Policy Analysis

CATO INSTITUTE

July 13, 2017 | Number 815

Cybersecurity or Protectionism?

Defusing the Most Volatile Issue in the U.S.–China Relationship

By Daniel Ikenson

EXECUTIVE SUMMARY

For more than a decade, the United States and China have been engaged in a low-profile, high-technology trade war that has been conducted in the name of protecting critical economic and national security infrastructure from cyber malfeasance. But the trade restrictions and subsidies suggest that the objectives of both governments have less to do with cybersecurity than they do with industrial policy and protectionism.

For several years, Chinese information and communications technology (ICT) companies effectively have been blacklisted by the U.S. government, which continues to actively advise U.S. telecommunications firms to avoid purchasing their products. On more than one occasion, the Committee on Foreign Investment in the United States (CFIUS) raised security concerns over prospective acquisitions of U.S. companies by Chinese ICT companies, ultimately preventing those transactions from taking place.

Meanwhile, following a decade of evolving indigenous innovation policies intended to catapult China into a position of global technological preeminence, the Chinese government has begun implementing a set of new laws that effectively require imported ICT products and components to be secure and controllable. U.S. companies are interpreting that to mean that there will be delays and other uncertainties that adversely affect their supply chains and that they will be forced to provide Chinese authorities with proprietary information about their products, which could compromise their intellectual property and deter trade, investment, and the scope for collaboration in these industries.

Cyberespionage, cybertheft, and cyberterrorism constitute real threats to infrastructure that governments have a legitimate interest and obligation to protect. But effective cybersecurity measures cannot be developed in a vacuum, as if there were no tradeoffs to consider.

To achieve greater cybersecurity, the United States and China can and should adopt policies that wed valid statistical methods with best business practices, while minimizing disruptions to legitimate, growth-enhancing trade and investment. Meanwhile, protectionism can and should be redressed by harnessing the rules and resources of the World Trade Organization (WTO).

Daniel Ikenson is director of the Cato Institute's Herbert A. Stiefel Center for Trade Policy Studies.

> "Economic protectionism, not cybersecurity, seems to be the primary objectives of both the U.S. and Chinese governments."

INTRODUCTION

Considering candidate Donald Trump's famously strident rhetoric about how he would deal with Chinese trade practices, President Trump's economic policy toward China so far has been unexpectedly mild. In fact, his highly anticipated April 2017 meeting with Chinese President Xi Jinping may be remembered best for its absence of fireworks, while the highlight of the U.S.–China economic relationship thus far is an agreement to work on removing several longstanding bilateral trade impediments. While comity in the relationship is welcomed and encouraged, any benefits derived from that agreement will pale in comparison to the costs of failing to remedy certain long-simmering grievances.

Among the most serious sources of trade policy tension are the measures taken by both the U.S. and Chinese governments in the name of cybersecurity. Washington and Beijing have instituted some ill-considered policies, ostensibly to protect critical economic and national security infrastructure from cyber malfeasance. But those measures also have the effect of impeding foreign trade and investment to the point that economic protectionism—and not cybersecurity—seems to be the primary objectives of both governments.

For several years, Chinese information and communications technology (ICT) companies effectively have been blacklisted by the U.S. government, which continues to actively advise U.S. telecommunications firms to avoid purchasing their products. On more than one occasion, the Committee on Foreign Investment in the United States raised security concerns over prospective acquisitions of U.S. companies by Chinese ICT companies, ultimately preventing those transactions from taking place. And since 2013, U.S. appropriations legislation has included provisions that effectively would prevent certain federal agencies from procuring or using ICT products made by Chinese companies.

Meanwhile, following a decade of evolving indigenous innovation policies intended to catapult China into a position of global technological preeminence, the Chinese government has begun implementing a set of new laws that effectively require imported ICT products and components to be "secure and controllable."[1] U.S. companies are interpreting those words to mean that there will be delays and other uncertainties that adversely affect their supply chains and that they will be forced to provide Chinese authorities with proprietary information about their products—under the guise of promoting national security and cybersecurity. These new laws are high on the list of concerns of U.S. ICT companies, which fear the measures could compromise their intellectual property and deter trade, investment, and the scope for collaboration in these industries.

Cyberespionage, cybertheft, and cyberterrorism constitute real threats to infrastructure that governments have a legitimate interest and obligation to protect. But effective cybersecurity measures cannot be developed in a vacuum, as if there were no tradeoffs to consider. ICT products are essential building blocks of the 21st century economy, so cybersecurity policies must strike the proper balance by securing those assets without unnecessarily impeding innovation and economic growth.

This paper argues that U.S. and Chinese cybersecurity policies fail to achieve that balance because their real objectives are economic protectionism. Accordingly, U.S. and Chinese policies provide a false sense of cybersecurity; reduce the scope for innovation, collaboration, and economic growth; and threaten the global trading system.

To achieve greater cybersecurity, the United States and China can and should adopt policies that wed valid statistical methods with best business practices, while minimizing disruptions to legitimate, growth-enhancing trade and investment. Meanwhile, protectionism need not be met with protectionism. Instead, protectionist policies can and should be redressed by harnessing the rules and resources of the WTO.

CHANGING PERCEPTIONS AND EVOLVING POLICIES

For nearly two decades ending roughly with the Great Recession in 2008, U.S. economic

policy toward China was essentially sequestered from other, more fraught policy matters such as human rights, security, and geopolitics. The economic relationship was intended to emphasize areas of agreement, where there was vast potential to broaden and deepen bilateral commercial ties. Inevitable frictions arose, but were managed reasonably well through quiet diplomacy, bilateral dialogue, WTO dispute settlement, and domestic trade remedy laws.[2]

Perceptions of the relationship began to change in Washington around 2007, when it became clear that China had succeeded—in the course of a single generation—at transforming itself from a mostly agrarian, subsistence economy into a manufacturing powerhouse, and that Beijing had designs on leapfrogging the United States to become the world's preeminent high-technology, information-intensive economy.

