Preventing Deglobalization:

An Economic and Security Argument for Free Trade and Investment in ICT

U.S. CHAMBER OF COMMERCE
International Affairs

Sponsors

U.S. CHAMBER OF COMMERCE FOUNDATION

U.S. CHAMBER OF COMMERCE CENTER FOR ADVANCED TECHNOLOGY & INNOVATION

Contributing Authors

COVINGTON

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Preventing Deglobalization:

An Economic and Security Argument for Free Trade and Investment in ICT

Table of Contents

PREVENTING DEGLOBALIZATION:

AN ECONOMIC AND SECURITY ARGUMENT FOR FREE TRADE AND INVESTMENT IN ICT

Executive Summary

While globalization of the ICT sector has been one of the most powerful drivers of global economic welfare during the past several decades, a number of factors—particularly at the policy level—are now threatening to slow or even reverse that trend.

In particular, some national governments, by intentionally or unintentionally defining security concerns in an overly broad manner, are applying intense pressure on the ICT sector to localize rather than globalize. Such pressures are manifesting in laws and regulations that expressly require the indigenization of R&D, manufacturing, and/or assembly of products or localization of data, or that otherwise effectively preference products and services that localize assembly, source code development and storage, or the storage of data. They are also manifesting through *de facto* requirements such as in:

(i) domestic technology standards and selective and often non-transparent product certification approvals;
(ii) requirements that products contain intellectual property developed domestically, supposedly to make them more secure;
(iii) discretionary subsidies and preferences in government procurement for domestic products on the purported basis that they are inherently more secure (which are particularly acute in state-driven economies);
(iv) discriminatory enforcement of competition laws to target the IP of particular foreign companies to support home-grown ICT hardware alternatives;
(v) domestic ownership and control requirements for vendors; and
(vi) various other levers of government power and pressure.

In such a globalized industry, ill-conceived security-related rules that erect trade barriers along national boundaries may, in practice, burden industry while failing to achieve legitimate policy objectives. They also may limit competition and the economic benefits of participating in a robust, global ICT industry, without providing security benefits (and potentially even weakening security).

Nevertheless, many countries—China, Russia, India, Brazil, several European nations and the EU itself, and even, in some instances, the United States (among others)—have considered, are pursuing or have adopted laws and policies that risk balkanizing the industry, without regard for their domestic—let alone the global—

welfare implications. At their core, these laws, policies and other steps favor perceived "domestic" products and services (including the domestic storage of data) over perceived "foreign" products and services, especially those sourced extraterritorially.

As a result, non-security interests—e.g., economic protectionism and political control—are becoming increasingly intermingled with real security concerns, undermining the legitimacy of essential security-oriented policies. Indeed, when governments commingle such interests, it makes it difficult to reject or refine any of their policies that are:

(i) justified on ostensible security concerns but actually based principally on industrial objectives, or

(ii) based on legitimate security interests but unnecessarily trade restrictive.

These trends raise serious economic risks to the global economy.

To be sure, certain uses or applications of ICT products and services can implicate national security interests. The defense ministry of any country, for example, might reasonably wish to procure information technology products and services from trusted firms that use robust product assurance systems. And a number of governments have security concerns with regard to their telecom networks because they are so fundamental to the operation of the information economy. This clash between efforts to capture and expand the many benefits enabled by the global ICT supply chain, and the plans by some governments to develop their own ICT industry so they can reduce reliance on foreign ICT products and services due to security concerns, is at risk of increasing over time. Thus, the challenge is to define the appropriate limits to such security-related preferences. This challenge is particularly acute in a globalized sector in which the location of the head office or registered address of a firm does not necessarily equate to where products are developed and assembled.

To motivate governments to carefully consider their security-based ICT policy requirements, this report, through rigorous economic analysis, demonstrates the negative effects which deglobalization policies can have not only on a country's ICT sector, but across its entire economy. The bulk of this paper is devoted to China not because China is exclusively engaging in behavior that is industrial policy in the guise of security enhancement, but because China is a unique case study for the effects of deglobalization policies for at least two reasons. First, China is a country that rapidly became a global hub for ICT trade in products and services following its WTO accession in 2001. Second, China is notable for the volume and expanse of the ICT regulation it is pursuing.

A modeling of the potential effects of deglobalization in China reminds us that globalization's gains are reversible—with such a reversal resulting in heavy economic consequences. Decreased openness to foreign firms and their technology results in diminished transfer of valuable know-how and an associated reduction in efficiencies and domestic innovation.

If China continues to pursue deglobalization in the ICT sector, economic modeling based on data from the Global Trade Analysis Project and defined shocks to the baseline of Chinese economic data suggests an annual reduction in China's GDP anywhere from 1.77–3.44%, or at least $200 billion based on 2015 GDP. By 2025, this would equate to a reduction in China's GDP of—at a minimum—nearly $3 trillion annually.[1]

To reverse the deepening trend of deglobalization of the ICT sector and its enormous downside economic costs, the U.S. Chamber calls upon governments, globally, to adhere to the following principles in their security-related regulation of the ICT industry:

- **Embrace a Globalized ICT Sector**. National policy approaches to the ICT sector should take into account that the ICT industry is diverse and dynamic, and based on a global supply chain.

- **Promote Market Competition**. Government policies should encourage both domestic and cross-border competition in ICT product and service markets, as this leads to the most secure solutions.

- **Promote Transparency**. The laws and regulations enacted to govern companies in pursuit of national security should be transparent. This will ensure that such laws accomplish their stated purpose.

- **Allow Commercial Procurers to Set Requirements.** While governments can set broad policies and encourage open and transparent business practices, commercial enterprises should set their own requirements for the equipment and software they purchase.

[1] Analysis by Rhodium Group. See Part II, pages 52-72.

Building on those general principles, it is important that any security-related regulatory measures adhere to the following standards:

1. **Security measures should be developed in a fully transparent manner and in partnership with the private sector**. The ICT industry has extensive experience in providing leadership and resources in every aspect of security, and can help governments ensure that their own security measures are effective and adaptive to rapidly changing circumstances. Product security is a function of how a product is made, used and maintained, not where it is made or developed—a reality that would be made clear by robust partnerships between governments and the private sector. Information exchange between the private and government sectors is vital to effective and efficient security regulation.

2. **The governmental authority promulgating the security measure should demonstrate that it is not more trade- restrictive than necessary to fulfill any legitimate security objective(s)**. The exercise should require a detailed explanation of the measure's security objective(s) and robust evaluation of feasible alternatives considered, including those proposed by the regulated community and other stakeholders, both foreign and domestic.

3. **The security measure should be consistent with the global trade requirements enshrined in the WTO agreements, including most-favored nation and national treatment principles**. Deviations from these general principles should be rare, thoroughly explained and supported, and regulations inconsistent with these principles should be proportional to the national security risk they seek to address and clearly fall under a specific national security exemption.

4. **The security measure should be fully consistent with existing globally recognized, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes**. This principle improves security because 1) it will help to ensure that procurement determinations are made on the basis of objective criteria, not solely on country of origin; 2) nationally-focused efforts may not have the benefit of the best peer review processes traditionally found in global standards bodies; 3) proven and effective security measures must be interoperable as they are deployed across the entire global digital infrastructure; and 4) it avoids the need to meet multiple, conflicting security and conformity assessment requirements in different jurisdictions, which raises enterprises' costs and consumes valuable security resources.

5. **Security requirements should be technology-neutral**. Mandates requiring certain technologies, including preferences for domestic technologies, decrease security because the country cuts itself off from

   leading-edge security solutions that could be developed anywhere in the world. Procurement agencies should require their suppliers to be transparent regarding their ownership structures, business practices, and security policies practices.

6. **Security requirements should not require forced technology transfer or review of IP such as source code**. Such IP is business proprietary information that is essential to a company' ability to innovate and remain economically competitive.

7. **Any prescriptive security requirements should be limited to those areas of the economy that are highly sensitive, such as government intelligence and military networks**. Many governments justifiably have very stringent requirements for security technologies sold into intelligence and military networks. Government procurement requirements for such systems should not extend to other government networks, government-licensed networks, or privately-run infrastructure or commercial companies which are not linked to such highly sensitive networks.

The Chamber recommends that like-minded governments voluntarily commit at the upcoming G20 meetings in Hangzhou, China to abide by the foregoing principles through a formal agreement. This non-binding agreement should establish an annual review mechanism to determine the benefits of applying the principles, whether any refinements or additions are needed, and how to encourage other governments to adopt those principles. Based on the data in this study and related information, those economies which abide by the foregoing principles will be both stronger and more secure than those that do not.

Part I: Risks of Balkanizing the ICT Industry Through Law and Regulation

A. Introduction

While many factors have contributed to the globalization of the world's economy over the last several decades, perhaps none has been as significant as the exponential advances in information and communications technology ("ICT"). Stated simply, the ICT sector has been the trigger for much of today's globalization. Technological advances and increased connectivity have made it easier to work on an integrated basis—with globally-integrated supply chains and R&D collaboration—across national borders. Investments in infrastructure have made possible greater and faster connectivity; enhancements in computing power and the proliferation of computing devices have made information and computing functionality more accessible; and the fungibility of reliable hardware and software inputs has enabled global product development. In turn, the creation of a global digital infrastructure has facilitated an unprecedented degree of information exchange and collaboration that benefits consumers globally. Each of these factors, among others, has helped to reduce costs for ICT products and services and expand competition in the ICT industry far beyond the state-of-the-art office parks of Silicon Valley.

The diffusion of technology also has contributed to broader competition within and between advanced and emerging economies, including in higher-value industries previously out of reach for lower-income countries. The result has been the emergence of truly global companies and global competition. The largest ICT firms have R&D, design, product development, manufacturing/assembly, and sales and marketing operations across the globe. The reach of the sector also has globalized and increased the productivity of other industries.[2] Utilizing ICT products and services, firms in various industry sectors are able to manage their own global supply chains, streamline and make operations more efficient, and reach broader markets.[3] As a general purpose technology, the productivity enhancing welfare impact of ICT spills over into most if not all sectors.

[2] According to the McKinsey Global Institute (MGI), global flows of all types support growth by raising productivity, and data flows amplify this effect by broadening participation and creating more efficient markets. MGI's analysis finds that over a decade, all types of flows acting together have raised world GDP by 10.1 percent over what would have resulted in a world without any cross-border flows. This added value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact. Both inflows and outflows matter for growth, as they expose economies to ideas, research, technologies, talent, and best practices from around the world. See McKinsey Global Institute, *Digital Globalization* (Feb. 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows (last visited July 18, 2016).

[3] Boston Consulting Group, *The Connected World: Greasing the Wheels of the Internet Economy*, ICANN (January, 2014), https://www.icann.org/en/system/files/files/bcg-internet-economy-27jan14-en.pdf (last visited July 15, 2016)

ICT encompasses all technology used for gathering, storing, transmitting, retrieving, and processing information. The companies that manufacture and sell ICT equipment are global, and their products are equally global. Thus, the entire code base for the software of a single ICT product, in addition to the open source components to the software, may come from multiple countries and regions, such as the United States, China, Taiwan, Israel, and Eastern Europe. The same holds true for hardware, such that a U.S. company may assemble products in China or elsewhere in Asia to distribute in the Asian market while assembling products in North America for the American market.

Such global supply chains and footprints are not the province of just a few industry titans. As a result of cloud-based services, sophisticated design and development tools that once required on-premises high performance computing power are now available to small and medium-sized businesses globally.

In this context, governments have begun evaluating the potential risks associated with global supply chains.[4] In determining the relevant national security risks, governments often look to the potential for cyberespionage or sabotage by foreign governments, facilitated through the insertion of malicious code and counterfeit assets into critical infrastructure. Governments have been alarmed by state-backed investors using investments to advance political objectives or conduct cyberespionage. A parallel concern is the rise of corporate espionage using state or political resources.

These are not unfounded concerns. It is well documented that major global companies and government agencies have repeatedly discovered malicious code and counterfeit software and hardware in their ICT networks, which could facilitate cyberattacks. A report by Verizon identified nearly 80,000 security incidents in 2015 alone, including over 2,100 confirmed data breaches.[5]

In the face of emerging cyber threats and public demands for an official response, governments have found themselves scrambling to act. But their responses have often been uneven and undermined by two key problems: (1) policymakers are utilizing blunt 20th-century policy tools — e.g., bans and localization requirements — to respond to rapidly evolving 21st-century problems, and (2) other motivations have become intermingled with security concerns, raising questions regarding the legitimacy of their efforts. In particular, while governments adopting restrictive, discriminatory laws and policies often justify them on security grounds, other motivations often co-exist with security rationales and frequently supersede them. Those other objectives most frequently include (a) an eagerness to implement industrial policies aimed at shielding domestic companies from competition to help them grow, and (b) the desire to exert greater control over the Internet, often for political reasons. There is one consistent and

[4] *See* [BOOZ ALLEN HAMILTON STUDY at 1.]

[5] Verizon, 2015 Data Breach Investigations Report, *available at* http://www.verizonenterprise.com/DBIR/2015/.

recurring theme in emerging policies globally: the use of security-related requirements to support the development of indigenous technologies.

Thus, with a mix of motivations and, in some cases, a limited understanding of the technical and economic repercussions of their actions, various countries are pursuing laws that would require "indigenization" of ICT products and services and/or discrimination against perceived non-native suppliers. The risks to individual economies and the global economy are considerable. Each government faces a fundamental policy challenge: namely, how to avoid isolating its economy from the benefits of a global ICT supply chain while also protecting national security.

Just as ICT globalization has generated large economic welfare gains, reversing that integration is likely to subtract from welfare. This is not a theoretical notion: globalization has worked in reverse before. A reverse shock that dismantled the international production chains, economic flows and interconnectedness that were the offspring of globalization would weigh heavily on the global economy and the economic welfare that accrues to citizens worldwide today. And if a departing player or players were big enough, the deleterious effects for the system as a whole would be large, and felt in GDP, in national consumption, and terms of trade.

International trade agreements and guidelines reflect important principles that support equal treatment of domestic and foreign ICT goods and services. Trade agreements also include exceptions that allow countries to take trade-restrictive measures to protect their "essential security" interests, but these exceptions can provide cover to countries seeking to discriminate against foreign-owned ICT goods and services for other domestic policy purposes. The effect of such laws and regulations may be the balkanization of the ICT industry, leading to increased costs and decreased productivity. Such self-inflicted economic harm may not be justified if the security benefits are small or non-existent. In fact, it is entirely possible that the use of less-advanced domestic ICT goods and services will create even greater security vulnerabilities. It is essential that countries make these policy choices carefully with a full understanding of the potential costs.

