the export of emerging and foundational technologies would copy the process used in CFIUS and focus on the end use and end user in China rather than the item itself. If a control threshold cannot be identified, this approach would need to identify end users of concern and buttress any reviews with agreements with partner nations. This CFIUS-like approach would not be necessary for those emerging technologies where control thresholds can be established, like hypersonic technology, including items already controlled under the Wassenaar Arrangement—the regime for conventional arms and dual-use technologies that is best suited to cover most emerging technologies—or other nonproliferation regimes. Given the technological immaturity of some emerging technologies, this end-user approach would work best.

End-user controls avoid the need to define and adjust performance thresholds to accommodate improvements in technology. End-user controls were developed in response to the failures of a threshold-based approach to control exports related to weapons of mass destruction and are now widely used by the United States and its allies. Long experience with end-user controls for WMDs will ease implementation burdens. By restricting transfers only to Chinese entities that pose a security risk, this approach poses less risk to U.S. innovation.

End-user controls depend on identifying with a reasonable degree of certainty the recipient's identity. The country of destination can usefully guide decision on risk. In this case, transfers of emerging technologies to recipients connected to China's armed forces (the PLA) or the security services in China create unacceptable risk. A matrix of sensitivity to guide decision-making can be derived from the recipient's relation to the Chinese state or military and the immediate military utility of the technology. An export's sensitivity can be determined by considering not only the military contribution of the technology but also its "controllability"—whether it is widely available or available from sources outside the United States.

The core of the controls would be that review and approval of the transaction by DOC would only be required if an exporter knew they were selling to an entity of concern or if an exporter was informed that the recipient was of concern. This imposes a burden on the government to ensure that exporters receive adequate information. Companies quickly learn how to make judgments on which transactions need additional scrutiny (in fact, an army of consulting firms has emerged to advise them for WMD end-user controls) and trade compliance software automates implementation. The burden is on the DOC and Intelligence Community to identify end users of concern and update any relevant lists. If an entity is not of concern, a transaction could proceed without the need for approval.

Some in the export community dislike end-user controls, but when a control threshold cannot be adequately defined, the alternative to an end-user approach is to let some emerging technologies flow freely, without review of any recipient. Setting a threshold is not particularly useful for technologies that are not yet mature in their development of application and use. Using an end-user control does not mean an item cannot go to China; it means that the government may need to review the proposed transaction for security concerns;.

To use AI as a case study, there are few if any chokepoints or thresholds. AI depends on straightforward math and statistics, uses widely available coding languages, and is trained on large data sets that are either publicly available or relatively easy to create. There are recipients in China connected to the military or security services for whom access to AI technologies should be denied, and specific AI algorithms designed for military or security applications should not be transferred. But in general, this class of emerging technology does not lend itself to export controls as they are currently structured.

The current state of development for AI or quantum technologies make them more like basic scientific research, which it is not in our interest to control. An actual quantum computer is at least a decade away, but specific applications, in encryption or communications, will appear sooner. Many of the algorithms used for artificial intelligence are publicly available, and AI research is based on widely available mathematical principles. These technologies are not amenable to conventional export controls. If a technology is not controllable because it is open-source or otherwise in the public domain, or if an effort to control transfers damages innovation capabilities, export controls are not the best tool for managing risk.

New controls should identify the end uses and end users to which new controls would apply. Some specific applications, such as quantum encryption or quantum communications, should be examined for potential control. Exports or cooperative research with end users connected to the Chinese military and security-related entities should generally be denied. This would leave open the ability to work with Chinese civilian and commercial entities. There is some risk of technology leakage here, but interviews with many companies show that they believe that they gain more than they lose by a significant margin. The entities of concern are specifically the PLA and research centers directly linked to it. Going beyond these entities, while perhaps necessary in a few cases, could harm potentially beneficial transactions.

One important element of revised export controls, particular when using end-user controls, is clarity and certainty for exporters. Clarity requires sharing intelligence on end users with exporters and stating which categories of technology require review before transfer to end users of concern. The intent is not an embargo but a narrowly scoped set of controls on emerging technologies.