A document published in 2006 by China's State Council titled "The National Medium- and Long-Term Program for Science and Technology Development" presented a road map for transforming the Chinese economy into a major innovation center by 2020 and an innovation leader by 2050.[3] The blueprint included a goal of dramatically reducing China's use of foreign technology by promoting "indigenous innovation,"[4] which would be achieved through implementation of policies that gave preference to companies with products containing intellectual property registered in China, and by developing new technology standards.[5]

As the protectionist implications of this document were being absorbed in Washington and in the boardrooms of U.S. and other western technology firms, a Chinese ICT company called Huawei Technologies made a bid to acquire U.S. software company 3Com. But opposition to the deal from certain U.S. policymakers—and eventually by the Committee on Foreign Investment in the United States (CFIUS) on the grounds that the transaction, if consummated, would present a threat to U.S. national security—caused the parties to abandon the deal in 2008.[6]

The financial crisis in 2008 and subsequent recession accelerated the change in perceptions in Washington. While the United States was mired in slow growth, high unemployment, and growing public debt (much of it owned by the Chinese government), China's economy was still chugging along at double-digit annual growth rates on a seemingly inexorable trend line to surpass the United States in every relevant economic metric. That set of circumstances alarmed U.S. policymakers and analysts and prompted a period of introspection over the questions of where the United States went wrong and what China got right.

One conclusion was that China's accomplishments had something to do with the successful execution of a supposedly well-disciplined, well-coordinated industrial policy, and that the United States should pursue a similar path. Another conclusion was that U.S. policy had been too accommodating of China's rise and that it was time to address the challenge presented by a rapidly ascending rival—and potential adversary. Ultimately, the consequence of this recalibration of perceptions was that U.S. economic policy toward China would no longer be viewed in isolation. Henceforth, the economic relationship would be viewed through the prism of our geopolitical differences.

INDUSTRIAL POLICY, PROTECTIONISM, AND CYBERSECURITY

In 2009, the Chinese government unveiled its "Indigenous Innovation Product Accreditation" system, which seemed to be an effort to limit access to the Chinese procurement market by forcing companies to file applications for their products to be considered for accreditation as "indigenous innovation." Many U.S. companies operating in China objected on the grounds that they were being coerced into handing over their technology as the price for market access.[7] On a visit to Washington in early 2011, as the issue was threatening to boil over, President Hu Jintao promised to retract the policy.

U.S. businesses in China confirmed that progress toward fulfilling that promise was being made. But many worried that Beijing's

> "Among the most serious sources of trade policy tension are the measures taken by both the U.S. and Chinese governments in the name of cybersecurity."

> "The U.S. government may consider Chinese information and communications technology companies intolerable risks to U.S. critical infrastructure, but the available evidence does not support that conclusion."

commitment to indigenous innovation and technological preeminence would live on through other policies. One observer put it like this: "Even if China reverses certain policies under U.S. pressure, it will remain dedicated to those goals. U.S. policy is likely to become a game of Whac-A-Mole, beating down one Chinese initiative on indigenous innovation only to see another pop up."[8]

Meanwhile, back in Washington, concerns that Chinese ICT firms could be conduits for government cyberespionage persisted after the 3Com deal was scuttled in 2008. In late 2011, the U.S. House Permanent Select Committee on Intelligence initiated a year-long investigation into whether two Chinese ICT companies presented security threats to U.S. telecommunications networks. The investigation culminated in a report recommending that U.S. firms—especially telecoms with hopes of participating in federally funded infrastructure projects—avoid contaminating their supply chains with equipment and components produced by these Chinese companies.[9]

But there is no smoking gun in the report, only innuendo. It includes generic assertions that telecommunications networks are vulnerable to malicious intrusions and that modern critical infrastructure systems are at great risk and that the sources of potential cyber threats are numerous. There is nothing to indicate that either Chinese company presents greater risk than the average Chinese, Korean, European, or American company in the supply chain. The most damning evidence in the whole report is that the Chinese ICTs were evasive or incomplete in providing answers to questions about corporate strategies that would have revealed sensitive commercial information that the companies understandably might not have wanted to share with U.S. policymakers.[10]

In 2013, six months after publication of the House Intelligence Committee report, U.S. lawmakers inserted language into the Continuing Budget Resolution making it illegal for U.S. government agencies to purchase or use Chinese ICT products.[11] Later that year, as conditions for its approval of a Japanese telecommunications company's acquisition of Sprint Nextel, CFIUS required the purchaser, Softbank, to purge Chinese ICT components from its supply chain and to obtain preapproval from Justice Department and Homeland Security officials for any new vendors it wished to bring into its supply chain.[12] Similar notification and approval conditions were imposed by the Federal Communications Commission to allow the transfer of spectrum licenses in relation to T-Mobile's acquisition of MetroPCS in 2013 and, again, by CFIUS as a condition of Altice's 2016 acquisition of Suddenlink and Cablevision.[13]

To leave no uncertainty about the U.S. government's position with respect to Chinese ICT companies, the Federal Bureau of Investigation publishes and distributes a newsletter called *Counterintelligence Strategic Partnership Intelligence Note* (SPIN), which is used, presumably, to alert businesses and the public to cybersecurity threats. Its February 2015 edition, which mostly rehashes the ambiguous findings and innuendo of the 2012 House Intelligence Committee report, is intended to scare U.S. companies away from doing business with Huawei, which is portrayed as a company beholden to the Chinese government and, consequently, a cybersecurity threat to the United States.[14]