Part I of this paper highlights the pressures on the ICT sector and the policies being pushed in a range of countries to "nativize" ICT production and services. Part II, as described below, uses trade models to explore the increasingly less hypothetical: what would happen if policies that shield domestic suppliers led to the secession of ICT trade between China and the rest of the world? The economic models highlight that China's ICT deglobalization affects all regions negatively in GDP and domestic consuming power terms, as the benefits of specialization around comparative advantage go into reverse. More importantly for Chinese policymakers, these negative impacts of such a unilateral deglobalization scenario would be much more pronounced for China than for the other regions.

China has been perhaps the most assertive and largest actor pursuing such indigenization policies, but as noted below, it is not the only one. China's substantial use of indigenization policies is highly ironic, as China's rise and the modern era of globalization are inseparable phenomena in many respects.

B. China

For more than a decade, China has persistently and systematically sought to develop its domestic ICT industry capabilities. This effort has included the use of laws, regulations, and other policy tools—including standards such as the initiation of the WAPI domestic standard in 2004 and regulatory restrictions on foreign cryptographic products—to block or restrict the sale of foreign ICT products and services (with exceptions made when beneficial from a technology acquisition perspective), provide preferential treatment to domestic ICT industry players or compel a transfer of equity or technology as the currency for market entry.

A report for the European Union Directorate-General for Trade ("DG Trade") in 2014 shows that many discriminatory policies remain woven through laws and regulations in China and concludes that the primary goals of such discriminatory provisions are (1) to promote the development of indigenous technologies, and (2) to foster domestic champion companies that can compete globally.[6] A follow-on DG Trade report in 2015 describes how Chinese investment approval and licensing processes can be used to impose discriminatory restrictions not expressly provided in published laws and regulations.[7] The findings of both reports are highly relevant to the ICT industry.

In the following section, we examine Chinese industrial policies in the ICT sector that directly or indirectly disadvantage foreign ICT companies and technologies. With this background in mind, we then discuss the recent evolution of cybersecurity and national security policies and how the government is blending those security policies with its standing indigenous innovation agenda.

1. Chinese Industrial Policy and the ICT Sector

Top Chinese leaders have made clear their objective to develop the country's domestic ICT industry. The main reasons for their objective stem from a blend of national, political, and economic security concerns. President Xi Jinping personally leads a new Central Leading Group on Internet Security and Informatization ("Central Leading Group"). Upon its establishment in 2014, President Xi stated his view that "to

[6] Covington and Burling LLP, *Measures and Practices Restraining Foreign Investment in China*, p. 36, European Commission Directorate-General for Trade (2014), http://trade.ec.europa.eu/doclib/docs/2014/august/tradoc_152739.08.10.pdf (last visited Jan. 28, 2016).

[7] Covington and Burling LLP, *Assessing "National Treatment" as a Basis for Securing Market Access Under a Comprehensive Agreement on Investment with the PRC*, European Commission Directorate-General for Trade (2015), http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153840.pdf (last visited Jul. 14, 2016).

build cyber power, [China] must have its own technology, solid technology; rich and comprehensive information services; prosperous cyber culture; sound infrastructure; [and] high-caliber experts in Internet security and information;" adding only at the end of the list, the need for "bilateral and multilateral international dialogue and cooperation."[8] President Xi's statement makes clear the Chinese leadership's ambition to use the country's industrial policy apparatus to foster domestic ICT capabilities for security purposes, political control, and economic power.

Understanding Chinese industrial policies is critical for deciphering the degree to which protectionist instincts underlie security-related policy and regulation in China. While the days of Soviet-style five-year plans containing long lists of production targets are long gone, in their place are national five-year plans that provide directional guidance to government agencies regulating nearly every aspect of the Chinese economy. These five-year plans are supplemented by a range of other plans and policies including medium- and long-term strategic plans (known as "MLPs," the most well-known of which is the *Outline of the National Medium- and Long-Term Plan for Science and Technology Development (2006-2020),*[9] commonly referred to as the "S&T MLP", as well as industry-specific plans and policies, and local or other geographically-delineated industrial plans and policies.

a) *"Informatizing" China's Economy and Society: Early Efforts*

Though the development of domestic ICT is increasingly a key feature of Chinese industrial policymaking, the focus on ICT in industrial policy and planning can be traced back at least several decades. In 1997, the government published its *9th Five-Year Plan and 2010 Vision for National Informatization*, calling for the "informatization" of the Chinese economy, society, and governance.[10] The plan promoted the application of modern information technology and information resources in a variety of fields including agriculture, industry, national defense, and science and technology research, all under the planning and coordination of the state.[11] Among other things, the plan called for the active development of telecommunications networks, radio and television networks, and computer networks.[12] It declared the nation's intention of turning the information industry into a "pillar industry" and a new growth point for the national economy to achieve robustness and scale by 2010.[13]

---

[8] *President Xi Jinping's Views on the Internet*, China Daily (Dec. 14, 2015, 09:29AM), http://usa.chinadaily.com.cn/china/2015-12/14/content_22706983.htm (last visited Feb. 17, 2016).

[9] 国家中长期科学和技术发展规划纲要(2006-2020年) [Outline of the National Medium- and Long-Term Plan for Science and Technology Development (2006-2020)] ("**S&T MLP**") (SC, *effective* Dec. 26, 2005).

[10] *National Informatization*, People's Education Press (Nov. 15, 2002), http://www.pep.com.cn/xxjs/jszj/jyxxh/201008/t20100827_785318.htm (last visited Mar. 1, 2016).

[11] *Id.*

[12] *Id.*

[13] *Id.*

In the last fifteen years, policies for advancing the informatization of Chinese society have become more systematic elements of China's national economic strategy. These policies have been manifested in China's five-year economic and social development plans—the most important industrial policy documents in China—and related industrial policy and planning documents. For example, to supplement the country's 10th Five-Year Plan, a National Informatization Leading Group headed by then Premier Zhu Rongji issued in 2002 the *Specific Plan for Informatization Priorities Under the 10th Five-Year Plan for National Economic and Social Development*.[14] Industry-specific plans, such as the 2009 *Plan on Adjusting and Revitalizing the Electronic Information Industry*, further developed the growing web of ICT-related industrial policies.[15]

An MLP on the topic of informatization, issued by the State Council in 2006, set out informatization-related goals for the 15-year period from 2006 to 2020.[16] This MLP, which remains in effect, emphasizes informatization in nine important aspects of economics and society: (1) promoting the informatization of the [private] economy, (2) promoting electronic government administration, (3) building advanced Internet culture, (4) promoting the informatization of society (including education and scientific research, healthcare, employment and welfare), (5) perfecting information infrastructure (e.g., broadband access), (6) strengthening the use and exploitation of information resources, (7) improving the competitiveness of the [Chinese] information industry, (8) building a national system for safeguarding information security, and (9) improving the ability of citizens to utilize information technology and train informatized human talent.[17] The MLP's eighth objective indicates that Chinese government officials now consider safeguarding information security as a key aspect of preserving national security.

b) *Bolstering Domestic ICT Capabilities in the 12th Five-Year Period and Beyond*

China's leaders, cognizant of the explosive development, global dissemination, and inherent economic value of ICT technology, and its immense power with respect to controlling information—as well as its importance to fulfilling China's broader

[14] *"十五"期间我国信息化发展概况 [China's Informatization Development During the 10th Five-Year Period]*, China.com.cn (Jun. 24, 2006), http://www.china.com.cn/chinese/PI-c/1254081.htm (last visited Mar. 1, 2016).

[15] 电子信息产业调整和振兴规划 [Planning on Adjusting and Revitalizing the Electronic Information Industry] (General Office of the State Council, *effective* 2009).

[16] 2006－2020年国家信息化发展战略 [National Informatization Development Strategy from 2006 to 2020] (General Office of the State Council, *effective* Mar. 19, 2006).

[17] *Id.*, Art. 4.

geopolitical ambitions[18]—have accelerated their efforts to ensure that the country's industrial policies help Chinese industry get a leg up on the competition. A growing reliance on industrial policymaking may in part be attributed to the view amongst many in the Chinese government that industrial policy support was a factor in the partial successes of the Chinese integrated circuits ("IC") software industries in the 2000s, a period referred to by some as the "Golden Ten Years"—see, e.g., the State Council's 2000 Circular on Policies for the Development of the Software and Integrated Circuits Industries.[19] More recently, this policy support for the software and IC industries has been expanded tremendously, as discussed in more detail below.

(1) 12th Five-Year Plan & Cross-Cutting Themes

The Chinese leadership's ambitions for developing domestic ICT capabilities now extend far beyond the software and semiconductor industries. The country's overarching 12th Five-Year Plan (for the period 2011-2015)[20] lists a "new-generation information technology industry" as one of the seven strategic and emerging industries the country's economic planners are most eager to develop.[21] The 12th Five-Year Plan names as ICT industry priorities new-generation mobile communications, next-generation Internet, three-network convergence (i.e., convergence of telecommunications, radio and television, and Internet networks), Internet of Things, cloud computing, integrated circuits, new display technologies (e.g., TFT-LCD, PDP, OLED, electronic paper, 3D displays, and laser displays), high-end software, high-end servers, and information services.[22]

In 2012, the State Council followed up the National Strategic Emerging Industries Plan ("SEI Plan")[23] providing more detailed policy prescriptions for the development during that same five-year period of the seven strategic and emerging industries listed in the 12th Five-Year Plan. The SEI Plan describes the principal

---

[18] 让工程科技造福人类、创造未来——习近平在2014年国际工程科技大会上的主旨演讲 [Let Engineering and Science and Technology Benefit Mankind and Create the Future – Xi Jinping's Keynote Speech at the International Conference on Engineering and Science and Technology 2014] (June 3, 2014)
Source: http://cpc.people.com.cn/n/2014/0603/c64094-25097532.html.

[19] Robert D. Atkinson, *ICT Innovation Policy in China: A Review*, p.2, The Information Technology & Innovation Foundation (Jul. 2014), http://www2.itif.org/2014-china-ict.pdf (last visited Mar. 1, 2016). 国务院关于印发鼓励软件产业和集成电路产业发展若干政策的通知 [Notice of the State Council on Issuing Several Policies on Encouraging the Development of the Software and Integrated Circuit Industries] (State Council, *effective* Jun. 24, 2000).

[20] 中华人民共和国国民经济和社会发展第十二个五年规划纲要 [Outline of the Twelfth Five-year Plan for National Economic and Social Development] (National People's Congress, *effective* Mar. 14, 2011) ("**12th Five-Year Plan**").

[21] *Id.*, Sec. 1, Ch. 10.

[22] *Id.*

[23] 国务院关于印发"十二五"国家战略性新兴产业发展规划的通知 [Notice of the State Council on Issuing the 12th Five-Year Plan for the Development of the National Strategic Emerging Industries] (State Council, *effective* Jul. 9, 2012) ("**SEI Plan**").

objectives for developing a new-generation information technology industry as follows:[24]

> *[For the purpose of] strengthening international competitiveness and transforming the information industry from [just] a large industry into a strong industry, by seizing the opportunity of information technology upgrading and integrated development of industries, we should [1] accelerate the building of a broadband, converged, secure, and ubiquitous next-generation information network; [2] create breakthrough new-generation information technologies in terms of super high-speed fiber optic and wireless communications, Internet of Things, cloud computing, digital virtual reality, advanced semiconductors, and new displays, etc.; [3] push forward the interaction and integration of information technology innovation, expansion of emerging applications, and network building; [4] innovate the model of industrial organization, [5] raise the security level of new types of equipment, and [6] foster emerging services. The new-generation information technology industry shall have an average annual sales growth rate of 20% or higher during the 12th five-year period.*

Most of the objectives in the SEI Plan are economy-oriented, except for the fifth objective listed above that focuses on equipment security. The SEI Plan contains a broad range of provisions geared towards fostering domestic ICT capabilities that distort market incentives and discriminate against foreign and foreign-invested companies and technologies. For example:

> Prioritizing Indigenous Innovation. The SEI Plan sets out as principles "adhering to indigenous innovation; and enhancing original innovation, integrated innovation, and re-innovation after introduction, digestion, and absorption [of] foreign technologies."[25] These principles became centerpieces of China's national economic strategy under the S&T MLP, which remains in effect today. Under the heading of increasing innovation capabilities, the SEI Plan calls for the country's ICT industry and other strategic and emerging industries to "control a batch of critical core technologies with leading positions, and establish a batch of internationally advanced innovation platforms."[26] Building on the successes of the previous decade, it promotes "enhancing the indigenous development abilities of high-performance integrated circuit products."[27] And it sets as a goal for the period greatly increasing the "ability of systems software, utility software, and security software with indigenous intellectual property rights" to serve as a

[24] *Id.*, Art. 3.2.

[25] *Id.*, Art. 2.2.

[26] *Id.*, Art. 2.3.

[27] *Id.*, Art. 3.2.2.

driving force for the industry.[28] Note the blending of security and indigenous elements in the SEI Plan (i.e., "control" of core technologies and "security software with indigenous intellectual property rights").

Promoting Domestic Champions. The SEI Plan also calls for "forming a batch of backbone enterprises that have relatively strong indigenous innovation abilities and a technical leading role in terms of technology."[29] It further describes strategies for fostering domestic champion companies, stating that to cultivate backbone enterprises, policy should "implement an innovative enterprise support plan" and "encourage M&A, reorganizations, and alliances between powerful upstream and downstream enterprises."[30] By 2020, the SEI Plan seeks to "significantly enhance the international influence of operating systems and utility software tools of indigenous brands and the international competitiveness of backbone enterprises…[with] a number of software and information services enterprises ranked at the top of the international market."[31]

The emphasis on indigenous innovation and the fostering of domestic champions is complemented by an international strategy that includes the following elements:

Encouraging Technology Acquisition, Participation in Standards-Setting, and Moving Up the Value Chain. The SEI Plan promotes continued support for "the introduction of advanced critical core technologies and equipment"[32] and encourages "domestic enterprises and R&D institutions to establish overseas R&D facilities"[33] ostensibly for the purpose of drawing in more foreign technologies for use by domestic players. This provision goes on to encourage domestic enterprises to "participate in the formulation of international standards."[34] In another provision, the SEI Plan supports "the popularization and application in other countries of technical standards with indigenous intellectual property rights."[35] Ultimately, China wants to move its enterprises up the global value chain. Under the heading "Steadily advance the status of [Chinese enterprises] in the international division of work," the SEI Plan calls for "cultivating a batch of internationalized enterprises that control critical core technologies, own indigenous brands, and have an advanced status in the

[28] *Id.*, Art. 3.2.3.