BIS Workforce

One implication of this is that DOC will need fewer “engineers” and more policy analysts in its export review processes. Engineers determine where a proposed export falls below a control threshold and should be approved. What DOC needs is a better ability to analyze potential end users and end uses. DOC has greatly scaled back the review process since its heyday at the end of the Cold War. It may need to ramp up given growing tensions with China.

Regulatory Modernization

What if the United States approached export controls with a clean slate? Would they look like what exists now? Probably not. In their current form, they are an artifact of an earlier and very different conflict. Dual-use controls are based on the Cold War's COCOM approach of listing categories of technologies that could contribute to the military capabilities of the Warsaw Pact forces and, within those categories, defining specific items that require government approval by setting thresholds. These have been somewhat modernized in the Wassenaar Arrangement, but ultimately, Wassenaar is based on its Cold War predecessor.[6]

Reforming and modernizing our export control system will be difficult, but the United States faces the unavoidable problem of trying to revitalize a Cold War approach, extensively modified over the years to make it more precise, less burdensome, and less restrictive, and apply it to a new strategic technology competition with China and a new technology base that is transnational and often led by the private sector. In thinking about a new approach, it should be attuned to a global innovation ecosystem and allow broad discretion in the conduct of research. This should be accompanied by cooperative arrangements and agreements among like-minded nation and by end-user controls and a robust end-user list to protect American technology without damaging American innovation.

Are There Trustworthy Recipients in China?

This is a key question for end-user controls. The more extreme China hawks would say that the answer is no. They argue that since Chinese practice and law compels citizens and companies to cooperate with any government request, backed by a readiness of the Chinese state to use coercion to achieve its ends, no recipient could deny a request to provide acquired research or technology.

In practice, however, the answer is more complex. All technology transfers, especially of end products or commodities, do not create risk. The precedent has been for China to use front companies or state-affiliated institutions to directly acquire technology, not to compel private Chinese entities to surrender it (and forcing a transfer itself could face difficulties in ensuring compliance). There are key industry sectors that the United States should prevent its companies and universities from assisting (and encourage its allies to do the same), but this needs to be caveated on whether China has access to technology from other sources, how advanced it is in indigenous development, and whether restriction does more to harm the United States

To use semiconductors as an example, the United States should not allow the transfer of production or design technology, but transfers of the products themselves do not create risk. Artificial intelligence is another example, where the United States should block work with Chinese entities connected to the PLA or security agencies but allow work with commercial entities. AI is not some all-purpose tool that is simply plugged into an existing product, and any AI product would need to be modified for military use, making end-user controls the most effective approach.

---

6. Wassenaar Arrangement Secretariat, *List of Dual-Use Goods and Technologies and Munitions List* (Vienna: December 2018), https://www.wassenaar.org/app/uploads/2018/12/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf.

Nor is Chinese government control of the economy absolute. Its practice has been to identify technologies of interest and then use state-affiliated or -supported companies or institutions to acquire them, not to vacuum up all technology entering China. The ability to monitor all transactions in an economy as vast and chaotic as China's would be challenging, especially since most Chinese domestic intelligence resources are directed at managing political dissent, and these regional and local offices are not always technologically astute. An internal collection program would pose serious management challenges, and this allows the United States to discriminate among transfers to block only those that are unacceptably risky.

The situation would be different if the intent was an embargo on China with absolutely no trade, but no reasonable person would advocate this, given the damage it would do to the U.S. economy. Nor would our allies, whose cooperation is crucial to manage technology transfer to China, be willing to accept an embargo.

For now, transfer of certain classes of commodities or non-military products and research should be allowed to certain classes of commercial and civilian end users. In general, production and design technology should not be transferred to China, but end items (like semiconductors) with little risk of reverse engineering or technology capture, should be allowed to go freely to commercial uses. These categories are those that pose acceptable risk to national security and where there are benefits of allowing continued interactions. Identifying these is a task for the Emerging Technologies Advisory Group DOC is re-establishing. The questions to ask are whether restrictions do more harm than good to America's own technological capabilities.