Whereas the U.S. government may have reasons to consider Chinese ICTs intolerable risks to U.S. critical infrastructure, the available evidence does not support that conclusion. The evidence that persuaded CFIUS to oppose the 3Com acquisition was never made public, and the evidence that led the House Intelligence Committee report to strongly suggest that U.S. businesses should steer clear of certain Chinese ICTs remains classified. Thus, it may be reasonable to conclude that these Chinese companies have been targeted for economic reasons—in response, perhaps, to China's emerging and evolving "indigenous innovation" policies. After all, if the Chinese government is intent on reducing its economy's dependence on foreign technology and becoming a global innovation leader, and believes that imposing obstacles on foreign suppliers

and subsidizing domestic research and development is the way to get there, maybe the U.S. government feels compelled to respond in kind by frustrating the ambitions of China's most successful technology companies. Lending credibility to that theory, U.S. Secretary of Commerce Wilbur Ross recently suggested that the Trump administration may launch its own investigation into whether Chinese industrial policies on semiconductors present a national security threat to the United States.[15]

But just as China's reliance on subsidies and barriers and other crutches of industrial policy is shortsighted, it is a mistake for the United States to respond unilaterally by thwarting imports of ICT or any other products dependent on semiconductors. Not only does the reduction in competition deprive U.S. customers of cutting-edge technology, but it mutes incentives for domestic and other firms to be responsive to consumer needs. It squelches innovation. Moreover, U.S. semiconductor makers depend on open markets and the smooth functioning of complex global supply chains.

According to the U.S. Semiconductor Industry Association (SIA), half of the industry's production capacity is located overseas, and foreign markets account for 80 percent of its sales.[16] So, rather than succumb to the temptation to act unilaterally, which inflicts collateral damage on U.S. entities and violates U.S. commitments to the rule of law in international trade, it is better to bring matters to the WTO, where there are effective tools to compel offending governments to change course.

Meanwhile, it's worth noting that other Western governments have not been spooked away from doing business with Chinese ICTs. Huawei, for example, has national telecommunications carriers as customers for its gear in nearly all major Western economies.[17] For 10 years Huawei has had a supplier relationship with British Telecom, and the company's components are ubiquitous in the United Kingdom's telecommunications infrastructure. In response to concerns about potential breaches, Huawei and British Telecom established a testing center where components are evaluated for cybersecurity risk before they are incorporated into critical infrastructure.[18] As reported in a 2016 article in *Bloomberg View*:

> Last year an independent audit conducted by a team of U.K. cybersecurity experts found no evidence that Huawei gear posed a threat to the country's national security. A U.K. government review in 2013 also concluded the dangers were not sufficient to block Huawei's participation in the country's broadband network, and that British Telecom had taken sufficient steps to mitigate any such threat.[19]

The U.S. government's claim that Chinese ICTs present intolerable cyber risks is not shared by allied governments, who either believe the risks can be reasonably mitigated or who are less concerned than the U.S. government about the prospect of Chinese ICT companies innovating and competing at the technological fore. No other government is as affronted by China's push to achieve technological preeminence as is the U.S. government because the U.S. economy is the incumbent in that space.

It seems plausible—even likely—that U.S. protectionism in the form of blacklisting Chinese ICT firms under the guise of cybersecurity is intended to compel China to reconsider its own protectionist industrial policies. If so, however, that effort apparently has not succeeded. In fact, China seems to be doubling down on its industrial policies.

TIT FOR TAT . . . FOR TIT

In June 2015, Beijing published a report titled "Guidelines to Promote National Integrated Circuit Industry Development" and followed up with a $160 billion investment to develop the domestic semiconductor industry.[20] China, apparently, wants to catch up to the world's leading semiconductor firms and produce 70 percent of domestically consumed chips by 2030.[21] In May 2015, the Chinese government

"China's reliance on subsidies, barriers, and other crutches of industrial policy is shortsighted, and it is a mistake for the United States to respond unilaterally by thwarting imports of products dependent on semiconductors."

> "The current approach provides, at best, a false sense of cybersecurity."

published a new 10-year plan called "Made in China 2025."[22] The plan includes a road map for China's ascent up the supply chain by enhancing its innovation capacity, by increasing the value of domestic content in its manufacturing output, and by improving the competitiveness of its multinational companies.

In addition to providing massive subsidies for semiconductor research and development, China has implemented the National Security Law and the Cybersecurity Law. The National Security Law requires data and technology used in certain sectors of its economy to be "secure and controllable," an ambiguous objective that U.S. companies fear grants too much discretion to Chinese authorities and could require the firms to share source code and other proprietary information to gain market entry.[23] The new Cybersecurity Law, which took effect on June 1, requires a security review of the data and information technology equipment used in key information infrastructure. To gain approval, suppliers will have to submit their products for review to the Cyberspace Administration of China. According to a *Wall Street Journal* story, the law is "aimed at tightening state control over technology and information," and "the measures will apply to foreign companies providing hardware or services to Chinese companies in sectors including energy, transportation and finance, as well as those selling to government agencies, public services and other 'critical infrastructure'."[24]

In May 2017, citing "significant concerns" about the Cybersecurity Law, a group of 54 trade associations from 11 different countries joined together in a letter urging the Chinese government to delay its implementation.

> [W]e are deeply concerned that current and pending security-related rules will effectively erect trade barriers along national boundaries that effectively bar participation in your market and affect companies across industry sectors that rely on information technology goods and services to conduct business. China's current course risks compromising its legitimate security objectives (and may even weaken security) while burdening industry and undermining the foundation of China's relations with its commercial partners. Indeed, our organizations remain concerned that China's current approach is leading to greater separation rather than integration among our economies. Further, at a time of significant political and social change globally, we are concerned such policies may exacerbate troubling trends in markets around the world that move China away from cooperative trade and the benefits of global trade.
>
> Regrettably, a number of recently-issued draft measures would place far-reaching restrictions on the export of data, restrict participation by foreign companies in China's cloud market, and institute onerous restrictions on commercial encryption products that could adversely impact billions of dollars in cross-border trade. These drafts suggest China is continuing to move away from its bilateral commitments, international obligations, and global norms, not toward them. . . .
>
> All countries have legitimate concerns over privacy and national security, but China is the principal country addressing these concerns by requiring foreign companies to transfer their technology and to surrender their brand and operating control in order to do business.[25]