[29] *Id.*, Art. 2.3.

[30] *Id.*, Art. 3.2.2.

[31] *Id.*, Art. 3.2.3.

[32] *Id.*, Art. 5.3.2.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[international] division of work and cooperation; greatly increasing the international market share of technologies, products, and services with indigenous intellectual property rights; and becoming important global R&D manufacturing bases in certain sectors."[36]

(2) ICT-Specific Industrial Policies

Under the high-level framework of the 12th Five-Year Plan and the SEI Plan, government agencies involved with the development of the ICT sector have issued a wide range of industrial policy documents presenting more detailed policy prescriptions for the development of the ICT sector and component industries. The agencies most directly involved with regulating the ICT sector are the Ministry of Industry and Information Technology ("MIIT"), the National Development and Reform Commission ("NDRC"), the Ministry of Science and Technology ("MOST"), and increasingly the Cyberspace Administration of China ("CAC"). The government agencies report to the State Council and the CAC reports to the Office of the Central Leading Group for Cyberspace Affairs, and all issue industrial policies related to the development of the ICT sector. The State Council itself has issued a range of regulations and policies specifically related to informatization and the development of the ICT sector. For a table listing examples of those issued by the State Council during the 12th and 13th five-year period see Appendix 1.

Case Study I: China's Semiconductor Industry

Cross-cutting themes identified in the SEI Plan above appear throughout Chinese regulations and policies. A case in point is the *Outline for Promoting the Development of the Nation's Integrated Circuit Industry* ("2014 IC Policy"),[37] issued by the State Council in 2014 as a basis for the renewed (and greatly magnified) effort to make China a semiconductor superpower.

The 2014 IC Policy calls for indigenous innovation, explaining that "heavy reliance on the importation of IC products makes it difficult to strongly support the formation of core competitiveness in national industries and the protection of information security."[38] It sets out a principal objective of cultivating domestic champion companies, with the goal that "by 2030, key links in the IC industry chain reach

[36] *Id.*, Art. 2.3.

[37] 国家集成电路产业发展推进纲要 [The Outline for Promoting the Development of the Nation's Integrated Circuit Industry] (State Council, *effective* Jun. 2014). ("**2014 IC Policy**")

[38] *Id.*, Art. 1.

internationally advanced levels, [and] a batch of [Chinese] enterprises become first-tier companies in the international market."[39] To this end, the document encourages "the raising of companies' capabilities, and M&A and [other forms of] reorganization."[40] This document further promotes highly prescriptive revenue targets and technology milestones, foreign technology acquisition through the establishment of R&D, production, and operations centers by international IC companies in mainland China,[41] and includes language that, again, calls for Chinese IC companies to move up the value chain ("move up the ladder and improve influence in the global industrial competition structure").[42] The policy is also justified by the need to reduce a large trade deficit in this sector, without regard to China's extraordinary and persistent overall trade surpluses.

Notably, under the 2014 IC Policy, the Chinese government has committed to marshaling US$100-150 billion in public and private funds toward the further development of the country's semiconductor industry, a figure which far exceeds the less than $1 billion spent by the government during the last major spending spree in the sector in the late 1990s.[43] Much of this funding is being used to acquire foreign technologies that China cannot develop on its own. Former MIIT officials manage some of the funds according to government policy.

(3) ICT Policies in Non-ICT Sectors and at the Provincial and Local Levels

Consistent with the government's goal of "informatizing" all aspects of the Chinese economy and society, government agencies responsible for regulating non-ICT industry sectors have issued industrial policies and regulations on the development and application of ICT to non-ICT industry sectors such as education, agriculture, and manufacturing. These policies set forth goals for the development of their respective industry sectors, often discriminating (explicitly or implicitly) against foreign players.

[39] *Id.*, Art. 2.3.

[40] *Id.*, Art. 4.2.

[41] *Id.*, Art. 4.8.

[42] *Id.*, Art. 2.2.

[43] *Chips on Their Shoulders*, The Economist (Jan. 23, 2016), http://www.economist.com/news/business/21688871-china-wants-become-superpower-semiconductors-and-plans-spend-colossal-sums (last visited Mar. 1, 2016).

For a table listing the highest-level industrial policy documents issued by central-level government agencies regulating each of ten sectors as examples, please see Appendix 2.[44]

Further, industrial policymaking is not limited to central level government agencies. Local governments, often keen to serve as the host of up-and-coming technologies, issue their own industrial policies, generally within the framework of industrial policies issued by central-level authorities.

By way of example, the table in Appendix 3 shows ICT-related industrial policies and regulations issued by local governments in the country's four metropolitan areas under direct central jurisdiction (Beijing, Shanghai, Tianjin, and Chongqing), Guangdong Province, and the municipalities of Shenzhen and Xiamen. These documents contain industrial policy language related to a range of ICT-related industries including software, integrated circuits, the Internet of Things, big data, and cloud computing.

c) *Implementing Industrial Policy in the ICT Sector through the 13th Five-Year Plan and Informatization Policies*

(1) 13th Five-Year Plan

The Chinese government has long used a wide range of legal and policy tools to carry out its industrial policy goals. These tools include subsidies and other forms of financial support for Chinese firms, restrictions and prohibitions on foreign investment (in terms of joint venture requirements, equity caps, sectoral limitations, regulatory and licensing hurdles, and so on), technology transfer requirements or inducements for foreign firms, discrimination against foreign firms in commercial and government procurement, discrimination against and targeting of foreign intellectual property, and the use of patent and anti-trust regimes to target foreign companies. The legal system also can sometimes be used to carry out the government's priorities.

The Chinese government has made clear its intent to continue to utilize its industrial policy apparatus to promote the development of the domestic ICT sector through the 13th Five-Year Plan,[45] which is generally oriented towards stronger control by the Chinese government over network-related issues, and calls for Chinese participation in the formulation of international network rules and in the protection of global cybersecurity. The 13th Five-Year Plan, covering the period 2016-2020 and published on March 17, 2016, contains a number of provisions related to the development of China's ICT sector, with a full section consisting of four chapters

[44] The contents of the table do not represent a comprehensive list of industrial policies and are provided for illustrative purposes only.

[45] 中华人民共和国国民经济和社会发展第十三个五年规划纲要 [Outline of the Thirteenth Five-year Plan for National Economic and Social Development] (National People's Congress, *effective* Mar. 16, 2016) ("**13th Five-Year Plan**").

focused on the "expansion of network economic space."[46] These chapters cover a number of topics including the construction of a new-generation information structure; development of the Internet and its integration with other industries; advancements in big data; and enhanced information security and cyberspace governance.

In addition, and in line with the 12th Five-Year Plan, the 13th Five-Year Plan continues to list the new-generation information technology industry as a strategic and emerging industry, and encourages innovation in the industry. It encourages the cultivation of an integrated circuits industrial system and the fostering of domestic industrial capabilities in technologies including artificial intelligence, smart hardware, new displays, intelligent mobile terminals, fifth-generation mobile communications, advanced sensors, and wearable devices.[47]

The 13th Five-Year Plan continues to emphasize indigenous innovation and the promotion of domestic champion companies. It calls for innovation to be "placed at the core of the country's overall development,"[48] demand the "enhancement of original innovation, integrated innovation, and re-innovation after the introduction, digestion, and absorption [of foreign technologies],"[49] and advocate "cultivating a batch of innovative enterprises that are industry leaders and are internationally competitive."[50]

The more granular 13th Five-Year Plan for Science and Technology Innovation ("S&T Plan"), issued on August 8, 2016, emphasizes identical themes.[51] It was the first sub-plan under the 13th Five-Year Plan to be issued and provides the blueprint for technical innovation over the 2016-2020 period. The S&T Plan calls for "strengthening indigenous innovation capabilities" and fully realizing the effectiveness of science and technology innovation in safeguarding national security.[52] It calls for "capturing critical and core technology" in a variety of industries—including integrated circuits, new medicines, and genetic medication—to "put effort into resolving restrictions to economic and social development and major science and technology problems concerning national security."[53] More specifically, the S&T Plan calls for "building the foundation for forming indigenous innovation capabilities for core electronic components, high-end general chips, and basic software products, [and] reversing China's passive approach to

[46] *Id.*, Chs. 25, 26, 27 and 28.

[47] *Id.*, Ch. 23.

[48] *Id.*, Ch. 4.

[49] *Id.*, Ch. 6.

[50] *Id.*, Ch. 6(2).

[51] "十三五" 国家科技创新规划 [13th Five-Year Plan for Science and Technology Innovation] (State Council, effective July 28, 2016) ("**The S&T Plan**")

[52] *Id.*, 1.2.1 and 1.2.2

[53] *Id.*, 2.4.1

[ensuring] secure and controllable and indigenous protections for basic information products."[54]

Beijing City 13th Five-Year Plan for Software and Information Services Industry Development

In response to guidance from the central government in the 13th Five-Year Plan, provincial- and municipal-level governments are now issuing their own plans that prioritize indigenous innovation under the guise of achieving national security. For example, the Beijing City 13th Five-Year Plan for Software and Information Services Industry Development ("The Beijing Plan), issued August 11, 2016, includes "Indigenous and Controllable Technical Innovation" as one of its "Important Action Points."[55] In addition to its focus on increasing indigenous innovation capabilities and indigenous intellectual property rights, the Beijing Plan calls on "the Party, government, military, and telecommunications, financial services, and over important industries, to gradually move from the scalable application of single-product breakthroughs to total system substitution."[56]

With its own subheading on indigenous and controllable technical innovation, the Beijing Plan arguably contains some of the most explicit language prioritizing indigenous innovation to achieve national security as well as a clear articulation of the Party's goal to achieve full deglobalization of commercial network systems in financial services and other areas.

In multiple speeches given in April 2016, President Xi Jinping reiterated the importance of China's pursuit of an indigenous innovation strategy and sought to play down the tension between indigenous innovation and openness to foreign technologies. In remarks on April 26, 2016 at the Advanced Technology Institute at the University of Science and Technology of China, President Xi called for the country to "press ahead with indigenous innovation [in an environment] of openness."[57] Seven days before that talk, at the Working Symposium on Cybersecurity and Informatization held on April 19, he gave a groundbreaking and detailed speech saying that it is critical that China pursue indigenous innovation for core technologies, which he defined as "fundamental or

[54] Id., 2.4.1 Special Column 2

[55] 北京市"十三五"时期软件和信息服务业发展规划 [Beijing City "13th Five-Year Plan" for Software and Information Services Industry Development](Beijing Municipal Commission of Economy and Informatization, August 2016) Art. 4.4 ("**The Beijing Plan**")

[56] *Id.*

[57] *习近平考察中科大：要在开放中推进自主创新 [XiJinping Inspected USTC: We Need to Press Ahead with Indigenous Innovation in an Open Environment]*, Xinhuanet.com (Apr. 27, 2016, 00:45 AM), http://news.xinhuanet.com/politics/2016-04/27/c_1118744858.htm.

commonly used technologies," "asymmetric or 'silver bullet' technologies," and "cutting-edge or groundbreaking technologies": "If the core components and parts largely depend on foreign countries, the lifeline of the entire supply chain is at the hands of others, which is like building a house on others' walls."[58]

At the same time, China's leader clarified that indigenous innovation is not contradictory to openness and does not mean closing the country's doors to foreign technologies.[59] President Xi argued that China must stick to "open innovation" and encourage Chinese ICT companies to go abroad and improve the level of exchange and cooperation with international science and technology communities.[60] "The problem," he explained, is to "clarify what kinds of technology can be brought into China and are 'secure and controllable'; what kinds of technology can be brought into China and be reverse engineered; what kinds of technology can China jointly develop with others; and what kinds of technology must China develop fully indigenously."[61] President Xi's solution is for China to develop cyber talent, double down on R&D of core ICT technologies, and make use of all available resources to develop technology on its own, acquiring expertise from abroad when indigenous development is not possible. He called for China's companies, government agencies, and academic institutions to "form a special forces assault team of elite R&D alliances" to not only promote indigenous development, but also to fully utilize the technologies they create and fund.[62]

On May 4, MIIT published some "initial thoughts on implementing the spirit of the April speech made by President Xi."[63] The article highlights the need to (i) understand the criticality of China owning core technologies "in the event external situations change dramatically"; (ii) combine production and application to integrate innovation, industrial, and value chains; (iii) properly manage the relationship between ICT development and security, and between opening up and indigenization; and (iv) promote the use of safe and reliable ICT products in finance, energy, electricity, communications, transportation, and other sectors. MIIT plans to publish an updated industrial policy plan for the ICT sector by end of this year.

---

[58] *习近平：在网络安全和信息化工作座谈会上的讲话 [XiJinping: Speech at Working Symposium on Cybersecurity and Informatization]*, People.com.cn (Apr. 26, 2016, 07:53 AM), http://cpc.people.com.cn/n1/2016/0426/c64094-28303771.html.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *See* China President Xi Jinping, remarks to the Cybersecurity and Information Work Conference (April 19, 2016); available at http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm (available in Chinese only).

[63] *See* http://www.miit.gov.cn/n1146285/n1146347/n1147601/n1147604/c4763061/content.html

While President Xi claimed that China "refuses no new technology," the country's emphasis on indigenous innovation begs the question of whether new technologies will start to refuse China. Such is the risk as indigenous innovation policies become increasingly intertwined with security rationales—or whether Chinese policies will reduce foreign companies' incentives to research and conduct the sorts of commercial activities that contribute to China's technological development. The review below of China's recent security-related actions demonstrates China's increased utilization of alleged security concerns to further develop and promote domestic technologies and champions. In fact, it is often difficult to separate attempts to regulate the ICT industry in ways that favor fostering domestic industry from policies purportedly enacted to strengthen security.