Ending Forced Tech Transfer

China has used forced technology transfers from the start of its opening to the West. This can involve requiring the provision of source code, design information, or other technology for "review" as a condition of purchase or mandating that a joint venture have a Chinese partner as majority owner. These are contrary to China's WTO obligations, and ending these requirements should be part of any trade agreement. The lesson is not to end trade but for the U.S. government to respond to Chinese requirements for transfer technology for market access and Chinese barriers to trade. Companies can be reluctant to push back, as they reasonably fear retaliation.

Until this goal is reached, the United States should expand and tighten its review of joint ventures—another mechanism used for forced transfers—and subject them to the same degree of restriction applied generally. A regulatory approach based on thresholds has been the source of many of the problems in forced technology transfer, since transfers that fell below the control threshold escaped review. The ability to point to regulatory oversight could also help U.S. firms in resisting Chinese demands, which most already do, by allowing them to point to regulatory requirements that prevent these transfers.

China's development of a commercial airliner is a good example of how joint ventures can build capacity. China's old Soviet-style aircraft factories made shoddy planes. When Western firms rushed to sell aircraft to China, part of the requirement imposed by Beijing for market access was coproduction, where Chinese companies worked with Western aircraft firms. Over 20 years, coproduction gave Chinese workers essential skills, and

the quality of Chinese aircraft improved. The problem, however, is not that China builds airliners, but that China will be tempted to give their manufacturers an edge in the global market through subsidies, pressure on domestic airlines to buy Chinese aircraft, and barriers to foreign companies. Similar stories could be told about semiconductors, high-speed trains and rail cars, and other technologies.

Moving away from a threshold-based technology control regime is important for closing loopholes. With skilled diplomacy, the United States could gain support for this from the European Union, Japan, and other G7 members. If China followed international market practices, its decision to invest in a domestic industry, while having potentially profound effects on business, would be unobjectionable. Moving China to adopt these practices is not impossible. Steady diplomatic pressure accompanied by skillful use of existing technology transfer restrictions and trade authorities can change China's behavior.

Things to Avoid in Export Controls

The history of export controls is replete with examples where an overly risk-averse approach or overly broad restrictions damaged or even destroyed strategic industries. In the late 1980s, two Western companies sold advanced machine tools to the Soviet Union that made Soviet submarines quieter and thus harder to detect. In response, the United States imposed new constraints on machine tools exports, which had the effect of driving machine tool production from the United States. In the mid-1990s, the United States imposed restrictions of satellite exports. As part of the Deng-era collaboration, China was allowed to launch U.S. communications satellites. This did not provide China with access to satellite technologies (satellites require delicate handling that made it very difficult for China to illicitly open or inspect a satellite as it was being prepared for launch, and in any case, each satellite was accompanied by monitors from the U.S. Air Force). Forbidding the launches denied the United States valuable and legitimate access to observing China's launch capabilities.

While China was the intended target, an overly broad approach that captured satellite technology exports to all recipients put U.S. companies at a disadvantage and led foreign competitors to advertise that they made satellites that did not require U.S. approval for sale. Similarly, when U.S. policy changed to permit the sale of U.S. earth observation satellites in the early 1990s, with the intent of strengthening U.S. industry by increasing revenues, timidity in the approval of exports cost the United States a leadership position in the market. The effect of these actions and others, such as the later restrictions on encryption exports, was to build foreign competitors and damage the U.S. technology base.

The common flaw in each of these policies was an overestimation of what the United States could control or deny. The diffusion of technology in the last quarter-century limits the effectiveness of export controls. People in other countries can also build technologies, and if the United States does not sell a technology, other countries will develop substitutes. One key lesson is that the cooperation of allies is essential. If the United States denies a technology but other advanced countries continue to sell it, as was the case with machine tools and satellites, the only effect is to damage America's technology base. For AI or quantum computing, Western coordination may involve only five or six nations. Recognizing the limits of what can be achieved is essential for a program that takes into account where an overly rigid approach will actually damage the national interest.