The sense of concern in the United States goes beyond the business community. In January 2017, the President's Council of Advisers on Science and Technology issued a report on U.S. semiconductor innovation, competitiveness, and security, warning that a "concerted push by China to reshape the market in its favor, using industrial policies backed by over one hundred billion dollars in government-directed funds, threatens the competitiveness of U.S. industry and the national and global benefits it brings."[26]

In reaction to Beijing's industrial policies and its seeming efforts to frustrate market access for U.S. technology companies, U.S. policymakers, advisers, and others have begun to recommend greater scrutiny of Chinese acquisitions of U.S. technology firms. In September 2016, a group of 16 members of the U.S. House of Representatives signed a letter to the Government Accountability Office (GAO) requesting that it conduct a review to "determine whether [CFIUS's] statutory and administrative authorities have effectively kept pace with the growing scope of foreign acquisitions in strategically important sectors in the U.S."[27] The letter cited concerns involving "the telecommunications, media, and agriculture sector, which raise questions of the degree to which foreign ownership—especially from Chinese companies designated as 'state champions' that often benefit from illegal subsidies designed to gain strategic access to markets like the U.S.—may pose a strategic rather than overt national security threat."[28]

In response to the letter, the GAO announced that it would conduct an assessment to determine "how the current statutory and administrative authorities of the Committee on Foreign Investment in the United States have kept pace with the growing scope of foreign acquisitions in important economic sectors in the United States."[29]

As of this writing, the GAO report has not been published. But even without the report or any changes to CFIUS's investigative scope or function, CFIUS seems to have become a major hurdle to Chinese acquisitions of U.S. technology. In 2016, several technology sector acquisitions were thwarted by CFIUS, including a bid from Tsinghua Holdings, a Chinese state-owned technology company, to purchase Micron Technologies for $23 billion; a $226 million offer for Global Communications Semiconductor from Chinese firm San'an Opto; and an effort by Fujian Grand Chip Investment Fund to purchase German-based Aixtron, a semiconductor firm with assets in the United States.

The actions and policies of the U.S. and Chinese governments over the past decade, which maintain some plausible links to cybersecurity, ultimately seem to be less concerned about securing supply chains from cyber threats than they are about protecting or creating domestic advantages in the race for 21st century technological preeminence. But playing this game of tit-for-tat protectionism serves neither cybersecurity nor the healthy evolution of technological innovation.

If cybersecurity is the objective, the current approach provides, at best, a false sense of cybersecurity. Real solutions are at hand.

VULNERABILITIES IN THE GLOBAL SUPPLY CHAIN

The imperative of protecting critical economic and national security infrastructure is the theoretical basis for cybersecurity policy. But like other areas in which governments are obligated to protect the public—from terrorism, military attacks, and other dangers—success requires proper identification of the sources and nature of the threats, as well as recognition that mitigation comes at a cost. Too narrow a threat focus is likely to provide insufficient protection, whereas the economic costs of too broad a focus are likely to be too burdensome.

Over the past 15 years, cross-border trade in ICT products has increased faster than trade overall. That trend is attributable, in part, to the reduction of tariffs and other trade and investment barriers. But the proliferation of transnational ICT production and supply chains, necessitated by robust competition and the imperative of finding lower-cost production models, has contributed, as well.[30]

The rapid dissemination of ICT has provided the world with unprecedented access to information. Virtually every sector of the U.S. and global economies, small enterprises and large, has come to rely on ICT to deliver continuously improving goods and services more efficiently. Information and communications technology products are to the modern economy what iron and coal were to the industrial revolution: building blocks essential to innovation and progress.

"In reaction to Beijing's industrial policies, U.S. policymakers, advisers, and others have begun to recommend greater scrutiny of Chinese acquisitions of U.S. technology firms."

"If the Chinese government—or any other entity—wanted to alter the software or hardware in technology products destined for U.S. critical infrastructure, the potential points of entry are ubiquitous."

But with this productivity-enhancing, living-standards-boosting technology arises a parallel potential to serve nefarious objectives. Indeed, according to Lloyds of London, cybercrime claims tens of thousands of corporate victims and costs global business up to $400 billion annually.[31] As industry experts attest, cybersecurity risk can be mitigated but not eliminated. Policies intended to eliminate risk generate enormous enforcement and opportunity costs without necessarily keeping us safer than we would be by deploying mitigation strategies on the basis of industry best practices and valid statistical methods.

All major ICT manufacturing companies produce in China or rely on inputs manufactured there. Most suppliers to global network infrastructure source their components from their Chinese facilities or through second- and third-tier Chinese suppliers.[32] In fact, there is more U.S. direct investment in the Chinese ICT industry—valued at more than $37 billion—than there is in any other segment of China's economy.[33] So, even with sales of gear produced by China's largest ICT companies essentially banned in the United States, imports from China still accounted for 60 percent of all U.S. imports of ICT products in 2016.[34] If the Chinese government—or any other entity—wanted to alter the software or hardware in ICT products destined for U.S. critical infrastructure, the potential points of entry are ubiquitous.

Meanwhile, nearly all of the semiconductors consumed in the ICT supply chain come from outside of China. In 2015, China accounted for 57 percent of the world's semiconductor consumption, but Chinese-produced chips accounted for only 9 percent of that consumption. Of the 91 percent of chips supplied to China from abroad, more than 56 percent were produced in the United States.[35]

The stretching of supply chains to include more entities operating in more countries has increased vulnerabilities to cyber malfeasance. Breaches can occur at any stage in the ICT supply chain, which means that all entities in the ICT ecosystem can present risk or be exposed to risk. That means risk-mitigation strategies must be reconsidered to reflect the fact that threats are omnipresent. But even in its call for vigilance in protecting the integrity of the supply chain, the President's Science and Technology Commission cautions about the perils of sweeping restrictions:

> Risks to the integrity of the semiconductor supply chain, while lower when critical items are designed and produced domestically or on the territories of U.S. allies, cannot be assured through domestic manufacturing and design alone and therefore ultimately need to be mitigated through other means (such as integrity standards and testing and greater system resilience), regardless of where production is located. Moreover, if the United States attempted to ensure security by simply restricting the set of producers that was allowed to sell semiconductors to U.S. firms, it would slow innovation by fragmenting markets and reducing competition.[36]

This is good advice to heed: be vigilant, but avoid overkill. If cybersecurity is the objective and a chain is as strong as its weakest link, all producers and vendors that depend on the success of a particular supply chain have stakes in securing its greatest vulnerabilities. That means that all entities in a supply chain must have reasonable assurances that what they purchase is safe, and as vendors they must be able to make the same assurances to their buyers.