(2) National Informatization Strategic Development Outline

In another example of China's ongoing commitment to utilize its industrial policy apparatus to promote the development of the domestic ICT sector, the General Office of the Central Committee of the Communist Party and the State Council on July 27, 2016 issued the "National Informatization Development Strategy Outline" ("the Outline").[64] Comprehensive in scope, the Outline touches upon a variety of issues, including critical information infrastructure, media, intellectual property, standards, data and privacy.[65] The Outline builds on and readjusts aspects of the 2006-2020 MLP on Informatization[66] to standardize and steer China's national informatization and information technology development over the next 10 years.

In addition to calling for renewed and accelerated efforts to informatize China's economy and society, the Outline highlights indigenous innovation and national security concerns as the principal rationales for China's informatization drive.

> **Indigenous Innovation**: The Outline mandates that by 2025, China must "fundamentally change the situation of relying on others for core and critical technology, and form a secure and controllable information technology industry system."[67] First on China's list of informatization development challenges is a "reliance on others for core technology and equipment." For it to transition from a technology follower to a technology leader, the Outline calls on China "to grab indigenous innovation…build a secure and controllable information technology

[64]国家信息化发展战略纲要 [National Informatization Development Strategy Outline] (China Communist Party Central Committee and State Council, July 27, 2016) ("**the Outline**")

[65] *Id.*

[66] 2006－2020年国家信息化发展战略 [National Informatization Development Strategy from 2006 to 2020] (General Office of the State Council, *effective* Mar. 19, 2006).

[67]国家信息化发展战略纲要 [National Informatization Development Strategy Outline] (China Communist Party Central Committee and State Council, July 27, 2016), Art. 2.2

system, [and] cultivate an industry ecosystem possessing international competitiveness."[68]

Security: The Outline links China's long-term peace and prosperity to informatization. Security is emphasized throughout the Outline, which includes at least three separate and specific calls to construct a secure and controllable information technology or core technology system. The Outline states that "whoever occupies the high ground in information and whoever is able to grasp the opportunity, will win the advantage, security, and the future."[69]

2. Chinese Cybersecurity and National Security

The Chinese government's systematic efforts to foster ICT industries in the country have been further bolstered through policy efforts focused on cybersecurity and national security. Cybersecurity concerns are not new, and they are not unfounded; certainly, all countries face cyber-based threats to their government and commercial systems. However, China, more than other countries, has aggressively reacted to such concerns in part by adopting rules favoring the domestic ICT industry that the government has promoted over the past several decades.

For instance, China promulgated the *Information Security Multi-Level Protection Administrative Measures*[70] in 2007. These measures classify Chinese information systems based on their impact on national security, social order, and economic interests.[71] IT security products for information systems considered to have a critical impact on these interests are essentially barred from the market if they contain foreign-owned intellectual property.[72] Specifically, these measures require that IT security products used in information systems at or above Level 3 on a 5-point scale must be developed and produced by pure domestic companies (i.e., Chinese-registered companies invested by Chinese individuals or companies) and the intellectual property related to the core technology and critical components of such products must be indigenous. Information systems pertaining to Chinese banks and telecommunications companies, among others, are rated at Level 3.[73]

---

[68] *Id.*, Art. 2.2

[69] *Id.*, Art. 1.1

[70] 信息安全等级保护管理办法 [Information Security Multi-Level Protection Administrative Measures] (Ministry of Public Security, State Secrets Bureau, State Encryption Administration, State Council Informatization Working Office (dissolved), *effective* Jun. 22, 2007).

[71] *Id.*, Art. 6.

[72] *Id.*, Art. 21.

[73] James McGregor, *supra, at* p. 31.

Policy language supporting the development of domestic ICT capabilities has been increasingly intermingled with cybersecurity-related language, sometimes making these two priorities difficult to distinguish. In 2015, several high-level policy documents—including *Made in China 2025*,[74] the *Guiding Opinions on Actively Advancing the 'Internet+' Action*,[75] and the *Outline for Actions to Promote the Development of Big Data*,[76] which, at least in part, aim to incorporate network technologies into key economic, social, and political spheres—all emphasized network security alongside provisions aimed at the indigenous development of core technologies and equipment as well as the cultivation of domestic champion companies. In his remarks upon the establishment of the Central Leading Group for Internet Security and Informatization, President Xi explicitly linked network security prerogatives and domestic ICT industry priorities, declaring that informatization and protecting cybersecurity are "two wings of a bird, and two wheels of an engine."[77] The discussion in the text box entitled "The 'Secure and Controllable' Standard in China" further illustrates this point.

The "Secure and Controllable" Standard in China: Banking and Insurance Regulations

The increased scrutiny of foreign ICT companies in China started well before the issuance of the *National Security Law* and the draft *Cybersecurity Law*. In May 2014, the official website of CAC announced that China would soon develop a broad and loosely worded policy framework, the Cybersecurity Review Regime, under which technologies that were determined to pose a national security risk could be banned from China.[78]

[74] 中国制造2025 [Made in China 2025] (State Council, *effective* May. 8, 2015).

国务院关于印发《中国制造2025》的通知

[75] 国务院关于积极推进"互联网＋"行动的指导意见 [Guiding Opinions of the State Council on Actively Advancing "Internet+" Action] (State Council, *effective* Jul. 1, 2015).

[76] 促进大数据发展行动纲要 [Outline for Action to Promote the Development of Big Data] (State Council, *effective* Aug. 31, 2015).

[77] *Xi Heads Internet Security Group*, Xinhuanet.com (Feb. 27, 2014, 09:54:33 PM), http://news.xinhuanet.com/english/china/2014-02/27/c_133148418.htm (last visited Mar. 1, 2016).

[78] *国家网信办：我国将出台网络安全审查制度 [CAC: China to Launch a Cybersecurity Review Regime]*, Cac.gov.cn (May 22, 2014, 12:41:03 PM), http://www.cac.gov.cn/2014-05/22/c_126534290.htm (last visited Jun. 15, 2016).

In late 2014 and early 2015, as part of that regime, the China Banking and Regulatory Commission ("CBRC") issued cybersecurity guidelines and related circulars (collectively, "Guidelines").[79] While the Guidelines were withdrawn and suspended by the Chinese government in response to concerns from foreign governments and business organizations, the China Insurance Regulatory Commission ("CIRC") issued in October 2015, and further amended in April 2016, the draft "Provisions on Insurance System Informatization" (the "Provisions") that contained similar provisions to the Guidelines and would require information technology in that industry to be "secure and controllable."[80] The "secure and controllable" phrase also now appears in regulations governing industries ranging from credit reporting, e-commerce, telecommunications, and healthcare.[81]

The Guidelines would have required banks operating in China to ensure that 75% of all technology they use is "secure and controllable" by 2019.[82]

---

[79] 中国银行业监督管理委员会关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见 [Guiding Opinions of the China Banking Regulatory Commission on Strengthening the Banking Network Security and Information Technology Construction through the Application of Secure and Controllable Information Technologies] (China Banking Regulatory Commission, *effective* Sep. 3, 2014); 中国银监会办公厅、工业和信息化部办公厅关于印发银行业应用安全可控信息技术推进指南（2014-2015年度）的通知 [Notice of the China Banking Regulatory Commission and the Ministry of Industry and Information Technology on Issuing the Promotion Guidelines for the Application of Secure and Controllable Information Technologies in the Banking Sector (2014 – 2015)] (China Banking Regulatory Commission and the Ministry of Industry and Information Technology, *effective* Dec. 26, 2015); 中国银监会关于《银行业应用安全可控信息技术推进指南(2014－2015年度)》(银监办发(2014)317号)的相关说明 [Explanations of the China Banking Regulatory Commission Related to the Promotion Guidelines for the Application of Secure and Controllable Information Technologies in the Banking Sector (2014 – 2015) (Yin Jian Fa No. (2014) 317)] (China Banking Regulatory Commission, *effective* Feb. 12, 2015).

[80] 保险机构信息化监管规定(征求意见稿) [Regulation on Supervision and Administration of Informatization of Insurance Organization (Draft for Comments)], Art. 53 (China Insurance Regulatory Commission, Apr. 19, 2016), https://members.wto.org/crnattachments/2016/TBT/CHN/16_1530_00_x.pdf (last visited Jun. 26, 2016). This draft regulation was first published on CIRC's website for comments on October 9, 2015, and was then updated on April 19, 2016 in the form of a filing to the WTO's Committee on Technical Barriers to Trade. The April 2016 draft removed all references to indigenous IPRs and R&D, as well as the use of domestically developed encryption technologies; however, a lot of other controversial provisions still survived, such as the applicability of MLPS, reference to other domestic encryption requirements, the use of domestic certification bodies, mandates to develop internal ICT systems, and data residency requirements.

[81] *See, e.g.*, 征信机构信息安全规范 [Information Security Standards for Credit Reporting Institutions], Art. 6 (China Banking Regulatory Commission, *effective* Nov. 17, 2014); 关于加强电信和互联网行业网络安全工作的指导意见 [Guiding Opinions on Enhancing the Cybersecurity Works in the Telecommunications and Internet Industries], Art. 2(4) (Ministry of Industry and Information Technology, *effective* Aug. 28, 2014).

[82] 中国银行业监督管理委员会关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见 [Guiding Opinions of the China Banking Regulatory Commission on Strengthening the Banking Network Security and

The Guidelines also categorize IT products used by banks and provide a rubric for how that goal is to be achieved, with banks required to increase the percentage of their IT inventory that meets the specified criteria by a minimum of 15% each year.[83] According to the Guidelines, "secure and controllable" products and technologies in the banking sector are those that are "capable of meeting the information security needs of the banking industry and whose *technical risks, outsourcing risks, and supply chain risks* are controllable" (emphasis added).[84] CBRC officials have acknowledged informally that the agency's understanding of what constitutes "secure and controllable" technology is that products should be manufactured locally, source code should be stored locally, and R&D should be carried out locally.

The annex to the Guidelines, which is currently not available through official sources, includes a list of IT devices, software, services, and specific conditions for what would satisfy the "secure and controllable" requirement for each.[85] Depending on the listed item, requirements may include indigenous intellectual property, the filing of source codes with CBRC, the use of domestic encryption, compliance with national standards, and/or conducting R&D and servicing of products locally.[86] The annex also sets percentages of newly procured devices, software, and services that must be "secure and controllable."[87] These requirements are problematic for ICT firms that (i) are already struggling to protect their intellectual property in the country, and (ii) may have licensing obligations that preclude the disclosure of such code to customers in other countries who would be deeply concerned about possible security issues if a foreign government is given access to the code.

Information Technology Construction through the Application of Secure and Controllable Information Technologies], Art. 1 (China Banking Regulatory Commission, *effective* Sep. 3, 2014).

[83] *Id.*, Art. 3(3).

[84] 中国银监会办公厅、工业和信息化部办公厅关于印发银行业应用安全可控信息技术推进指南（2014-2015年度）的通知 [Notice of the China Banking Regulatory Commission and the Ministry of Industry and Information Technology on Issuing the Promotion Guidelines for the Application of Secure and Controllable Information Technologies in the Banking Sector (2014 – 2015)], Art. 1(2) (China Banking Regulatory Commission and the Ministry of Industry and Information Technology, *effective* Dec. 26, 2015).

[85] 银行业信息技术资产分类目录和安全可控指标(2014-2015年度) [Classified Catalogue of and Secure and Controllable Indicators for the Information Technology Assets in the Banking Industry (China Banking Regulatory Commission and the Ministry of Industry and Information Technology, *effective* Dec. 26, 2015).

[86] *Id.*

[87] *Id.*

Beyond the "secure and controllable" standard, the Guidelines promote indigenous technologies and prioritize foreign suppliers who are willing to facilitate the transfer of core technical know-how to financial institutions.[88] They were of significant concern not only to foreign multinationals doing business in China, which would have been forced to operate with different technologies to compete on a level playing field, but also global service providers.

Concern with the CBRC Guidelines was so great[89] that: (a) in the late spring of 2015, China, in response to pressure by the Japanese, European and U.S. governments, announced that it would suspend implementation of the Guidelines pending further feedback; and (b) during the U.S.-China Strategic & Economic Dialogue ("S&ED") in June 2015, China vowed to withdraw the guidelines and provide an opportunity for public comment on a new, presumably more amenable, draft.[90]

Nevertheless, there is a question of whether this pull-back is likely to be temporary,[91] and the concept of "secure and controllable" has already been included in other recent Chinese regulations and policy statements. In January 2016 People's Bank of China Science and Technology Office Director General Wang Yonghong in an article on the PBOC website expressed the need for national security policies to be interwoven into banking regulations. The Director General emphasized the importance of creating a secure and controllable industry ecosystem—reinforcing the

[88] 中国银监会办公厅、工业和信息化部办公厅关于印发银行业应用安全可控信息技术推进指南（2014-2015年度）的通知 [Notice of the China Banking Regulatory Commission and the Ministry of Industry and Information Technology on Issuing the Promotion Guidelines for the Application of Secure and Controllable Information Technologies in the Banking Sector (2014 – 2015)], Art. 2(9) (China Banking Regulatory Commission and the Ministry of Industry and Information Technology, *effective* Dec. 26, 2015).

[89] See letter from 18 trade associations, to the Chinese Communist Party Central Leading Group for Cyberspace Affairs (January 18, 2015); letter from 17 trade associations, to Secretary John Kerry, Secretary Jacob Lew, Secretary Penny Pritzker, Ambassador Michael Froman, and Director Jeffrey Zients (February 4, 2015); and letter from 31 trade associations, to the Chinese Communist Party Central Leading Group for Cyberspace Affairs (April 13, 2015).

[90] Concerns regarding discrimination and a lack of transparency in the formulation of relevant laws and regulations are reflected in the joint U.S.-China fact sheet published by the U.S. Department of Treasury. *2015 U.S.-China Strategic and Economic Dialogue Joint U.S.-China Fact Sheet – Economic Track Cite* (US Department of the Treasury, Jun. 25, 2015), https://www.treasury.gov/press-center/press-releases/Pages/jl0092.aspx (last visited Jan. 28, 2016).