Tool 3: Counterespionage

China has engaged in a massive industrial espionage campaign for decades, primarily targeting the United States and its allies. China is not the only country to use economic espionage, but it is the most aggressive. Chinese espionage against the United States is at unprecedented levels. The prosecution of Chinese intelligence collectors now makes up about 90 percent of Department of Justice espionage cases. U.S. efforts to counter this espionage campaign need to intensify, but as with the previous tools, use must be predicated on a balance that delivers the best outcomes. In this case, the default position should be openness, which is the source of U.S. growth and technological advantage.

China combines official collection programs with efforts by individuals, companies, and civilian agencies. This reflects China's broad approach to foreign intelligence gathering. Instead of relying only on intelligence officers operating under cover, China uses businessmen, researchers, and students to acquire information. Chinese individuals acquire knowledge and skills by studying and working in the United States.[7] Most of these individuals pose no risk, and a cold economic calculation would show that when what they contribute while here outweighs whatever they manage to take back, they should be allowed to stay. Companies, and universities (to a lesser extent), already manage and mitigate the potential risk of Chinese employees and students, and government activities should focus on how best to improve these efforts.

It is important to note that a review of espionage cases shows that Chinese recruitment is successful with recent immigrants and temporary residents. Americans of Chinese descent are not a problem. The United States should not yield to paranoia.

Accessing the Talent Pool: Students, Deemed Exports, and Visa Policy

A "deemed export" is a term used in American regulations when a foreign national resident in the United States is given access to intangible technology. If this technology would require a license for export, it is "deemed" an export to the foreign national resident even though no border is crossed. This obligation appears to be routinely ignored, as there are tens of thousands of foreign workers but only a few thousand deemed export licenses.

7. Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrop Gunman, October 2009), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

The answer is not to expand efforts to require deemed export licenses but to strengthen company and university programs to mitigate insider risk.

In considering whether to allow Chinese individuals into the workforce or to study at American universities, the question is whether the United States would rather have them here working for us or there working for China. Answering this requires balancing the potential loss of intellectual property when Chinese employees and students return to China against the value they contribute to U.S. companies and universities while in the United States. Interviews with company officials show that they are aware of the risk of technology loss and take steps to guard against it. A common theme in these interviews is that the United States would also benefit if it made it easier for these talented individuals to stay.

Bear in mind that one of the foundations of U.S. technological strength was the flood of European scientists who arrived in the 1930s fleeing Hitler. Moreover, the ability to recruit foreign talent is a crucial part of U.S. success in science for the last 80 years. Again, an absolute perspective on restricting a foreign workforce does immense harm; a balanced approach would be to improve counterintelligence activities and let skilled workers stay.

Chinese students and high-tech workers come to the United States and learn valuable skills. The Chinese government recognizes this and makes a significant effort to lure these people back to China, often with success. There is risk from skills transfer and IP theft. However, most high-tech companies are cognizant of risk of IP theft and technology leakage and take steps to protect their IP. Based on interviews with company and university officials, Chinese individuals studying or working in the United States can be a source of technology leakage, but this leakage is outweighed by their contributions to American research and the tech industry. While heightened attention to countering Chinese espionage is important, it must not come at the cost of harming America's overall technological capabilities, and this could be the result if the United States cuts itself off from the global talent pool, including China.

There are close to 350,000 Chinese students in the United States. Some percentage of them are intelligence collectors. This is far too large a number to monitor and, in any case, such monitoring would be both distasteful and inefficient. This has led some to call for draconian measures, such as banning Chinese students or workers. This kind of ban would harm the United States. Helping universities better asses risk and providing guidelines for managing access to research would help. Universities are understaffed and often ill-informed for dealing with espionage risks. Other measures, such as disclosing the source of research funding, may be less useful if the disclosures do not also provide the conditions under which funding was provided. The issue is not where the money to support research comes from but where the products of the research will go.

The top priority is to ensure that companies and universities receive intelligence support and have robust systems in place to ensure that access to sensitive technologies is controlled. This is primarily a task for the FBI, which needs to provide advice and assistance. Some categories of student activities, however, deserve review. Undergraduate students pose little risk, but Chinese connected to the PLA should not be allowed to study in the United States, and there are some categories of applied research with potential military applications that Chinese students should not be allowed to participate in at the graduate level.

