Department of Commerce, Bureau of Industry and Security: Advanced Notice of Proposed Rule-making: Review of Controls for Certain Emerging Technologies

James A. Lewis, Center for Strategic and International Studies
January 2, 2018

Recent legislative changes call for enhanced scrutiny on potential transfers of "emerging and foundational technologies." These are broadly defined as technologies essential to U.S. national security. The Congressional intent is for agencies to develop a more specific list, with robotics and artificial intelligence as primary concerns. Developing this list raises several issues. These include how to determine the military utility of an emerging technology, how to control the diffusion of the technology, and how to manage the risks of increased control for American innovation.

Enhancing controls on the transfer of emerging technologies is necessary for several reasons. First, the U.S. finds itself in a contest with China. China intends to eventually displace the U.S as a global leader in technology, part of its larger effort to expands its influence and power. China is a technological rival of a kind the U.S. has never had before, given the deep interconnections between the two economies. China is still dependent on the West for advanced technology and uses a combination of techniques to acquire it. The 2015 Obama-Xi agreement on commercial cyber espionage attempted to address the problem, but China now ignores that agreement. In this environment, strengthening oversight of technology transfers from the U.S. and its allies to China is essential. In particular, new rules are needed to review technology transfers through coproduction, join ventures, or intangible exports, as these have been a major source of China's access to technology.

Second, current controls on technology transfers do not adequately protect emerging and foundational technologies. The current technology transfer control system is too close to its Cold War roots. Thresholds were set by asking what was the state of the art, how close our Soviet competitor was to this, and whether a technology was "controllable" or if it had become a commodity or was widely available from foreign sources. These are no longer the right questions to ask. The approach needed now is whether we want to transfer a technology to China and whether an effort to prevent this would do more harm than good to America's own technological capabilities. This calls the whole complex structure of precise control thresholds into question.

Modernizing export controls will be difficult, but the proposed rulemaking offers an opportunity to begin the process of revision. Export controls have their background in the 20th Century, when two bifurcated economic blocs were in competition and where thresholds for controls could be set with a degree of precision. This is no longer the case. Attempting to layer a 20th century export control regime over the new dynamics of global trade and innovation will not adequately protect emerging technologies. Reform will necessarily be an iterative process, part of a larger restructuring of export controls for a new international environment.

A key point to bear in mind is that since China is still dependent on advanced Western technology (and this is unlikely change in the near future), access to western technology should be used to gain leverage in talks to change China's aggressively mercantilist policies. This will

be difficult, and it will take time, but a failure to confront China and bring about change will lead to the outcomes that technology controls seek to avoid. The goal is not to defeat or contain China, but to brings its practices in line with international expectations in ways that allow commercial relationships to continue without risk to national security.

Rethinking Technology Transfer

Technology transfer has been an issue since China's opening in 1979. The original U.S. policies assumed bilateral cooperation. The U.S. supplied military technology (such as Blackhawk helicopters and Copperhead guided artillery rounds) and allowed China to launch U.S. commercial satellites. Security cooperation was based on the presence of a common opponent, the Soviet Union. Commercial cooperation was shaped by the belief that China would become a market democracy and that bilateral relations would be amicable. Whatever the soundness of these assumptions at the time, with the ascent of Xi Jinping they are no longer valid.

A 2017 Defense Department Report[1] described intense Chinese efforts in Silicon Valley to acquire advanced technology licitly or illicitly. In response, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA), signed into law by the President in August. FIRRMA closes many gaps in regulation used by China to acquire technology by expanding the CFIUS review to include, among other things, "critical technologies," and was conditioned on the assumption that strengthened exports controls could reinforce its protections. FIRRMA is the cornerstone of a larger effort to use the regulatory tools for foreign investment and technology transfer, such as the Committee on Foreign Investment in the United States (CFIUS) to block risky acquisitions.

Managing this new competition with China using these regulatory tools will be difficult given the close interconnection between the U.S. and Chinese economies. This is a 30-year commercial and technological partnership not easily dismantled by either side. Given the deep interconnections that have grown between the Chinese economy and the rest of the world, a bifurcation similar to that seen the Cold War would be difficult and costly, and it is not in our interest. An abrupt rupture would damage U.S. interests; creating a greater degree of separation must be carefully mapped to individual technologies and part of a larger strategy to change China's behavior to make it consistent with international norms.