[91] *China Rows Back on Bank Technology Regulation* (Financial Times, Apr. 17, 2015, 7:31 AM), http://www.ft.com/cms/s/0/3a0e7e8c-e4be-11e4-8b61-00144feab7de.html#axzz409wGFZFY (last visited Feb. 14, 2016).

continued promotion of secure and controllable technology policies by China's financial regulators.[92]

China on April 19, 2016 submitted [G/TBT/N/CHN/1172] to the Committee on Technical Barriers to Trade of the WTO, notifying WTO members that the CIRC would adopt the Provisions 60 days after circulation by the WTO Secretariat (June 16), and the Rules would become effective 6 months after adoption. However, CIRC has yet to promulgate the Provisions in final form. The Provisions would have a broad impact on foreign businesses operating in China well beyond insurance companies, as they would materially affect information technology providers that service the insurance industry, as well as accounting, actuarial, legal and consulting service providers to insurers.

The confluence of the Chinese government's longstanding, strong desire to develop its domestic ICT industry and its growing, related emphasis on cybersecurity have been enhanced further by the current leadership's broad conception of national security—vividly displayed since key pieces of a new, more comprehensive national security regime began to emerge in late 2014. Deeply embedded in this broad understanding of national security are cybersecurity and control of the internet. Since he entered office, President Xi has asserted that "national security no longer exists without network security."[93] During his speech at the launch of the Central Leading Group, he asserted that "network security and informatization are key strategic issues related to national security and development."[94] In those remarks, President Xi called for the development of a legal infrastructure for the administration of cyberspace, with particular emphasis on the protection of "critical information infrastructure."[95]

China views control of the Internet as a national security issue. Thus, the Chinese government has become a champion for what it calls "Internet sovereignty," a concept under which the currently free, borderless Internet would be subject to surveillance, significant content moderation, and extensive regulation by national governments. The Chinese government has justified its push for "Internet sovereignty" partly on the need for defensive cybersecurity measures. China's emphasis on "Internet sovereignty," however, is also widely understood to be tied to its desire to exert control over Internet

[92] U.S. Chamber of Commerce analysis of PBOC Science and Technology Director General Wang Yonghong's article: http://image.uschamber.com/lib/feed13797d6c06/m/1/PBOC+English+Final.pdf.

[93] *习近平：没有网络安全就没有国家安全* [*Xi Jinping: National Security No Longer Exists Without Network Security*], People.cn (Feb. 28, 2014, 04:27 AM), http://it.people.com.cn/n/2014/0228/c1009-24495308.html (last visited Jan. 28, 2016).

[94] *Id.*

[95] *Id.*

content. The country's chief Internet watchdog, CAC, oversees the country's Internet censorship apparatus. CAC's mandate also includes data privacy and cybersecurity issues that traditionally fell under the supervision of MIIT—presumably allowing measures related to data privacy, which may attract greater public support, to be grouped together with other more aggressive CAC policies.

Case Study II: "Server Sinification"

The case of China's first wholly domestically-produced, high-end server illustrates the point of interconnectivity between China's industrial and cybersecurity policies. To reduce China's reliance on foreign IT companies—such as IBM, Oracle, and Hewlett-Packard—in 2009 the government launched an "import substitution campaign" to simultaneously advance both the country's industrial goals and national security imperatives.[96] The result was the successful production and market launch of the Tiansuo K1 high-end computer server that culminated in January 2013.[97]

The government enshrined its "server sinification" policy in China's 11th Five Year Plan. In justifying such an approach, various Chinese officials have long advocated that the over- reliance on foreign IT systems "jeopardizes the country's information security."[98] They argue further that the failure of China to maintain an independent domestic production capability results in an economic disadvantage because servers in China sell for an average of 2.4 times their price in the United States.[99]

The production of the K1 server has had a notable impact throughout other areas of China's domestic policy goals. Chinese state-owned enterprises in the banking industry have adopted the Tiansuo K1 server. It is estimated that the K1 is "in 14 second tier bank branches, nearly 200 trading websites, more than 3,000 bank tellers, 20,000 self-service and electronic equipment supply services, as well as in financial transaction communications."[100] For a further discussion of China's cybersecurity goals as they relate to the banking industry, see the text-box "The "Secure and Controllable" Standard in China" above.

[96] China's "Server Sinification" Campaign for Import Substitution: Strategy and Snowden (Part 2), China Brief Volume 15 Issue 2 (Jan. 23,2015) http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=43437&cHash=248b4fdc547a80f3209b2a3aad3a1b1b#.VwoJ3k0UW71

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

a) *National Security Law & National Security Reviews*

The Standing Committee of the National People's Congress ("NPC") passed the country's most comprehensive piece of national security legislation in July 2015, a sweeping *National Security Law* that establishes an expansive framework on security and that describes in broad terms how the country's leadership understands its security interests.[101]

The new law's breadth is evident in its assertion that China's security interests extend far beyond its physical borders, even into the depths of the oceans, the Arctic, outer space, and, of course, cyberspace.[102] It describes national security as encompassing political security, military security, social and cultural security, ecological security, agricultural security, and much more. The law emphasizes the importance of cybersecurity, and has been hailed by the Chinese government as a milestone in transforming the country's outmoded legal framework for dealing with security-related matters into one that addresses 21st-century challenges presented by globalization and information technology. It is clear that the broad definition of national security is not merely rhetoric. Government agencies have already begun to use similar definitions in other legal documents. For example, an opinion issued by the State Council in October 2015 suggested that in implementing a nationwide system under which market access would be presumed unless included on a "negative list", the government should include on that negative list, among other things, a broad exception for:

> "industries, fields, businesses, etc., that raise national security concerns such as those concerning the security of human life and property, political security, homeland security, military security, economic security, financial security, cultural security, social security, S&T security, information security, ecological security, security of resources, nuclear security, security in new fields, etc."[103]

Furthermore, in June 2016, the State Council issued an opinion on establishing a Fair Competition Review System, in an effort to regulate government behavior, prevent issuance of policies that restrict or eliminate competition, and gradually eliminate barriers to a unified national market. However, the opinions contain a broad exemption for:

---

[101] 中华人民共和国国家安全法 [National Security Law of the People's Republic of China] (Standing Committee of the National People's Congress, *effective* Jul. 1, 2015).

[102] *Id.*, Arts. 25 and 32

[103] 国务院关于实行市场准入负面清单制度的意见 [Opinions of the State Council on Implementing a Market Access Negative List System], Art. 2(7) (State Council, *effective* Dec. 1, 2015).

"safeguarding national and economic security, cultural security, or that involves national defense construction."[104]

Beyond the definition of national security, the *National Security Law* is replete with high-level policy exhortations but vague when it comes to details. This is typical of important laws in the Chinese legal system, which leave the details to implementing regulations issued by government agencies and departments. Thus, it will be some time before the full impact of the law is known.

Nonetheless, the law itself establishes basic guidelines that set the direction for the development of China's evolving national security regime and how the government is to coordinate national security-related work.[105] It also creates broadly worded obligations for citizens and corporations to assist the government in protecting national security.[106] How those obligations are interpreted and applied may have significant repercussions for foreign investors, especially ICT companies whose networks and technologies play important roles in today's digital infrastructure.

Article 24 states that "the state shall strengthen the building of capability of indigenous innovation, accelerate the development of indigenous and controllable strategic new and high technologies and core technologies in important fields, strengthen the utilization and protection of intellectual property rights and the building of science and technology secrecy capability, and guarantee the security of major technologies and projects." Article 25 mentions the "secure and controllable standard" that has become an increasingly prevalent and important feature in Chinese law and policy. We discuss the "secure and controllable" standard in more detail above.

Recent years have also witnessed a resurgence in and expansion of China's regime for the review of investments on national security grounds. This may in part be a reaction to Chinese frustrations with the analogous process for national security review of foreign investments in the United States by the Committee on Foreign Investment into the United States ("CFIUS"), but the mandate of Chinese national security review mechanisms is much broader and equally, if not more, opaque. Under procedures first formalized in February 2011, a proposed M&A transaction would be subject to national security review if it would involve a foreign investor obtaining "actual control" over a domestic enterprise falling into one of the following categories:

1) military and military support enterprises;
2) enterprises in the vicinity of key and/or sensitive military facilities;

[104] 国务院关于在市场体系建设中建立公平竞争审查制度的意见 [Opinion on Establishing a Fair Competition Review System in a Market System] (State Council, released June 14, 2016) ("Opinion on the Fair Competition Review System") (Article 3.4.1: Policy measures that safeguard national economic security, cultural security, or are related to national defense construction.), http://www.gov.cn/zhengce/content/2016-06/14/content_5082066.htm.

[105] 中华人民共和国国家安全法 [National Security Law of the People's Republic of China] (Standing Committee of the National People's Congress, *effective* Jul. 1, 2015), Ch. 4.

[106] *Id.*, Ch. 6.

3) other entities associated with national defence and security; and
4) domestic enterprises engaged in sectors that "relate to national security":
   a) important agricultural products;
   b) important energy and resources;
   c) important infrastructure;
   d) important transportation services;
   e) key technologies; and
   f) major equipment manufacturing industries.[107]

These categories have been steadily expanding, with a set of trial measures for national security reviews for transactions in the country's pilot free trade zones ("FTZ Trial Measures") further adding "IT products and services" and "important culture" as sectors that "relate to national security" as sub-items under list item #4 above.[108] Furthermore the list of review criteria for national security reviews nationally under the 2011 regulation are broad and vague, requiring an assessment of the impact of a proposed M&A transaction on:

- national defense and security (specifically, impact on production capacity, service capacity, and equipment and facilities associated with national defense);
- national economic stability;
- social order; and
- research and development capacity for key technologies related to national security.[109]

The FTZ Trial Measures add to this list the impact of the transaction on the "network security of the state" as well as on "cultural security and public morality."[110] They also expand the scope of national security reviews in the pilot FTZs beyond M&A

[107] 关于建立外国投资者并购境内企业安全审查制度的通知 [Circular on the Establishment of a System for Security Review of Acquisition of Domestic Enterprises by Foreign Investors], Art. 1(1) (General Office of the State Council, *effective* Mar. 5, 2011).

[108] 国务院办公厅关于印发自由贸易试验区外商投资国家安全审查试行办法的通知 [Notice of the General Office of the State Council on Distributing Pilot Rules for National Security Review of Foreign Investment in Free Trade Zones], Art.1(1) (General Office of the State Council, *effective* May 8, 2015). ("**FTZ Trial Measures**")

[109] 关于建立外国投资者并购境内企业安全审查制度的通知 [Circular on the Establishment of a System for Security Review of Acquisition of Domestic Enterprises by Foreign Investors], Art. 2 (General Office of the State Council, *effective* Mar. 5, 2011).

[110] 国务院办公厅关于印发自由贸易试验区外商投资国家安全审查试行办法的通知 [Notice of the General Office of the State Council on Distributing Pilot Rules for National Security Review of Foreign Investment in Free Trade Zones], Art.2 (General Office of the State Council, *effective* May 8, 2015).

transactions, adding coverage to greenfield projects and investments in domestic enterprises through contractual control, commissioned shareholding, trust, reinvestment, overseas transaction, lease, or subscription of convertible bonds.[111]

China's Draft Foreign Investment Law

Although still in draft form, China's draft Foreign Investment Law would expand the definition of "foreign" investments covered by the review process.[112] Once complete, the law will abrogate existing laws covering foreign investment.

The new law expands the definition of what constitutes a foreign investment by focusing on "substance over form." No longer will the authorities subject a transaction to review only if the immediate investor is a foreign entity. Instead, regulators will look to see if the parent shareholders of an investor are foreign—even when investing through a China-incorporated wholly-owned subsidiary. This expanded definition applies to foreign interests acquired through the establishment of domestic enterprises, obtaining equity interests, the provision of financing with a term of one year or more, obtaining concession rights, as well as a number of other methods.[113]

Expanding the definition of what constitutes a foreign investment will result in increased opportunities for Chinese regulators to object to transactions seen to jeopardize national security or are at odds with China's industrial policy. The broadening of the definition–in combination with the gradual expansion of the covered categories listed above–could increase the rate at which China deglobalizes.

The new *National Security Law* gives a nod to these developments in the country's nascent regime for national security reviews, stating in Article 59 that "foreign investments that infringe upon, or may infringe upon, national security" must undergo national security review.[114] It then goes on to state that investments involving "key materials and technologies," "Internet or information technology products and services," and "other major projects and events" must also be subjected to national security review—requirements that will affect ICT companies nationwide, unlike those

[111] *Id.*, Art. 1(2).

[112] 中华人民共和国外国投资法(草案征求意见稿) [The Foreign Investment Law of the People's Republic of China (Draft for Consultation)] (MOFCOM, Jan. 19, 2015).

[113] Denton's analysis of China's Draft Foreign Investment Law (Mar. 5, 2015): http://www.dentons.com/en/insights/articles/2015/march/5/chinas-draft-foreign-investment-law?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[114]中华人民共和国国家安全法 [National Security Law of the People's Republic of China] (Standing Committee of the National People's Congress, *effective* Jul. 1, 2015) Art. 59

contained in the FTZ Trial Measures.[115] It is possible that the broad definition of national security under the new law may lead to an ever-expanding scope for Chinese national security reviews of foreign investments.

b) *(Draft) Cybersecurity Law*

The same week China's new *National Security Law* was passed, the NPC published a draft *Cybersecurity Law* for public comment,[116] which articulated further the government's priorities related to cyberspace and information networks more broadly. A second draft of the law was circulated for public comment on July 5, 2016.[117]

The draft law is engineered to govern most activities that take place over "computer networks," defined broadly in Article 72(1) to encompass essentially any "network or system, composed of computers or other terminals together with relevant devices, that serves to collect, store, transmit, exchange, or process information following predefined rules and procedures."[118] Compared to the much more general terms in the *National Security Law*, the seven chapters and 75 articles of the draft *Cybersecurity Law* provide more detail on, among other things, security requirements for network-related products and services; data privacy; and monitoring and emergency response systems. The draft attempts to (1) implement new, high-priority mandates such as provisions on the protection of critical information infrastructure; and (2) sort out and develop, in a more systematic way, existing but scattered legal requirements (*e.g.*, obligations of network users to provide real identities and obligations of network operators to protect personal information of users). Its implications for ICT companies, and other companies with business operations or interests in China, may be enormous.