As described in a National Defense University report on cybersecurity in the ICT industry:

> Throughout most of American history, threats to national security fell squarely within the purview of government agencies. Cyber threats changed that paradigm, as the U.S. government can no longer effectively secure its assets without assistance from the private sector. Nearly 85 percent of U.S. critical infrastructure is owned by the private sector, including the ICT industry.[37]

If the U.S. government is interested in cybersecurity in the ICT space and not trade protectionism, it should subject all ICT components and end-user equipment (imported and domestic) destined for application in critical infrastructure to greater scrutiny instead of blacklisting particular companies. It could do so without imposing major supply chain disruptions by developing policies that apply valid statistical methods to best business practices.

USING STATISTICS AND BEST BUSINESS PRACTICES TO ACHIEVE GREATER CYBERSECURITY

In 2013, President Barack Obama issued an executive order to U.S. agencies to take stock of critical infrastructure and develop plans to protect it from cybersecurity threats.[38] Other executive orders have followed and tens of billions of dollars have been spent by the federal government to identify threats and develop effective safeguards. The National Institute of Standards and Technology was tasked with developing a framework to help organizations manage cybersecurity risk in the nation's critical infrastructure. After collaboration among industry, academia, and various government agencies, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0" was published in 2014, and it is currently being updated.[39]

Beyond this government-led effort, the private sector has marshaled its expertise, sharing information about purchasing, processing, inventorying, and quality assurance practices to get as precise a picture as possible of the supply chain, how it operates, and where its greatest vulnerabilities lie. The management consulting firm PricewaterhouseCoopers publishes annually the results of its *Global State of Information Security Survey*, which is essentially an inventory of best business practices in cybersecurity.[40] In 2016, the East-West Institute published a buyers' guide for purchasing secure ICT products, which seems to leave no stone unturned in its identification of all the questions that must be asked, all the internal and external systems that must be in place, and all the additional safeguards that should be taken for a given enterprise to minimize threats.[41]

In other words, the private sector and government, in collaboration and operating independently, have created a reasonable set of best practices that companies in the ICT supply chain should be expected to implement. The consolidated list of best practices may include superfluous measures or procedures that are determined, ultimately, to be unnecessary. But the list should serve as the basis for creating a comprehensive set of best practices with which companies should comport in order to import, purchase, or sell ICT products in the United States. Compliance with these best practices can be demonstrated to the U.S. Department of Homeland Security (DHS), for example, not only by confirming that all of the necessary boxes have been checked, but by demonstrating that the company has implemented automated, auditable systems that are shown to be statistically reliable in identifying vulnerabilities and mitigating the associated risks.

As incentives to invest in the development of these systems and to stand ready for spot checks or more comprehensive audits, participating companies would earn something akin to a seal of approval and, ultimately, would not be held accountable if a product that breaches cybersecurity passes through their supply chain. Companies that chose not to develop secure systems would not receive a seal of approval and would be subject to heavy fines if breaches were to occur. The program details, of course, would need to be derived from culling and assessing the industry expertise and from translating these best practices into an objective compliance program.

This compliance concept isn't especially new to the U.S. government. U.S. Customs and Border Protection, an agency within DHS, has been administering a program for 25 years called "Informed Compliance," which was developed in collaboration with the private sector to incentivize accurate classification and valuation of imported and exported merchandise. It is premised on the idea that the private

"If the U.S. government is interested in cybersecurity and not trade protectionism, it should subject all components and equipment destined for critical infrastructure use to greater scrutiny instead of blacklisting particular companies."

“Many elements of the Informed Compliance program could be incorporated into a cybersecurity program without impeding trade, investment, and innovation.”

sector can be deputized to self-monitor its compliance if the appropriate balance of carrots and sticks are deployed.

The biggest carrot in the informed compliance program is that cargo isn't stopped and inspected to determine product classification and valuation (the basis for collection of import duties) by customs officials, which can be a time-consuming and costly exercise. Instead, importers can demonstrate to customs that they have developed and are using automated systems that properly classify and value their own merchandise. The major stick is that importers are subject to random audits in which they are compelled to demonstrate that their systems are working accurately. If they're not working properly, the importers are subject to very stiff fines.

Many of the elements of the Informed Compliance program could be incorporated into an efficacious, nondiscriminatory cybersecurity program on the basis of best business practices without unnecessarily impeding trade, investment, and innovation. A more comprehensive, statistically valid approach such as this would improve security by significantly broadening the scope and capabilities of mitigation efforts, while encouraging companies in the supply chain not to free ride and generate negative externalities. Rather than ban or discourage imports and investments from Chinese ICT companies on the grounds that they present high risk to U.S. critical infrastructure, new policy would increase security and reduce trade and investment discrimination, thereby encouraging innovation and economic growth.

This program is the kind that most of the world's ICT companies—and governments more interested in cybersecurity than protectionism—could get behind. The companies represented by the 54 trade associations from 11 countries that signed the letter to the Chinese government asking that it defer implementation of the Cybersecurity Law would seem to support such policies. They write the following:

> We have been and remain hopeful that the Chinese government at the highest levels will take concrete, meaningful steps to implement its past commitments to work with foreign counterparts to promote pro-competitive and non-discriminatory information communication technology (ICT) security policies. These commitments include ensuring that ICT security measures should be narrowly tailored, take into account international norms, be nondiscriminatory, and not unnecessarily impose nationality-based conditions or restrictions on the purchase, sale, or use of ICT products and services by commercial enterprises.[42]

Clearly, that passage—the last sentence, especially—could have been addressed to the U.S. government, as well.