21st Century Innovation

Two significant changes affect the U.S.' ability to regulate emerging technology transfers. The first is in how research and innovation are conducted. These are no longer national activities. They are transitional, increasingly relying on a globally mobile workforce and the exchange of ideas and investments across borders. This multinational approach is now the most productive for research and business and the U.S. has an advantage over China as it increasingly turns to a reliance on national champions and indigenous innovation.

The global economy has evolved in ways not envisioned when the U.S. established its export control programs decades ago. Commercial activities are now routinely conducted through

[1] https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf

international partnerships, through mergers or long-term strategic relationships. Companies routinely partner with foreign vendors to take advantage of specialization, to spread the risk of development or to insure market entry for new products. International partnering is the norm,

Multinational research provides an advantage in both cost and innovation over nationally based systems. Unlike the Cold War, emerging technologies are created in a transnational research and innovation ecosystem. In this environment, there will always be some technology leakage and the leakage will be greater than it was thirty years ago. Recognition of the changed nature of technology research and creation is a fundamental problem for this interagency effort. This includes considering where Chinese investment in American technology and joint ventures provide more benefit than cost. Layering national regulations on top of this transnational ecosystem is will be difficult.

The second issue complicating this effort is that innovation is now largely a commercial activity. The innovations and emerging technologies that will shape military power in the future come largely from commercial sources. They are not specially designed for military application and will need to be modified and adopted to provide military utility. This means they are not "dual-use" in the conventional sense any more than cloth or steel, which may be used for military purposes, are not considered as falling within in the scope of controlled goods. Congressional intent was not to impose an embargo on China (beyond the current restrictions on munitions and proliferation-related items). This means that technology transfers to China for commercial or fundamental research purposes should continue.

The costs of denying technology transfers include reduced revenue and market share for U.S. companies, reduced access to high skilled foreign individuals such as researchers or engineers, and, potentially, a reduction in the scope of innovation in the U.S. The best decision may sometimes be counterintuitive – in considering whether to allow Chinese into the workforce or to study at American universities, the question is whether we would rather have them here working for us or there working for them? Answering this requires balancing the loss of intellectual property when Chinese employees and students return to China against the loss to U.S. companies and universities. The answer will not be black or white, and part of any solution will require developing measures to reduce the outflow, and the best measures might be internal company controls accompanied by expanded counter-espionage efforts.

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 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 for the U.S.

To use AI as an example, this ecosystem stretches from the UK, Canada, and Israel to China and other economies in Asia, with Silicon Valley at the center. Constraining this global ecosystem could slow the pace of American innovation. AI, like many emerging and foundational technologies, depends upon an international workforce; the U.S. needs to weigh carefully any workforce restrictions (or on foreign students) in light of this. AI research depends on open

processes; closing it in the US will slow innovation in the US and likely advantage other countries. In light of these challenges, developing an effective regime for controlling the transfer of emerging technologies will be difficult. However, it is possible to identify a set of principles that any successful regime must adhere.

Fundamental research or open source technology should not be subject to control.

Basic or fundamental research should not be subject to control. The decision made by the Reagan Administration in 1985 National Security Decision Directive 189 to exempt fundamental research from control has justified itself many times in that the return to American science and innovation outweighs any possible loss. This decision was reviewed by both the George W. Bush and the Obama administrations, who came to the same conclusion that fundamental research should be exempt from control as an open research system is more likely to maintain U.S. technological advantage.

The current state of development for AI and quantum technologies makes them more like fundamental research. Many of the algorithms used for artificial intelligence are publicly available and some AI research is based on basic research using widely available mathematical principles. If a technology it is not controllable because it is "open source" or otherwise in the public domain, or if an effort to control transfers damages innovation capabilities, other investment, trade and counter-intelligence tools may be better for protecting an American advantage.