The draft *Cybersecurity Law* proposes that network products and services that operators of "critical information infrastructure" procure must pass a security review if they "may affect national security."[119] However, unlike the first draft of the law, which defined "critical information infrastructure" broadly to include networks and systems in sensitive areas such as public communications, radio and television, energy, transportation, water, finance, utilities, healthcare, social security, military, and government administration, as well as those "owned or managed by service providers

---

[115] *Id.*

[116] 中华人民共和国网络安全法(草案) [Cybersecurity Law of the People's Republic of China (Draft)] (Standing Committee of the National People's Congress, Jul. 6, 2015), http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (last visited Jul. 14, 2016).

[117] 中华人民共和国网络安全法(草案)(二次审议稿) [Cybersecurity Law of the People's Republic of China (Second Reading Draft)] (Standing Committee of the National People's Congress, Jul. 5, 2016), http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm (last visited Jul. 14, 2016).

[118] *Id.*, Art. 72(1).

[119] *Id.*, Art. 33.

with massive numbers of users,"[120] the second draft leaves the scope of critical infrastructure undefined, to be determined by the State Council in subsequent regulations.[121]

The draft law proposes to formulate and revise national and industry standards on network safety management and on network products, services, and operations;[122] grant government support to key industries and innovation projects related to network security technology and promote "secure and trustworthy" network products and services;[123] adopt a multi-level protection system on network security;[124] and publish a catalogue on key network equipment and network security products.[125] Given past experience in the security area, it is possible, if not likely, that such standards and policies may be formulated in a way that favors homegrown technologies, products, and services. [126]

The draft *Cybersecurity Law* also consolidates a number of data privacy requirements currently scattered across a range of laws and regulations under its high-level legal mandate, and also adds some new ones. Among the new requirements are an expanded definition of personal information[127] and notification requirements for data breaches.[128] Operators of critical information infrastructure must store citizens' personal information and "important business data" collected and generated during onshore operations within PRC territory.[129] If they seek to provide such information and data overseas for business reasons, their request must pass a new government security assessment.[130] The draft is unclear as to what would be considered to be "important business data" for these purposes.

---

[120] 中华人民共和国网络安全法(草案) [Cybersecurity Law of the People's Republic of China (Draft)], Art. 25 (Standing Committee of the National People's Congress, Jul. 6, 2015), http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (last visited Jul. 14, 2016).

[121] 中华人民共和国网络安全法(草案)(二次审议稿) [Cybersecurity Law of the People's Republic of China (Second Reading Draft)], Art. 29 (Standing Committee of the National People's Congress, Jul. 5, 2016), http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm (last visited Jul. 14, 2016).

[122] *Id.*, Art. 14.

[123] *Id.*, Art. 15.

[124] *Id.*, Art. 20.

[125] *Id.*, Art. 22.

[126] *Id.*, Art. Articles 10, 14, 15, 20, 21, 22, 33, and 22
See also: *See, e.g., A Cybersecurity Law in China Squeezes Foreign Tech Companies*, Bloomberg (Jan. 22, 2016, 05:14 AM), http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies (last visited Jul. 27, 2016).

[127] *Id.*, Art. 72(5).

[128] *Id.*, Art. 41.

[129] *Id.*, Art. 35.

[130] *Id.*

It remains to be seen what the final law will look like and whether the concerns of ICT companies and others are taken into account. Once the law is passed, as with the *National Security Law*, implementing regulations will play an important role in how it affects business. These security laws—when combined with the MLPs, banking regulations, and regulations from the CIRC (discussed above)—provide Chinese authorities with a multifaceted toolkit to regulate individuals and companies into compliance with its stated policy objectives.[131] There is one consistent and recurring theme in these recent measures: the use of security-related requirements to support the development of indigenous technologies and exclude foreign technologies from China unless they have been acquired or controlled by Chinese parties.

Case Study III: Use of National Security to Impede Market Access for Foreign Payment Networks

For the last 14 years, China has conferred on China UnionPay ("CUP") a *de facto* monopoly on the processing of transactions on RMB-denominated payment cards (*i.e.*, credit and debit cards) in China. During that time, there was no process in place for foreign payment networks like Visa or MasterCard to even apply for a license to process such transactions.

In 2012, a WTO panel found that China was required to allow foreign payment networks to establish a commercial presence in China to provide electronic payment services, including for RMB-denominated transactions.[132] Four years later, on June 7, 2016, China issued new regulations, the Administrative Measures on Bankcard Clearing Institutions (the "Administrative Measures"), which allow foreign payment networks to apply for a license to process RMB-denominated transaction. In reality, the regulations raise new market access obstacles that have the potential not only to perpetuate the *de facto* ban on the processing of RMB-denominated transactions by foreign payment networks, but also to roll back existing opportunities to process foreign currency transactions, such as transactions made by Americans travelling in China with US-issued payment cards.

Many of those new restrictions are imposed in the name of cybersecurity or national security. For example, regulators will suspend the processing of a license application to allow for a national security review, as required by law.[133] It is not clear how this provision will be applied in practice, or the circumstances that would call for a national security review. No other country in the world builds such a review into a license application process for provision of payment card services.

[131] See letter from approximately 40 trade associations to Chinese Premier Li Keqiang (August 10, 2016).

[132] Panel Report, *China – Certain Measures Affecting Electronic Payment Services*, WT/DS413/R and Add.1, adopted 31 August 2012, DSR 2012:X, p. 5305, para. 7.575.

[133] 银行卡清算机构管理办法 [Administrative Measures on Bank Card Clearing] Article 13 (final clause). ("**Administrative Measures**")

The Administrative Measures also impose burdensome requirements, also in the name of security, including a requirement to use only commercial products recognized by China's State Encryption Management Institution.[134] To the extent these provisions require use of domestic products and technology, these requirements are unprecedented elsewhere in the world. In short, China appears to be using national security and cybersecurity mandates to advance its general industrial policy, and to restrict commercial opportunities for foreign companies.

These requirements harm not only U.S. companies, but also Chinese consumers (including cardholders and merchants) that would benefit from greater competition in the market for payment services. Keeping foreign companies out of the market and relying on indigenous, non-interoperable technology standards and "secure and controllable" products will limit consumers' choice, and introduce unnecessary risks into the payment system. Consumers are unable to enjoy a range of convenient and cutting-edge digital innovations that are excluded, and are deprived of the benefits that might arise from real competition between Chinese and international companies. Over time, cutting off Chinese cardholders and merchants from an innovative, competitive market could also harm China's broader national economy.

c) *Counter-Terrorism Law*

At the end of December 2015, the NPC Standing Committee enacted a *Counter-Terrorism Law*, which went into effect on January 1, 2016.[135] Drafts of the law were originally released in November 2014 and February 2015 and attracted significant controversy. The *Counter-Terrorism Law* reinforces the government's broad powers to investigate and prevent incidents of terrorism, and requires citizens and companies to assist and cooperate with the government in dealing with such matters. It also imposes new obligations on companies in certain sectors. Non-compliance or non-cooperation can lead to significant penalties, including fines on companies and criminal charges or detention for responsible individuals.[136]

The law provides a definition of terrorism and includes provisions regarding procedures to designate a terrorist organization or individual, functions and responsibilities of counter-terrorism agencies, response plans for terrorist attacks,

[134] *Id.*, Article 4.

[135] 中华人民共和国反恐怖主义法 [Counterterrorism Law of the People's Republic of China] (Standing Committee of the National People's Congress, *effective* Jan. 1, 2016).

[136] *Id.*, Ch. 9.

international counter-terrorism cooperation, and obligations on citizens and companies to assist and cooperate with the government.[137]

In addition to imposing broad obligations to assist and cooperate, the law requires companies operating in many sectors to take specific actions when investigating terrorism cases. For example, companies in many sectors, such as freight, transportation, and hospitality (including car rental), as well as providers of telecommunications, internet, and financial services, are required to conduct identity checks of their customers or clients and deny service to whoever declines to provide such information.[138]

The final version of the law does not explicitly mention some of the requirements in the publicly released draft versions of the law that drew the greatest criticism—including requirements to register encryption keys and keep servers and user data within China—but it still requires companies in the telecommunications and internet services sectors to:

- "provide technical support and assistance, including handing over access or interface information and decryption keys;"[139] and
- "establish content monitoring, network security programs, and other precautionary security measures to prevent the dissemination of information on terrorism or extremism…[and] report terrorism- and extremism-related information to the authorities in a timely manner; and promptly delete such messages, while keeping original records, to prevent further circulation."[140]

Non-compliance may result in fines on both companies and responsible individuals, as well as detention or criminal charges.[141]

The new obligations on telecommunications and internet service operators to proactively monitor their networks for terrorism information and disclose such information to the authorities could present a significant additional burden on companies' operations, especially in the ICT sector. The law has not clarified what types of content monitoring and security programs will be deemed as sufficient, but implementation guidelines providing further details are expected to be issued.

---

[137] 中华人民共和国反恐怖主义法(草案) [Counterterrorism Law of the People's Republic of China (Draft)], Chs. 2, 3. 5. 6. 7. 10 (Standing Committee of the National People's Congress, Nov. 3, 2014).

[138] 中华人民共和国反恐怖主义法 [Counterterrorism Law of the People's Republic of China], Art. 21 (Standing Committee of the National People's Congress, *effective* Jan. 1, 2016).

[139] *Id.*, Art. 18.

[140] *Id.*, Art. 19.

[141] *Id.*, Art. 84.

* * *

All of these laws and regulations, ostensibly developed to protect national security and cybersecurity, create new tools for Chinese regulators to promote domestic industry. Many have been specifically developed, at least in part, to promote the development of a domestic ICT industry in the name or under the guise of security. A few have been promulgated largely or entirely for security purposes, but their ambiguities could be used against foreign ICT companies and their products.

C. Other Governments Adopting Policies Targeting ICT Sector

While China has been the most active and assertive nation promoting technology acquisition and indigenization, it is not the only one. To the contrary, a number of other countries have recently imposed new requirements on foreign ICT companies, particularly in the wake of Edward Snowden's revelations of U.S. intelligence operations.

Russia. Russia stands out as a country that has moved to enact new laws and regulations for both ICT companies and data that erect trade barriers without security benefits. The Russian government has adopted laws requiring certain types of data to remain within Russia. Under a legislative package adopted by the Russian Parliament on June 24, 2016, for example, telecom and Internet providers are obligated to store records of all communications for six months and all metadata for three years, as well as help intelligence agencies decode encrypted messaging services. Russian telecoms firms have voiced concern that users rather than providers typically possess the encryption keys, and that storing this huge amount of information would require expensive new infrastructure.

Under the most recent amendment to the "On Personal Data" Law ("OPL"), any data operator who stores the data of Russian citizens must store such data within Russia. Prior to amendment, companies involved in data collection such as Google and Facebook were permitted to collect data in Russia and store it in data centers located in other countries.[142] The OPL Law applies to any "operator" that "process"[es] "the "personal data" of Russian citizens. "Operator" means not only those who operate physically in Russia, but also those who operate websites that "target" Russia, such as by offering Russian language versions or using Russian domain names.[143] In addition to data localization laws, Moscow has also drafted a law that would grant preferential treatment to domestic software companies in government procurement. Foreign IT companies have sharply criticized these laws, with some companies threatening to

[142] http://www.bna.com/russia-clarifies-looming-n17179934521/.

[143] http://www.law360.com/articles/698895/3-things-to-know-about-russia-s-new-data-localization-law.

suspend investment or withdraw entirely from the Russian economy.[144] A recent study published by the European Centre for International Political Economy ("ECIPE") found that the data localization requirements will have a negative impact on foreign trade because of the additional costs to be imposed upon foreign companies who must move data storage facilities into Russia.[145]

In addition to the Russian Government's ongoing efforts to localize data, it has been subjecting commercial ICT products incorporating encryption to import and export licensing and reporting requirements. Specifically, encryption products being imported into Russia must undergo examination by the Russian Federal Security Service (FSB), which essentially requires that applicants submit technical product specifications and a product sample to the FSB Licensing Center to secure an import permission. Once the FSB authorization is granted, an import license must be approved by the Ministry of Industry and Trade.

Furthermore, Russian authorities regulate temporary imports of ICT products implementing encryption for activities such as research & development, marketing, certification, and internal importer use (e.g. engineering samples and development vehicles). There are also a number of general purpose ICT devices that require a notification to be submitted to the Russian Government, including wireless products that use encryption for communication channel security and solid state drives (SSDs) which utilize encryption for authentication and access control purposes.

To address the heavy administrative burdens and border delays that evolving Russian encryption requirements were causing for U.S. technology companies, the U.S. and Russian governments entered a bilateral agreement in 2006 that obligated Russia to (i) not impose more restrictive conditions for importation of goods with encryption that solely performs authentication functions than existed as of the date of the agreement, and (ii) apply to those same goods the same treatment as goods covered under the exemptions indicated in the Notes to Category 5, Part 2 "Information Security" of the Wassenaar Arrangement Dual Use List.[146] However, the implementation of the exemptions articulated under the Wassenaar Arrangement Dual Use List may be difficult to fully implement, as there is no direct correlation between harmonized tariff schedule codes used in the import process and the Export Control Classification Number (ECCN) based nomenclature the Wassenaar Arrangement utilizes. As a result, the U.S. and Russian governments should examine how the current Russian government licensing and reporting requirements for ICT products incorporating encryption are complying with the 2006 bilateral agreement requirements.

---

[144] http://www.themoscowtimes.com/business/business/article/foreign-it-companies-threaten-to-quit-russia-over-restrictive-legislation/541483.html.

[145] http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

[146] Letter From Susan C. Schwab, United States Trade Representative, to H.E. German Gref, Minister of Ministry of Economic Development and Trade of Russian Federation (November 19, 2006). Compliance with this bilateral agreement became a condition of Russia's WTO accession.