If the United States were to adopt such a sensible system that applies statistical methods to best business practices, it could be developed with input from Chinese business and government and then codified as part of a bilateral investment treaty, trade agreement, or some other kind of agreement, superseding China's Cybersecurity Law, National Security Law, and the U.S. blacklisting of specific ICT companies.

THWARTING PROTECTIONISM

If Chinese ICT sector protectionism is a legitimate problem, the United States (and other governments representing aggrieved companies) should seek resolution by formally requesting WTO consultations with China. Certainly, the persistence of industrial policies intended to propel China into a position of global technological preeminence—WTO-forbidden subsidies on domestic industries and market access impediments on foreign competitors—seems a matter ripe for WTO resolution. However, responding as U.S. policymakers seem to have responded, by unilaterally imposing discriminatory measures on particular Chinese companies, also seems to violate U.S. WTO commitments, while depriving U.S. telecoms and end users of better prices, better technology, better choices, and the promise of greater innovation.

As compelling as the economic and moral arguments for free trade are, governments would never consider trade openness a higher priority than their obligations to protect national security. That's why, in 1947, a necessary loophole was born within the trade liberalizing provisions of the General Agreement on Tariffs and Trade (GATT). Article XXI of the GATT is known as the "National Security Exception." It permits members to impose trade restrictions for purposes of national security without obligating them to demonstrate that their rationale conforms with some agreed-upon definition of national security or national security threats.

By characterizing their respective ICT industry protectionism as security imperatives, Washington and Beijing have given themselves some wiggle room if they intend to defy their WTO commitments. China's discriminatory treatment of foreign ICT companies under its Cybersecurity or National Security laws and its attempted cultivation, through subsidies and other favors, of an indigenous semiconductor industry could very well be defended as national security imperatives. Likewise, U.S. blacklisting of Chinese ICT companies could be portrayed as measures vital to protecting U.S. national security. That is worrisome.

The key to the national security loophole not being abused is recognition by all contracting parties that prudence—not political expediency—must inform any government's decision to invoke this provision as a justification for imposing trade restrictions. Legal scholar Roger Alford characterized the provision this way:

> The security exception is an anomaly, a unique provision in international trade law that grants the Member States freedom to avoid trade rules to protect national security. In the long history of GATT and the short history of the WTO, that freedom has never been challenged seriously. Member States understand the exception to be self-judging, and presume that it will be exercised with wisdom and in good faith. Thus far, the record has been impressive. While no doubt there have been departures, the self-judging security exception has worked reasonably well. It certainly has not undermined the effective functioning of the WTO.[43]

What makes the present matter so fraught is that security-based rationales for protection have been invoked so rarely over the 70 years since the GATT was established that its discovery, use, and ultimately abuse as a rationale for protectionism could permanently cripple the WTO's capacity to reverse or rein in unilateral, rogue trade measures. Governments should be discouraged from cavalierly invoking national security as a justification for protectionism because the consequences could be adverse and long lasting.

Yet, earlier this year, President Trump launched two national security–based investigations under section 232 of the Trade Expansion Act of 1962 to determine whether U.S. reliance on foreign steel and foreign aluminum constitute threats to national security. Affirmative findings in either of those cases, if followed by U.S. trade restrictions, would open the door to China following suit on semiconductors. That outcome likely would be followed by more far-reaching U.S. measures on Chinese semiconductors and downstream ICT products.

Avoiding that outcome is so fundamentally in the interest of the health of the U.S., Chinese, and global economies that Washington and Beijing should commit to coming to the table to find a reasonable solution. If the specter of a semiconductor trade war isn't enough to get the attention of U.S. policymakers, they should bear in mind that such an outcome risks further balkanization of product standards. Fragmenting markets around competing sets of ICT product standards is something that should worry U.S. entities throughout the supply chain because, with President Trump having withdrawn the United States from the Trans-Pacific Partnership, China has been bequeathed greater latitude to influence the evolution of ICT standards. The development of new sets of product standards would put

"By characterizing their respective protectionism as security imperatives, Washington and Beijing have given themselves wiggle room if they intend to defy their World Trade Organization commitments."

> "Washington and Beijing must reach an economic solution before industrial policy begets a high technology trade war."

pressure on regional semiconductor and component manufacturers—in South Korea and Taiwan, particularly—to produce to those standards, which could reduce opportunities for U.S. collaboration and commerce in the region.

Time is running out for the Trump administration and Congress to get a handle on what's at stake and to develop and implement a plan to defuse this potentially volatile matter.

CONCLUSION

Governments have a legitimate interest and an obligation to protect critical infrastructure from cybersecurity threats. But they are also obligated to minimize the collateral damage inflicted by—or under the guise of—those efforts.

Current policies adopted by both the United States and China in the name of cybersecurity are either weighted disproportionately to the security goal or are fig leaves for protectionism. China's policies to promote technological preeminence, including the imposition of market access barriers and the bestowing of subsidies on indigenous producers, have been met with U.S. policies that blacklist China's most successful technology companies. Those actions, it seems, have been met with Chinese policies that further frustrate access of U.S. ICT companies to the Chinese market. And those policies have prompted U.S. policymakers to call for greater scrutiny—if not a moratorium—on acquisitions by Chinese companies of U.S. (and other) technology firms. Amid all of this tit for tat, each layer of which is shrouded in justification as a security imperative, critical national security and economic infrastructure remain vulnerable to attacks.

If cybersecurity is the real objective, there are far less intrusive approaches that are much more likely to keep us secure. A cybersecurity regime that weds best business practices with valid statistical methods and implements the right combination of carrots and sticks could be the right solution. Some of the elements and architecture of the U.S. Customs and Border Protection's Informed Compliance program could serve as a model for policymakers formulating a comprehensive solution to cybersecurity threats.