Chinese studying or working in the U.S. are a source of technology leakage, but the U.S. gains more than it loses. Chinese students and high-tech workers come to the U.S. and learn valuable skills. The Chinese government recognizes this and makes a significant effort to lure these people back to China (such as the 1000 Talents Program), often with success. There is risk from skills transfer and IP theft, but export controls are not the best way to mitigate this risk. Many high-tech companies are cognizant of risk of technology leakage and take steps to protect IP and know-how, finding ways to reinforce this approaches could be developed in cooperation with companies and universities as part of a larger package of foreign investment reviews, export controls, counterespionage activities and enhanced intellectual property enforcement.

Catch All for Some Emerging Technologies, Thresholds for Others

Many emerging technologies are not described on the Commerce Control List and have not yet been evaluated for their national security effect nor accepted for control by multilateral regimes. Most emerging technologies are not at the point where some can be designated as defense articles or services, nor where the traditional commerce approach of setting control thresholds can be meaningfully applied. We cannot assume their military utility with a degree of precision and, in some instances, even the direction the technology will take. Nor will it be easy in many cases to define precise thresholds to allow for export of technologies deemed not to provide military or strategic advantage to an opponent while controlling the most advanced technology. These problems are part of the rationale for export control reform.

Some emerging technologies can be clearly linked to potential military applications. A few

listed by Commerce (such as hypersonic technologies) will be easier to fit into existing control paradigms. Others cannot, unless they are specially designed or modified for military use. An interim approach to emerging and foundational technologies would copy the process used in CFIUS and use a combination of catch-all controls focusing on the end-use and end-user in China rather than the item itself, identifying end users of concern, and agreements with partner nations. This CFIUS-like approach would not be necessary for emerging technologies where clear control thresholds can be established, including items already controlled under the Wassenaar arrangement or other regimes.

Overly broad restrictions on emerging technologies will damage the national interest. Scoping controls by setting technical thresholds is problematic, as emerging technologies can evolve quickly and could make thresholds either obsolete or ineffective There has been reluctance in the past to make it clear that these controls would be China specific, but among our opponents, only China is in a position to take advantage of access. Our concerns will not come as a surprise to the Chinese and other technological competitors do not pose a national security risk. Focusing specifically on China avoids the burden of extensive reviews. A catch-all avoids the need to define precise thresholds for technologies whose military application is not yet established. In combination with a list of Chinese entities that cannot receive these technologies, this approach poses less risk to U.S. innovation.

Some in the export community dislike a catch-all, and for some of the technology categories being considered, a threshold can be defined. But when a control threshold cannot be adequately defined, the alternative to a catch all is to let some technologies flow freely, a particular problem for technologies that are not yet mature in the development of their application and use. Given the technological immaturity of some emerging technologies, this approach would work best. Congressional intent is to reduce the transfer of technology to China, which means that some transfers that did not raise objections in the past will no longer go through.

The problem with a catch all is that it may catch too much. The usual solution is to include a list of end uses and end users to which the catch all would apply, in this case, end users connected to the Chinese military and security-related entities. This would leave open the ability to work with Chinese civilian and commercial entities (putting aside the issues of the difficulty of discerning the background of Chinese). 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. In the past, the U.S. policy has emphasized openness. Counterintuitively, this has proven to be best for national security. Using a catch all to over-control can kill industries without hampering opponents. This suggests that the initial scope of new controls should be narrowly scoped (allowing for later adjustment as technologies mature and as the interagency community gains experience).

Controls for emerging technologies should not apply to commercial end items.

Controls on emerging technologies should focus on restricting transfers of intellectual property, "know how," and production equipment. Controls on end items should generally be avoided. "Reverse engineering" from a commercial product for developing new military capabilities is less of a concern than is Chinese acquisition of intellectual property and know-how, and this is

where controls on emerging technology should focus.

Kuka, an advanced robotics firm, is a salient example. The Germans regret the decision to allow a Chinese company to buy Kuka, as it gave China access to technologies (and markets) which had been unattainable. The Kuka example allows us to parse what kinds of emerging technology should be controlled. Any joint venture between a firm developing emerging technologies and a Chinese firm should be subject to careful review and require approval, as should any transfer of technology or intellectual property. Transfers of robots intended for commercial manufacturing should generally be allowed to legitimate end users. Efforts by the Chinese to reverse engineer or copy the technology (which are not uncommon) should be addressed through a campaign using all the tools available for patent infringement, including penalties, lawsuits, sanctions and broader trade measures.