Brazil. The Brazilian government implemented security testing in the ICT sector. A 2002 resolution ("Resolution 322) by the Brazilian National Telecommunications Agency mandates local testing of all telecommunications equipment imported from the United States—even though the testing and certification is already conducted within the United States.[147] This duplicative testing—implicitly justified on national security grounds—is a barrier to trade because it increases the costs for foreign imports and delays implementation of international contracts in the telecommunications sector. As a result of regulations implementing these requirements, domestic manufacturers are favored.[148] Further, Brazil has raised tariffs in the ICT sector.[149]

Further, following the allegation by Edward Snowden of U.S. intelligence community operations, including the U.S. government intercepting the communications of Brazilian President Dilma Rousseff and Brazil's largest company, Petrobras, the Brazilian legislature proposed adding a provision to the country's Internet law that would give the executive branch the power to require that data about Brazilians be stored in Brazil. The provision was later removed from the law after widespread opposition focused on the financial burden that the law would place on foreign and domestic companies forced to relocate their data storage centers to Brazil.[150]

India. In recent years, India has promulgated various measures allegedly to secure its telecom networks and broader ICT infrastructure, although it has removed or amended a number of requirements that would have discriminated against foreign ICT products and services in response to domestic and foreign concerns. As justification, certain officials in the Ministry of Communications and Information Technology (MCIT) repeatedly stressed the need to ensure security due to the Mumbai terrorist attacks that were coordinated using cell phones. However, along with security considerations, the purpose of some of the regulatory requirements that have been proposed clearly has been to encourage the development and manufacture of local ICT products.

For instance, in late 2009 the Department of Technology (DOT) in MCIT issued an initial draft of a telecom license amendment affecting telecom service providers and licensees that (i) mandated the transfer of technology from foreign equipment manufacturers to domestic ones, and (ii) required all equipment manufacturers to escrow source code and other sensitive design elements when selling equipment to telecommunications operators in India. On March 18, 2010, DoT clarified its license amendment, which imposed a security clearance process for the procurement of

[147] https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[148] https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[149] https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[150] http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-Internet-bill; *see also* http://articles.chicagotribune.com/2013-11-04/news/sns-rt-us-brazil-Internet-20131028_1_alessandro-molon-Internet-constitution-in-country-data-storage.

equipment and software used in Indian telecom infrastructure. The revised license amendment exempted from the security clearance process any equipment and software that is manufactured and developed in India by Indian owned or controlled manufacturers. The more specific license amendment repeated the technology transfer requirement, indicating that non-compliance could trigger criminal penalties. The amendment also required that the operation and maintenance of telecom networks be done entirely by Indian engineers. One of the reasons industry remained skeptical as to the alleged security purpose behind many if not all of these DoT license requirements is that in late 2010 the Telecom Regulatory Authority of India (TRAI) issued a new telecom equipment manufacturing policy, followed by specific recommendations in April 2011 that contemplated the use of preferential procurement and other market access measures as well as tax and other incentives to favor local products and manufacturers of telecom equipment. As the European Union Directorate-General for Trade and various ambassadors from European member states made clear, a number of those TRAI recommendations discriminated against foreign ICT products in violation of WTO obligations.[151] The resulting international pressure on DoT and TRAI sidelined many of the draft license amendments and TRAI recommendations.[152]

In another notable development, in February 2012 the Department of Electronics and Information Technology (DeitY) in MCIT issued a Preferential Market Access ("PMA") policy which requires that "[a] specified share of each product's market—anywhere from 30 to possibly even up to 100 percent—would have to be filled by India-based manufacturers, with the local content share for each product rising over time."[153] The PMA mandate initially covered procurement by private entities requiring a license and government entities with "security implications for the country," which was written broadly enough to cover nearly half of India's ICT market.[154] One of the original long-term goals of the PMA was to have 80 percent of electronics produced domestically by 2020. The security concerns used to justify the PMA mandate were vague, revolving around vulnerability to cyber-attacks and malicious hardware that is not easily detected. Given the breadth of the PMA provisions, however, many concluded that they were a pretext to protectionism despite the alleged security concerns.

---

[151] Letter from Rupert Schlegelmilch, European Commission Directorate-General for Trade, to Lav Gupta, Telecom Regulatory Authority of India (20 January 2011); Letter from Ambassadors from Finland, France, Germany, Italy and Sweden to Shri R. Chandrashekhar, Secretary of Department of Telecommunications, Ministry of Communications of Information Technology (20 September 2011).

[152] E.g., Letter from Vini Mahajan, Joint Secretary to Indian Prime Minister (06 August 2010) (suggesting that compliance can be achieved under the old or newly proposed license amendment).

[153] Dr. Ajay Kumar, Joint Secretary, Department of Electronics and Information Technology, Notificaton on Preference to Domestically Manufactured Electronic Products in Procurement Due to Security Considerations and in Government Procurement (10 February 2012).

[154] *Hearing on U.S.-India Trade Relations: Opportunities and Challenges: Hearing Before the H. Comm. on Ways and Means Trade Subcomm.*, 113th Cong. 2 (2013) (statement of Stephen Ezell).

Indeed, the provisions of the PMA as applied to the private market violate the General Agreement on Tariffs and Trade ("GATT") because WTO member states are not permitted to discriminate against foreign competitors by forcing them into "buy local" contracts, at least to the extent that this results in discrimination against foreign goods.[155] In reaction to the multiple forceful arguments by other governments that the PMA mandate unjustifiably discriminated against foreign ICT products, in December 2013 DeitY cut back the scope of its PMA mandate so that it now applies only to government procurement. Although still a problem, this more limited discrimination is potentially lawful because India has not signed the WTO Government Procurement Agreement that prohibits it.[156] We also note that security concerns are certainly more legitimate with at least the more sensitive government procurement than with procurement among private parties.

India is learning the hard way how to balance economic development via ICT use and security concerns in light of its WTO obligations. All of the significant time spent by some of India's agencies, other governments, and international industry in fighting and then refining just the several measures mentioned above could have been easily avoided by applying a set of international principles on how to achieve the right balance between security and ICT development and deployment.

Europe. In May 2015, the European Commission adopted *A Digital Single Market Strategy for Europe*.[157] The strategy envisions a digital single market "where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence."[158] Germany's economic minister claims the strategy is about achieving "digital sovereignty,"[159] while the European Union's Digital Commissioner sees the strategy as a way to achieve "digital independence."[160] These requirements impact trade through data localization requirements. Shortly after its enactment, United States President Barack Obama rebuked the European version of creating domestic champions as a strategy "just designed to carve out some of their commercial interests."[161] Following this rebuke, the European Commission slowed its efforts and made diplomatic approaches to Washington to smooth over the controversy.[162] As the effect of the strategy is now in

[155] *Id.*

[156] Dr. Notification from Department of Electronics and Information Technology, "Preference to domestically manufactured electronic products in Government procurement" (23 December 2013).

[157] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN.

[158] https://ec.europa.eu/digital-single-market/en/digital-single-market.

[159] http://www.bmwi.de/EN/Press/press-releases,did=698066.html.

[160] http://capx.co/the-eus-digital-protectionism-will-cost-europe-dear/.

[161] http://www.ft.com/cms/s/0/41d968d6-b5d2-11e4-b58d-00144feab7de.html#axzz436X63NN5.

[162] http://www.brookings.edu/blogs/up-front/posts/2015/09/22-european-union-digital-single-market-sapiro.

limbo as EU regulators seek out public comment, foreign investors are apprehensive of what is to come.

While national security is a competency reserved to the Member States, the interface at the Member State-level between national security policy proposals and the EU's Digital Single Market merits close monitoring. This is particularly true with regard to cybersecurity. Further, there are some who are calling for the EU to gain more competency over national security matters.

Germany. The German government recently issued new rules for federal procurement that are ostensibly aimed at security and protecting sensitive information.[163] The rules, however, fail to provide clear reasoning as to why local standards and storage will achieve these goals. The approach effectively eliminates foreign multinational companies from providing federal services, as no company operating in a foreign jurisdiction can satisfy the criteria in the rules.

D. The U.S. Approach to Investment and Trade in the ICT Sector

The United States has generally resisted pressure to address ICT security concerns through measures based on country of origin. U.S. law does not, for example, create a preference for "U.S." firms in procurements in the commercial sector, nor are there information security testing requirements for commercial procurements. As discussed further below, in the government procurement space, while the Buy American Act imposes some discriminatory requirements allowed under WTO law, it largely exempts commercial off-the-shelf technology.

The United States' reluctance to impose country-of-origin requirements is consistent with the United States' longstanding policy of openness to foreign investment. While there have been times when protectionist views have gained ground, every presidential administration over the past two decades has expressly adopted policy statements confirming that the United States is open to foreign investment and supports free trade. This policy approach recognizes the substantial benefits of foreign investment and, indeed, the degree to which foreign investment is vital to growing the U.S. economy. For example, a prior report by the U.S. Chamber of Commerce estimated that "more than $8 trillion in new investment will be needed in U.S. transportation, energy, and wastewater and drinking water (water-related) infrastructure from 2013 through 2030—totaling some $455 billion per year" and that domestic sources of capital would be insufficient to meet this demand.[164]

[163] https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/

[164] U.S. CHAMBER OF COMMERCE, *supra* note 66, at 3.

While in practice the United States has generally resisted taking discriminatory actions to address ICT-related supply chains, that does not mean that the United States lacks the legal authority to take such action, as described below.

1. Broad Authorities to Address Security-Related Risks in Foreign-Origin Products

There are a range of authorities available to the Executive Branch to address perceived risks to U.S. national security arising from foreign origin ICT products, including the following:

- **International Emergency Economic Powers Act ("IEEPA")**: IEEPA authorizes the President, with the consent of Congress, to "prevent or prohibit, any acquisition, holding . . . use, transfer . . . importation or exportation of . . . any property in which any foreign country or national thereof has any interest."[165] IEEPA grants this power "to deal with any unusual and extraordinary threat, which has its source in whole or in substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat."[166] The President has broad discretion to determine what constitutes a "threat" within the statute's meaning and this decision is not subject to judicial review.[167] Thus, IEEPA would permit the President to prohibit the importation of foreign-origin equipment and software or prohibit U.S. companies from procuring or using products that the Executive Branch has reason to believe poses a national security threat.[168]

- **Export Administration Act and related statutes**: Through the Export Administration Act (EAA), the Arms Export Control Act (AECA), and other authorities, the United States restricts the export of defense items or munitions; so-called "dual-use" goods and technology—items with both civilian and military applications; certain nuclear materials and technology; and items that would assist in the proliferation of nuclear, chemical, and biological weapons or the missile technology used to deliver them. U.S. export controls are also used to restrict exports to certain countries on which the United States imposes economic

[165] International Emergency Economic Powers Act ("IEEPA"), Pub. L. No. 95–223, § 203, 91 Stat. 1625, 1626 (1977) (codified as amended at 50 U.S.C. § 1702(a)(1)(B)).

[166] 50 U.S.C. § 1701(a) (2012).

[167] *See, e.g.*, *Bernstein v. U.S. Dep't of State*, 974 F. Supp. 1288, 1310 (N.D. Cal. 1997).

[168] The Trading with the Enemy Act of 1917 ("TWEA") grants substantially the same powers as IEEPA, but may only be invoked during wartime and does not require congressional approval. Trading with the Enemy Act of 1917 ("TWEA"), ch. 106, 40 Stat. 411 (codified as amended at 50 U.S.C. app. § 5). IEEPA amended the TWEA to apply only in a time of "war" and left IEEPA to govern non-wartime national emergencies. *See Unidyne Corp. v. Gov't of Iran*, 512 F. Supp. 705, 708–09 (E.D. Va. 1981).

sanctions. At present, the EAA has expired and dual-use controls are maintained under IEEPA. As stated in a report by the Congressional Research Service, "[t]he balance between national security and export competitiveness has made the subject of export controls controversial for decades." China has repeatedly complained that U.S. export controls limit its ability to develop its own ICT industry. U.S. export controls, however, tend to be narrowly tailored to capture only the application of technologies with at least partial military use; in fact, the American high tech industry has pushed the U.S. government for decades to both update and liberalize export controls to ensure they are as least trade restrictive as possible because most of that industry's revenue is generated outside of the United States.

- **Trade Expansion Act of 1967 § 232**: Section 232 of the Trade Expansion Act provides that upon a finding by the Secretary of Commerce that certain imports pose a threat to national security, the President may "adjust" the imports to protect national security.[169] The purpose of the statute is to permit the President to protect domestic industries critical to national security. While the statute has never been applied to foreign-origin ICT, the provision has been interpreted broadly[170] and the text has been characterized as authorizing the President "to take whatever action he deems necessary to adjust imports . . . [including the use of] tariffs, quotas, import taxes, or other methods of import restriction."[171]

- **National Defense Authorization Act of 2011**: Section 806 of the National Defense Authorization Act of 2011 expanded the government's authority to exclude government contractors whose supply chains the Secretary of Defense determines are not sufficiently secure.[172] Authorized officials (i.e., the Secretaries of Defense, Army, Navy, and Air Force) may exclude a source or withhold consent to contract to address a "supply chain risk" in procurements "for information technology, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a [national

[169] Trade Expansion Act of 1967, Pub. L. No. 87–794, § 232, 76 Stat. 872, 877 (codified as amended at 19 U.S.C. § 1862).

[170] *See Fed. Energy Admin. v. Algonquin SNG*, 426 U.S. 548, 552 (1976) (holding that the President could use § 232 to institute a system of fees on imported petroleum products because the language of the statute granted the President "a measure of discretion in determining the method to be used to adjust imports"); *Consumers Union of the U.S. v. Kissinger*, 506 F.2d 136, 144 (D.C. Cir. 1974) (rejecting a challenge to the use of voluntary restraint agreements pursuant to § 232, noting the Supreme Court's broad interpretation of the provision).

[171] *Algonquin*, 426 U.S. at 564 (quoting 101 Cong. Rec. 5299 (1955).

[172] Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111–383, §806, 124 Stat. 4137, 4260 (codified as amended at 10 U.S.C. § 23).

security system]" (a "Section 806 Action").[173] The provision further allows this exclusion without revealing the reasons for doing so and limiting the right to review before the Government Accountability Office or federal courts.[174] Using its Section 806 authority, the DoD may employ three different supply-chain risk management tools: (a) exclude a source prior to award that fails to meet qualification standards for the purpose of reducing supply chain risk in the acquisition of covered systems; (b) exclude a source prior to award that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order; or (c) withhold consent after award for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude. More generally, contractors supporting procurements "for information technology, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system" must also "mitigate supply chain risk."[175]

- **The "Wolf Provision."** The Consolidated Appropriations Act of 2014 included a supply chain-related provision authored by Representative Frank Wolf (R-VA), who was then chairman of the House Appropriations Subcommittee that funds the Departments of Justice ("DoJ") and Commerce ("Commerce"), the National Science Foundation ("NSF"), and National Aeronautics and Space Administration ("NASA"). The provision—which is found in Section 515 of the Act—specifically requires those agencies to review and evaluate the supply chain risk associated with any acquisition of so-called "high-impact" or "moderate-impact" information systems, according to criteria established by the National Institute of Standards and Technology. An earlier provision authored by Representative Wolf and included in the Consolidated and Further Continuing Appropriations Act of 2013 precluded DoJ, Commerce, NASA, and NSF from acquiring IT systems from entities "owned, directed, or subsidized by the People's Republic of China." This provision was largely seen as a reaction to the 2012 Congressional report on "U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE."[176] The provision was subject to considerable criticism and pushback from U.S. industry, and was modified by the 2014 law described above. The revised approach provides for an arguably narrower scope of the types of systems subject to the requirement, but also expands the suppliers that may be

[173] Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 806, 123 Stat. 4137, 806 (2006).