It is not easy to determine how much risk a Chinese visa applicant poses, given the paucity of information available for background checks, but there are measures that could reduce risk. One would be to identify Chinese "minders" sent to universities to keep an eye on other Chinese students and ensure political conformity. Judging from past practice, recent counterdemonstrations, for example, over Hong Kong, were likely orchestrated by the Chinese government throughs embassy officials and these minders. These individuals are agents of the Chinese government and should have their visas revoked. FBI programs to advise universities and companies on the risk of espionage and the "insider threat" should be reinforced, and the FBI presence in American technology centers like Silicon Valley, Austin, or Cambridge, should be expanded, both for building partnerships with the technology and research community and to engage in traditional counterintelligence activities. Reinforcing these efforts to expand cooperation between companies, universities, and government means that counterintelligence activities will be complemented by foreign investment reviews and export controls.

It is clearly not in the national interest to have sensitive and unique weapons-related information, classified or not, leak from the United States. It can be difficult to weigh the benefits brought by the work of foreign researchers in U.S. laboratories and universities against the potential cost of their gaining technical knowledge in the United States and then returning home. At the same time, the United States cannot afford to cut itself off from sources of highly-skilled labor or from the advances in research that foreign nationals bring to U.S. universities, labs, and companies. There is real concern that the United States will find it harder to conduct research at the cutting-edge if foreign nationals are routinely denied access. However, this is not a new issue: a push to expand the use of deemed exports came up early in the Bush administration, and the experience from that period reinforces the need for openness.

Three broad principles should guide U.S. actions. First, Chinese individuals connected to the military and security services should, when identified, be denied access to research and technology. Second, Chinese students and researchers should continue to be denied access to technologies of direct military relevance without prior government approval. Third, Chinese acting as agents of the governments (as "minders" for other students, for example) should have their visas revoked. Students and researchers who do not fall into one of these categories should be allowed to continue their work.

Reaffirm NSDD-189

In 1985, the Reagan administration, at a time of great concern about the Soviet threat, issued the National Security Decision Directive 189 (NSDD-189), which stated that "to the maximum extent possible, the products of fundamental research remain unrestricted." NSDD 189 made the primary method for controlling access to information generated in universities and research centers the classification process, not regulatory extensions of export controls. It recognized that an open environment is crucial to the advancement of basic science, and that national security depends not just on protecting secrets but also on a healthy and vibrant economy that grows through the introduction of new ideas.

Some now ask if NSDD-189 should be reversed and basic research made subject to technology transfer restrictions. But extending export controls to basic research would do

more harm than good for the United States. Scientists from labs and universities say that this would make it increasingly difficult to carry out their research. This is not a question of science versus security but of what approach best serves U.S. national interests.

If China's increasingly restrictive domestic policies create an "innovation deficit," the Chinese government will respond by increasing investments in science and technology, by exploiting legitimate means of technology transfer, such as sending students to Western universities, and by increasing its espionage activities. A more restrictive China, however, may also encourage Chinese researchers to move. As with export controls and CFIUS, the United States must balance competing priorities in counterespionage. The first goal is to reduce spying, but the second and more important goal is to ensure continued American access to the global talent pool, including talent from China. There is more than 30 years of experience to show that NSDD-189 serves American interests.

Cybersecurity

Cyberespionage is the primary vehicle for illicit acquisition of American technology by China. This has been going on for two decades. Chinese cyber espionage and the theft of IP costs the United States tens of billions of dollars annually. A 2015 agreement between China and the United States to stop cyber espionage for commercial purposes by state actors is no longer observed, and the United States will need to consider how to respond to China's cyber espionage.

How to improve cybersecurity has been discussed at length (and some would say ad nauseum) in the United States, but progress has been slow. The usual solutions involve information sharing, better cyber hygiene, and voluntary efforts, although DOD and DOE are adopting mandatory cybersecurity requirements. Companies have improved their cybersecurity performance over the last decade, but opponents' offensive cyber capabilities have kept apace. The fundamentals remain the same: better cyber "hygiene" and authentication of identity, greater reliance on "cloud services," and improved monitoring of networks. The incentives to mandate such action will increase as more devices are connected to the internet and risk grows.