Finally, policymakers must bear in mind that protectionism as a response to protectionism only worsens the problems, economically and politically. It is imperative that Washington and Beijing find a way to reach a solution before industrial policy begets a high-technology trade war, which will leave the U.S., Chinese, and global economies in bad shape and the trading system in tatters.

NOTES

1. Ray Shaw, "China Tightens Tech Laws—Must be Secure and Controllable," *ITWire*, December 5, 2016, https://www.itwire.com/technology-regulation/76036-china-tightens-tech-laws-%E2%80%93-must-be-secure-and-controllable.html.

2. For a more in-depth discussion of the evolution of bilateral economic frictions and how they were handled, see Daniel Ikenson, "Into the Abyss: Is a U.S.-China Trade War Inevitable?" *Cato Institute Free Trade Bulletin* no. 69, February 6, 2017, https://www.cato.org/publications/free-trade-bulletin/abyss-us-china-trade-war-inevitable.

3. The State Council, The People's Republic of China, "The National Medium- and Long-Term Program for Science and Technology Development (2006–2020): An Outline," https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf.

4. Ibid., p. 9.

5. Wayne M. Morrison, "China-U.S. Trade Issues," Congressional Research Service Report, April 24, 2017, https://fas.org/sgp/crs/row/RL33536.pdf.

6. Created in 1975, CFIUS is an interagency committee composed of nine members, including the Secretaries of State, Treasury, Defense, Homeland Security, Commerce, and Energy, as well as the Attorney General and the U.S. Trade Representative. The committee advises the

president on the national security implications of foreign direct investment in the United States.

7. American Chamber of Commerce in the People's Republic of China, *American Business in China: 2011 White Paper* (Beijing: The American Chamber of Commerce in the People's Republic of China, April 2011), http://web.resource.amchamchina.org/cmsfile/2011/04/28/8ff8c3d4d14f50713e1be8f538b43f80.pdf.

8. Adam Segal, "China's Innovation Wall: Beijing's Push for Homegrown Technology," *Foreign Affairs*, September 28, 2010, https://www.foreignaffairs.com/articles/asia/2010-09-28/chinas-innovation-wall.

9. U.S. House of Representatives Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Committee Report, October 8, 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

10. Daniel J. Ikenson, "Huawei, ZTE, and the Slippery Slope of Excusing Protectionism on National Security Grounds," Cato Institute Blogpost, October 9, 2012, https://www.cato.org/blog/huawei-zte-slippery-slope-excusing-protectionism-national-security-grounds.

11. Daniel J. Ikenson, "Do New Cybersecurity Restrictions Amount to Regulatory Protectionism?" Cato Institute Blogpost, April 10, 2013, https://www.cato.org/blog/do-new-cybersecurity-restrictions-amount-regulatory-protectionism.

12. Alina Selyukh, "Sprint, SoftBank Agree to U.S. National Security Deal," Reuters, May 29, 2013, http://www.reuters.com/article/us-sprint-offer-idUSBRE94S0IG20130530.

13. "Applications of Deutche Telekom AG, T-Mobile USA, Inc., and MetroPCS Communications Inc.," *Memorandum Opinion and Order and Declaratory Ruling*, Federal Communications Commission, WT Docket 12-301 para. 97–99 and Appendix B, March 12, 2013, and "Applications Filed by Altice N.V. and Cablevision Systems Corporation to Transfer Control of Authorizations from Cablevision Systems Corporation to Altice N.V.," *Memorandum Opinion and Order*, Federal Communications Commission, WC Docket 15-257 para. 49, May 3, 2016; and "Applications Filed by Altice N.V. and Cequel Corporation d/b/a Suddenlink: Communications to Transfer Control of Authorizations from Suddenlink Communications to Altice N.V.," *Memorandum Opinion and Order*, Federal Communications Commission, WC Docket No. 15-135 para. 24, December 18, 2015.

14. Federal Bureau of Investigation, "Huawei: A Chinese Government Subsidized Telecommunications Company," *Counterintelligence Strategic Partner Intelligence Note (SPIN)*, February 2015, http://documents.tips/documents/u-fouo-fbi-counterintelligence-note-huawei-chinese-government-subsidized.html.

15. David Lawder, "Commerce's Ross: China's Plans Threaten U.S. Semiconductor Dominance," Reuters, May 11, 2017, http://www.reuters.com/article/us-usa-trade-ross-semiconductors-idUSKBN1872CO.

16. Ibid.

17. Michael Hiltzik, "Suspicions Keep Chinese Telecom Firm Huawei out of U.S. Market," *Los Angeles Times*, December 5, 2014, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-20141207-column.html.

18. Paul Sandle, "China's Huawei Given Clean Bill of Health by UK Security Board," Reuters, March 25, 2015, http://www.reuters.com/article/us-britain-security-huawei-tech-idUSKBN0ML20U20150325.

19. Eli Lake, "U.S. Spies Think China Wants to Read Your E-mail," *Bloomberg View*, September 13, 2016, https://www.bloomberg.com/view/articles/2016-09-13/u-s-spies-think-china-wants-to-read-your-e-mail.

20. Government of the People's Republic of China, Ministry of Industry and Information Technology, "Guidelines to Promote National Integrated Circuit Industry Development," June 24, 2015. Cited in U.S.-China Economic and Security Review Commission, "Monthly Analysis of U.S.-China Trade Data," August 5, 2015, https://www.uscc.gov/sites/default/files/Research/August%20Trade%20Bulletin%202015.pdf.

21. "Chips on Their Shoulders," *The Economist*, January 23, 2016.

22. U.S. Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protections," Chamber of Commerce Publication, 2017, https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

23. U.S.-China Business Council, "Technology Security and IT in China: Benchmarking and Best Practices," USCBC Report, July 2016, p.16, https://www.uschina.org/sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices.pdf.

24. Eva Dou, "China to Start Security Checks on Technology Companies in June," *Wall Street Journal*, May 3, 2017, https://www.wsj.com/articles/china-to-start-security-checks-on-technology-companies-in-june-1493799352.