The risk of transferring consumer goods that incorporate advanced technologies is a long-standing debate in export controls (such as concerns about exports of the Xbox to China because it contained an advanced chip), but these rarely make sense. A recent example involves the export of GPUs to Chinese smart car companies, which some said should be blocked. While GPUs may be considered a foundational technology, their export to commercial end users does not create unacceptable risk. In only a few emerging technology areas, such as biotechnology, material research, advanced surveillance technologies, and some AI applications (like audio and video manipulation), is China likely to have equivalent technological capability that will allow them to succeed in reverse engineering.

"Start-ups," new innovative firms, pose a different challenge. Their products are not yet (and may never become) commodities. These small companies do not have the resources to fully protect their IP and are usually unfamiliar with regulation. The primary concern is the transfer of intangible technologies through Chinese investment or participation. FIRMMA rejected greater controls on "Greenfield" investment by China in emerging technologies and chose instead to rely on regulatory processes to decide when Chinese investment should be blocked and when it could be allowed. The best response for startups is a combination of increased counter-intelligence and enforcement activities, including CFIUS oversight on investment from China, accompanied by a broader outreach and enforcement effort to make entrepreneurs and venture capitalists aware of their obligations for technology transfers, particularly in-country transfers.

Controls for emerging technologies will need a new approach to likeminded cooperation in parallel with existing multilateral regimes

While agreement on control in the Wassenaar Arrangement or other regimes remains desirable, it should not be used as an excuse for not imposing new controls. It will be easier to start with a limited approach, working with technologically advanced, like-minded nations that share our security concerns over China. A new approach would draw on precedents other than the Wassenaar Arrangement. For example, the bilateral agreement between the U.S. and Japan on the export of high-performance computers, although ultimately folded into Wassenaar controls, allowed both countries to coordinate safeguards on sales of an advanced technology. For AI or quantum computing, western coordination for example, this may involve only five or six nations.

The reasons for controlling technology transfers include seeking to deny an opponent improved military capabilities, restricting access to technology to reduce the risk of proliferation, and to improve regional stability by preventing dangerous buildups of weapons and military-related technologies. In the past, the U.S. has not restricted technology transfer to maintain a commercial advantage – this issue of protecting "economic security" came up in the recent debates over CFIUS reform, which decided against an economic security approach. "Economic Security" is not a criteria in Wassenaar or the proliferation regimes; it should not be used as a justification for control in any new approach to China.

Given the deep interconnections that have grown up between the Chinese economy and the rest of the world in the last decades, a bifurcation similar to that seen the Cold War would be difficult, costly, and not easy to impose, nor would it be in our interest to do so. This creates the fundamental tension for policy – how to restrict Chinese access to emerging and foundational technologies while minimizing risk and damage to the economies of the U.S. and its allies. Blanket denials or other draconian measures are likely to do more harm than good.

Broad discretion in the conduct of research, accompanied by cooperative arrangements and agreements among likeminded nations, and by catch-all controls and a robust end-users list are, for now, the approach most likely to protect American technology without damaging American innovation. The fundamental tension for policy is how to restrict Chinese access to emerging and foundational technologies while minimizing risk and damage to the innovation economies of the U.S. and its allies. Blanket denials or other draconian measures are likely to do more harm than good. China's unfair trade practices and industrial espionage are no longer tolerable, but any response should do more to constrain China than it does to the U.S. and its allies.

Export controls grow out of arms embargos and economic warfare, but these blunt instruments were modified in recognition that not all transfers posed risk and the net benefit to the U.S. usually justified an export. This led to the development of a complex system to decide what goods and technologies should scrutinized and when their export required explicit government approval. Our goal cannot be to cut the two-way flow of technology and expertise between the two countries, but to manage it in ways that mitigate risk to national security. Displeasure with China's rampant espionage (against which we should retaliate) and unfair practices should not disguise the fact that this two-way flow, properly regulated, can serve our interest more than China's.