However, improved protections will only take the United States so far, since China is a determined, well-resourced, and persistent cyber adversary. While improving cybersecurity at businesses and universities is important, as is making American entities aware of the threat, the United States will need to reengage with China on the topic. Since reaching another agreement to constrain cyber espionage could take years (the United States and China agreed to limit commercial espionage in 2015, but China no longer observes the agreement), the United States will need to develop and use countermeasures, such as the continued use of sanctions and indictments, as well as other retaliatory actions, against Chinese actors. U.S. cyber strategy is increasingly defined by "persistent engagement" and "defend forward." These policies bring some risk, but unless the United States increases the consequences for Chinese espionage in ways that are painful but also temporary and reversible, there is no incentive for China to stop its cyber espionage campaign.

An Alliance Strategy is Crucial

It is possible to change Chinese behavior but only in partnership with other key economies—Japan, Canada, Germany, and other EU members. A coordinated international response is the cornerstone of a campaign to change Chinese behavior, and many of our allies are ready to cooperate. An alliance strategy is crucial for counterintelligence, financial restrictions, and export controls. The United States will need a broad partnership to effectively use diplomatic and economic tools to compel change by China.

This joint approach made it clear that it was not just the United States that had concerns with China's behavior, something that is important for China in its own decision-making processes. Coordinating financial reviews and export controls will make it more difficult for China to circumvent American rules in its efforts to acquire technology.

This partnership may require a new grouping, perhaps informal, whose core might start with the "Five Eyes," a group of Western intelligence partners but be expanded to include other important economies. A growing number of nations agree on the risk from China's predatory economic behavior and are willing to coordinate policies to curb Chinese technology acquisition and espionage. The United States can build on existing cooperation in investment screening and on the Wassenaar Arrangement, which provides a platform for cooperation on export controls. Whether they would curtail trade is another matter, and the desire to continue selling to China is one of the greatest challenges to a broad alliance strategy. Japan and Australia, perhaps because they are closer geographically to China, are ready to cooperate in restricting technology transfer. But some European nations, while they realize that the "Golden Age" of cooperation with China (as UK prime minister Cameron used to call it) is over, are unsure what will take its place.

In the past, China has made concessions when these nations delivered a consistent message about the need for change (the most salient example would be nonproliferation). Repeating this will be more difficult now, as China's leadership has become more assertive with its economic success and accustomed to ignoring WTO commitments, but an alliance approach with a common message for China offers a greater chance of success. Its absence is perhaps the greatest weakness of this administration's China policy. The goal is not containment but to compel China to observe international rules and practices, and one American advantage is that it has allies and China does not. The Unites States needs to take advantage of this.

Defense Is Not Enough

U.S. technological leadership has flourished by embracing openness. Technology and innovation do not follow the political map nor is it in the U.S. interest to pursue reliance on national supply chains. Technology is no longer created in discrete national systems, and there is considerable research that shows that the best outcomes are provided by transnational innovation and research systems. Imposing regulations that restrict scientific openness would harm the United States.

Being open makes the United States stronger than being closed, but this openness cannot be laissez-faire and unguided. When Western companies first went to China, they believed that the damage from espionage was tolerable, that it was merely the cost of doing business in the world's fastest-growing market, and that they could "run faster" in creating new technologies, thereby minimizing any loss. But what was tolerable when China was a developing economy is no longer acceptable when it is the second-largest economy in the world and a potential military competitor.

Until Chinese policy changes, the United States should not assume that FIRRMA and ECRA are the end of the story. U.S. opponents are inventive and opportunistic. FIRRMA closed several loopholes; the Chinese will look for new ones. For example, Huawei now goes to an infamous court in Texas used by patent trolls and files suits alleging that its patents have been violated, thus forcing the American target to provide access to proprietary technology as part of its defense. The cases are specious but serve as a new way to obtain American technology.

These tools—continued screening of Chinese investment, adoption of "end user"-based controls for most emerging technologies (similar to what is used in the CFIUS process), and an increased effort at countering Chinese espionage in the United States—will let the United States manage technology transfer risk to an increasingly hostile power. However, they are defensive. They block transfers. The most important response to China is to strengthen America's own innovative capabilities. The United States cut investment in science, research, and education after the Cold War; now that it is back in a strategic conflict, it needs to resume this support.