25. Letter to the Chinese Communist Party Central Leading Group for Cyberspace Affairs, Office of the Central Leading Small Group for Cyberspace Affairs, Cyberspace Administration of China regarding implementation of China's Cybersecurity Law from 54 technology trade associations from 11 countries dated May 15, 2017, https://www.itic.org/dotAsset/7/1/71024cc0-a857-448a-8ea0-c7812855d263.pdf.

26. The White House, Office of Science and Technology Policy, "Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors," January 2017, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf.

27. Letter from U.S. Representative Robert Pittenger et al. to Gene L. Dodaro, Comptroller General, U.S. Government Accountability Office, September 15, 2016, https://pittenger.house.gov/sites/pittenger.house.gov/files/Letter%20to%20GAO%20re%20CFIUS%20Report%209.15.16.pdf.

28. Ibid.

29. Letter from Katherine Siggerud, Managing Director, Congressional Relations Government Accountability Office to U.S. Representative Robert Pittenger, September 30, 2016, https://pmcdeadline2.files.wordpress.com/2016/10/gao-letter-wm.pdf.

30. The Economist Intelligence Unit, "Politics, Cyber-Security, Trade, and the Future of ICT Supply Chains," custom research report by The Economist Intelligence Unit for Huawei Technologies, Inc., February 2014, p. 7. Supply chain diversification also is considered helpful in the protection of intellectual property, as it precludes a concentration of proprietary information with any one entity.

31. Stephen Gandel, "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year," *Fortune*, January 23, 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

32. The Economist Intelligence Unit, "Politics, Cyber-Security, Trade, and the Future of ICT Supply Chains," p. 13.

33. Thilo Hanemann, Daniel H. Rosen, and Cassie Gao, "Two-Way Street: 2017 Update: US-China Direct Investment Trends," report by Rhodium Group and the National Committee on U.S.-China Relations, May 2017, http://rhg.com/wp-content/uploads/2017/05/RHG_Two-Way-Street_2017-Update_Final_9May2017.pdf.

34. U.S. International Trade Commission, Interactive Tariff and Trade Dataweb, based on Official

U.S. Trade Statistics published by the U.S. Census Bureau, https://dataweb.usitc.gov/.

35. Wayne M. Morrison, "China-U.S. Trade Issues," Congressional Research Service Report, April 24, 2017, https://fas.org/sgp/crs/row/RL33536.pdf.

36. The White House, Office of Science and Technology Policy, "Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors," p. 5.

37. Reginald Ash III et al., "Final Report: Information and Communications Technology (ICT)," industry study, Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University, Fort McNair, Washington, DC, 2013, p. 9, http://es.ndu.edu/Portals/75/Documents/industry-study/reports/2013/es-is-report-info-technology-2013.pdf.

38. Rita Tehan, "Cybersecurity: Critical Infrastructure Authoritative Reports and Resources," Congressional Research Service Report, April 21, 2017, https://fas.org/sgp/crs/misc/R44410.pdf. "Critical infrastructure is defined in the USA PATRIOT Act (P.L. 107-56, §1016(e)) as 'systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.'"

39. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

40. See *Global State of Information Security® Survey 2017*, PricewaterhouseCoopers, London, 2017, https://www.pwc.com/gx/en/issues/cybersecurity/information-security-survey.html.

41. See *Purchasing Secure ICT Products and Services: A Buyers Guide* (New York: East-West Institute, 2016), https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf.

42. Letter to the Chinese Communist Party Central Leading Group for Cyberspace Affairs, May 15, 2017.

43. Roger P. Alford, "The Self-Judging WTO Security Exception," *Scholarly Works* 330, (January 2011), http://scholarship.law.nd.edu/law_faculty_scholarship/330.

RELATED PUBLICATIONS FROM THE CATO INSTITUTE

Into the Abyss: Is a U.S.-China Trade War Inevitable? by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 69 (February 6, 2017)

Should Free Traders Support the Trans-Pacific Partnership? An Assessment of America's Largest Preferential Trade Agreement by Daniel J. Ikenson, Simon Lester, Scott Lincicome, Daniel R. Pearson, and K. William Watson, Cato Institute Working Paper no. 39 (September 12, 2016)

Beyond the American Manufacturing Competitiveness Act: Congress Should Get More Serious About Tariff Reform by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 67 (April 26, 2016)

Trade Promotion Authority and the Trans-Pacific Partnership: What Lies Ahead? by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 61 (June 8, 2015)

The Export-Import Bank and Its Victims: Which Industries and States Bear the Brunt? by Daniel J. Ikenson, Cato Institute Policy Analysis no. 756 (September 10, 2014)

A Compromise to Advance the Trade Agenda: Purge Negotiations of Investor-State Dispute Settlement by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 57 (March 4, 2014)

The Transatlantic Trade and Investment Partnership: A Roadmap for Success by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 55 (October 14, 2013)

Reversing Worrisome Trends: How to Attract and Retain Investment in a Competitive Global Economy by Daniel J. Ikenson, Cato Institute Policy Analysis no. 735 (August 22, 2013)

Trade Policy Priority One: Averting a U.S.-China "Trade War" by Daniel J. Ikenson, Cato Institute Free Trade Bulletin no. 47 (March 5, 2012)

Economic Self-Flagellation: How U.S. Antidumping Policy Subverts the National Export Initiative by Daniel J. Ikenson, Cato Institute Trade Policy Analysis no. 46 (May 31, 2011)

Beyond Exports: A Better Case for Free Trade by Daniel J. Ikenson and Scott Lincicome, Cato Institute Free Trade Bulletin no. 43 (January 31, 2011)

Protection Made to Order: Domestic Industry's Capture and Reconfiguration of U.S. Antidumping Policy by Daniel J. Ikenson, Cato Institute Trade Policy Analysis no. 44 (December 21, 2010)

CATO INSTITUTE

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. All policy studies can be viewed online at www.cato.org. Additional printed copies of Cato Institute Policy Analysis are $6.00 each ($3.00 each for five or more). To order, please email catostore@cato.org.