IP theft is not the only source of China's growth. China gave priority to the development of research and engineering skills. While the Chinese are trapped by their own politics in taking the less successful path for innovation, they have one clear strength when

compared to the United States: their willingness to spend on public goods, like education and research.

We often hear that the private sector will drive innovation, but this is inaccurate and an excuse for cutting federal spending. First, many key innovations—from semiconductors to the internet—grew out of federally-funded research. The ability of the United States to take federal research and turn it over to the private sector for commercialization is an immense strength for U.S. innovation, but if there is no federal research, there is nothing to turn over. Second, the private sector will not adequately supply advanced military technologies. While there are commercial technologies that can be adopted for military use, some military technologies have no commercial application, making it unlikely the market will supply them.

Equally important, federal support for research, science, and education builds the technological workforce American industry needs. If the number of Chinese students is a concern, the United States is doing nothing to replace them with American students. One reason there are so many foreign employees in U.S. companies is that there are not Americans with the skills needed for these technology sectors. The United States has made it prohibitively expensive for students to get advanced degrees.

The United States spent $66.5 billion in basic and applied science and technology research in 2017. This is about 1.7 percent of all federal spending and only 0.3 percent of GDP. For historical contrast, the United States spent a similar amount (0.2 percent of GDP in 1956), comfortable in its technological lead. But after the launch of Sputnik in 1957 and the realization that it had entered a serious contest where the United States risked being surpassed, research spending rose to 3.6 percent of the federal budget.

Federal research spending today is also skewed away from the sciences that produce military advantage. Almost half of all civilian spending on R&D goes to the National Institutes of Health. The Department of Energy spends its funding on nuclear security and energy. These do not build the hard sciences (which include most of the emerging technologies) that underpin military technology. The National Science Foundation, which funds hard sciences, received 0.01 percent of the federal budget in 2017, which cannot be regarded as a serious investment if the United States is indeed in a technological race with China. Private-sector spending will also not remedy this. U.S. companies spend about $24 billion a year in basic research federal investment but focus the bulk of their spending on development. This makes sense from a commercial perspective, but not for national security. In contrast, China's R&D spending reached $410 billion in 2016—more than Japan and Germany. China graduated 5 million STEM graduates—almost 10 times the U.S. number. Can we call it a race if one side appears strolling and not to be running?

Additionally, our best researchers spend a third of their time not doing research but filling out forms and applying for a shrinking pool of grants (a remarkable inefficiency, like having the star players of a major league baseball team sweep the field rather than practice and play ball). The Chinese do not have these problems and provide immense, consistent support for research and education. This may ultimately allow them to pull ahead.

None of these recommendations on how to strengthen technological innovation in the United States are particularly new, and there are major political obstacles to acting on

them. It is disinterest by elected leaders in preserving American's technological advantage that is most troubling. At the start of the Cold War, under Eisenhower, America built the science and education programs that allowed it to outperform the Soviets, but the impetus for this was a single incident—the Soviet launch of Sputnik—which was widely heralded as evidence that the state-centric model for science and industry was inherently superior to market democracies. Sputnik sailing overhead energized American innovation. This time, however, there may be no Sputnik, nor can the United States afford to wait for one.

About the Author

James Andrew Lewis is a senior vice president at CSIS and director of the Technology Policy Program. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes a broad range of political-military, negotiating, and intelligence assignments, including leading the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civilian and military technologies. He worked on presidential policies on a range of topics, including securing and commercializing the internet. He was the Commerce Department lead for national security and espionage concerns related to high-technology trade with China. Formerly, Lewis was the rapporteur for the UN Group of Government Experts on Information Security. He has led long running Track 1.5 discussions on cybersecurity with the China Institutes of Contemporary International Relations. He has served on several federal advisory committees, including as chair of the Committee on Commercial Remote Sensing. He was the director for CSIS's Commission on Cybersecurity for the 44th Presidency and is an internationally recognized expert on cybersecurity. He received his PhD from the University of Chicago.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**