[174] *See id.* § 806(a)(2).

[175] For more information, *see* DoD Issues Final Rule Addressing Exclusion of Contractors that Present Supply Chain Risk in National Security System Procurements, Covington & Burling LLP (Nov. 2, 2015).

[176] https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf.

subject to the supply chain assessment and requires procurement officials to provide a certification to Congress—an extremely high administrative bar that may well have a tempering effect on procurements that involve supply from certain countries, including China.[177]

Federal Procurement Rules:
The Buy American and the Trade Agreements Acts

U.S. Government procurements may be impacted by one of a number of different domestic sourcing requirements. The two broadest and most frequently encountered are the Buy American Act ("BAA")[178] and the Trade Agreements Act of 1979 ("TAA").[179]

The BAA mandates a preference for American goods in direct government purchases (not the private market). As implemented by Part 25 of the Federal Acquisition Regulation ("FAR"), the Act generally requires the Government to purchase only end products that have been manufactured domestically and assembled substantially from domestically-manufactured components, unless an exception applies.[180] The law applies a two-part test: (1) the end product must be manufactured in the United States, and (2) more than 50 percent of all component parts (by cost) must also be manufactured in the United States. However, the second part of this test requiring products to be manufactured from domestic components—commonly known as the "domestic components test"—has been waived with respect to procurements for commercially available off-the-shelf ("COTS") items.[181] Thus, vendors are not required to track the various countries of origin of the components of a COTS end product, although the final product must still be manufactured in the United States. The relevant portions of the Federal Acquisition Regulation implementing the BAA do, however, provide a waiver effectively giving a signatory of the WTO's GPA "national treatment" for products above a certain threshold.[182]

[177] A version of the Wolf Provision was also included in the 2015 version of the same appropriations bill.

[178] Buy American Act of 1988, Pub. L. No. 100–418, 102 Stat. 1545 (2006).

[179] Trade Agreements Act of 1979, Pub. L. No. 96–39, 93 Stat. 144 (2006).

[180] Buy American Act of 1988, Pub. L. No. 100–418, 102 Stat. 1545 (2006).

[181] Buy American Act of 1988, Pub. L. No. 100–418, 102 Stat. 1545 (2006).

[182] Federal Acquisition Regulation 52.225.

The TAA, which generally applies to federal procurements that exceed a threshold of $191,000,[183] prohibits the purchase by the federal government of goods and services unless they are manufactured or "substantially transformed" in the United States or a "designated country." Because the TAA provides that end products from "designated countries" are treated the same as U.S. end products, it essentially serves as an exception to the BAA's strict domestic-only preference. There are over 100 "designated countries," which principally include countries with which the United States has entered into free trade agreements, including Canada, Mexico, and South Korea. China is not currently a "designated country."

Together, these statutes provide authority for the executive branch to take action to address supply chain risk. The severity of potential actions the executive may take in doing so often varies from what is theoretically possible to what in reality is the case. Indeed, IEEPA and the Trading with the Enemy Act ("TWEA") potentially authorize draconian measures—such as blocking the importation of ICT equipment from certain countries—but these authorities have never been used in that fashion. The remaining authorities, including those in the NDAA, are non-discriminatory on their face.

The United States does, however, regularly use certain narrower authorities to identify and address national security risks, including risks arising from ICT supply chains. The legal tools available to the U.S. government are significantly more robust when foreign parties undertake mergers, acquisitions, or other transactions that trigger formalized review mechanisms, or when foreign parties sell to U.S. federal government customers. By contrast, foreign parties that sell to the commercial sector and do not engage in acquisitions of U.S. businesses are subject to far fewer regulatory authorities.

2. The Committee on Foreign Investment in the United States ("CFIUS")

The principal manner in which the U.S. government addresses risks that may arise from foreign investments in American businesses is through national security reviews conducted by the Committee on Foreign Investment in the United States ("CFIUS"). Section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 ("FINSA"), provides the President with express authority to review the national security effects of foreign acquisitions, mergers, and takeovers.[184] More specifically, the President has authority to review for national security implications "any merger, acquisition, or takeover…by or with any foreign person which could result in foreign control of any person engaged in

[183] Trade Agreements Act of 1979, Pub. L. No. 96–39, 93 Stat. 144 (2006).

[184] Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat 1107, 1425 (1988), (codified as amended at 50 U.S.C. App. § 2170).

interstate commerce in the United States."[185] The President ultimately has authority to suspend or prohibit any transaction that threatens to impair the national security if "there is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security,"[186] and other laws (except for IEEPA)[187] "do not in the judgment of the President provide adequate and appropriate authority for the President to protect the national security in the matter before the President."[188]

The President has delegated his initial review and decision-making authorities to CFIUS, an inter-agency body originally established in 1975 to monitor and evaluate the impact of foreign investment in the United States.[189] CFIUS is chaired by the Secretary of the Treasury, and includes eight other voting members (the Departments of Commerce, Defense, Homeland Security, Justice, State, and Energy; the U.S. Trade Representative; and the White House Office of Science and Technology).

FINSA formally requires CFIUS to conduct a risk-based analysis for transactions that it reviews. For every transaction, CFIUS engages in a three-part analysis of: (1) whether a foreign person has the capability or intention to exploit or cause harm (i.e., the "threat" associated with the buyer); (2) the vulnerabilities associated with the U.S. assets at issue (i.e., whether there are weaknesses or shortcomings in the assets that create a susceptibility to impairment of U.S. national security); and (3) the transaction's potential consequences, which relates to the "interaction between threat and vulnerability."[190] Transactions in the ICT industries often receive heightened scrutiny by CFIUS because the perceived "vulnerability" is often high, especially where the target company has existing networks in the United States, or where a target company's products are used by sensitive U.S. government customers. Nevertheless, CFIUS has approved a number of high-profile transactions in the ICT area, including Lenovo's acquisition of IBM's x86 server division in 2014.

If CFIUS determines that a particular transaction presents national security risks, it may seek to mitigate the perceived threats by imposing conditions or requiring commitments from the parties to a transaction. Such conditions and commitments may take the form of a signed agreement with agreed-upon penalties between the parties to the transaction and the relevant government agencies. Alternatively, parties have been

[185] 50 U.S.C. App. § 2170(a)(3).

[186] FINSA, § 6 (codified as amended at 50 U.S.C. App. § 2170(d).

[187] 50 U.S.C. §§ 1701–1706.

[188] FINSA, § 6 (codified as amended at 50 U.S.C. App. § 2170(d)).

[189] Executive Order 11858 (1975).

[190] *Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States,* U.S. DEPARTMENT OF TREASURY, 73 Fed. Reg. 74567, 74569 (Dec. 8, 2008).

requested to provide somewhat more informal "assurances" via a letter to the concerned agencies.

The types of commitments and assurances sought by CFIUS can vary. At the most basic level, they can be straightforward assurances that the foreign acquiror does not intend to change the business's production levels, U.S. facilities, or participation in certain U.S. government programs. Such assurances also can include concomitant recordkeeping and reporting obligations. On the other end of the spectrum, certain mitigation agreements impose various governance requirements and more costly and onerous security measures, including technical and physical security requirements, U.S. government access to systems and personnel, testing and screening of personnel, and third-party auditing. The most extreme agreements can also limit a foreign acquiror's decision-making authority and access to the U.S. company.

In ICT transactions, CFIUS may require mitigation measures specifically designed to address supply chain risk. For example, CFIUS previously has required parties to maintain code development processes and servers in the United States; subject third party equipment and service suppliers to prior review and approval by CFIUS; locate certain manufacturing processes in the United States; and make source code available for review by the U.S. government. For example, as a condition of approving SoftBank Corporation's acquisition of Sprint Nextel Corporation, CFIUS required the right to review and approve certain network equipment vendors and managed service providers of Sprint and certain of its subsidiaries.[191]

3. Team Telecom

"Team Telecom" is an ad hoc group of federal law enforcement agencies that reviews telecommunications transactions to protect U.S. interests related to national security, law enforcement, and public safety. Team Telecom is comprised of the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Department of Justice (DOJ). The Federal Bureau of Investigation (FBI), which is a component of DOJ, also participates. Other agencies, such as the National Security Agency, may play role in Team Telecom review vis-à-vis its role in a member department such as the DOD.

The primary mechanism through which Team Telecom operates is by intervening in the Federal Communications Commission ("FCC") consideration of Section 214 applications to transfer certain licenses. As Team Telecom is merely a moniker for an unofficial agency collaboration that does not operate pursuant to any specific statute or regulation, its process is notoriously opaque. While Team Telecom's authority is not expressly limited to transactions involving foreign parties, in reality that is the focus of its effort. Whenever an FCC applicant seeks a new license or whenever control of an existing license will transfer or be assigned, any ten percent or greater direct or indirect

[191] Sprint Nextel Corporation, Form 8k Report to the U.S. Security and Exchange Commission, May 29, 2013.

foreign ownership must be identified and the FCC typically notifies Team Telecom in turn.

Based on its risk assessment of a transaction, Team Telecom may: (1) object to the streamlined processing of an application such as a Section 214 application, which means that the application will not be automatically approved as might otherwise be the case for certain application; (2) request that the FCC defer consideration of a transaction; (3) object to the transaction; or (4) inform the FCC that it has no comment on the transaction (Team Telecom does not ordinarily affirmatively approve transactions).

Team Telecom initially conducts its assessment by requiring parties to respond to one or more sets of "triage questions." These triage questions request extensive information about the operations and network of the U.S. business and the foreign acquirer. In recent years, Team Telecom has used the triage questions to require that foreign parties provide information about their networks overseas (even where those networks do not connect to the United States), including network diagrams, types of encryption used, and the identities of equipment suppliers

Unlike national security agreements entered into with CFIUS, which are confidential, agreements with Team Telecom typically are made public by the FCC. Team Telecom mitigation agreements often impose the following requirements on telecom companies:

- Maintain certain facilities in the United States, subject to security requirements and U.S. government oversight;
- Prohibit disclosure of domestic U.S. communications and associated data to foreign government authorities;
- Maintain points of contact or accepting and overseeing compliance with lawful process requests; and
- Locate infrastructure supporting U.S. domestic communications inside the United States.

More recently, Team Telecom has focused increasingly on equipment providers and managed service providers. As part of this focus, Team Telecom has required approval rights over parties' use of such providers, just as CFIUS did in the SoftBank-Sprint transaction described above.

Informal Mechanisms to Influence Trade

In addition to the more formalized mechanisms discussed above, the U.S. government also employs less formal means to address perceived risks arising from foreign-origin ICT equipment. For example, suppliers of equipment for the cloud service that Amazon Web Services is developing for the U.S. intelligence community reportedly have been required to submit information relating to foreign ownership, presumably so that certain foreign-owned equipment suppliers may be excluded. In another example, in 2010 when Sprint Nextel was considering procuring Huawei equipment for its network, Commerce Secretary Gary Locke called Sprint Chief Executive Dan Hesse "to relay some very deep concerns from the defense sector and also even members of Congress."[192] Sprint later excluded Huawei from competition. It is important to note, however, these examples of informal pressure are far and few between.

E. Applicability of Global Trade Norms

As the foregoing illustrates, governments around the world—in some form or fashion—are attempting to balance the benefits from the increasing flow of ICT goods and services against the perceived security concerns they raise. There are significant differences in their approach—and some countries are using "security-related" regulations to advance other policy goals, such as supporting the development of an indigenous ICT industry.

As highlighted at the outset, each government faces a fundamental policy challenge: namely, how to avoid isolating its economy from the benefits of a global ICT supply chain while also protecting national security. In Section II below, the paper examines the economic impact of certain policy choices. Before turning to that section, however, it is useful to examine some of the existing global trade rules that discipline domestic ICT regulations and the ability of national governments to address national security.

To start, it is worth noting that the World Trade Organization ("WTO") and its associated agreements are based on the foundational principle that countries should not discriminate between or against their trading partners regarding like goods or services, although there are certain narrow exceptions to that general rule and national security concerns is one of them. At the core of the WTO regime are two different but related principles that are relevant to the ICT industries:

[192] http://www.bloomberg.com/news/articles/2010-12-07/commerce-s-locke-says-sprint-s-chief-was-called-about-huawei-bid-concerns.

- Most-Favored Nation (MFN): This is the principle that countries cannot discriminate between their trading partners. Thus, if a country wishes to grant a trade benefit to one trading partner, the same benefit must be extended to all other WTO members.

- National Treatment: National treatment, often described as prohibiting discrimination based on nationality or origin, requires that imported products or suppliers are treated no less favorably than like domestic products or suppliers. Similar rules apply to services (where applicable) and to intellectual property.[193]

These principles are enshrined in five key WTO trade agreements that impact the ICT sector, namely the General Agreement on Tariffs and Trade ("GATT"), the Trade-Related Aspects of Intellectual Property Rights Agreement ("TRIPS"), the Revised Agreement on Government Procurement ("GPA"), the General Agreement on Trade in Services ("GATS"), and the Technical Barriers to Trade Agreement ("TBT"). [194]

1. WTO General Agreement on Tariffs and Trade ("GATT")

The General Agreement on Tariffs and Trade ("GATT"),[195] originally signed in 1947, is the foundational multilateral agreement regulating international trade among the 162 members of the WTO. GATT was formulated to ensure a stable world trade and economic environment in the aftermath of WWII and does so by "regulat[ing] the foreign commerce of contracting parties."[196] The GATT was then reaffirmed in 1994 in connection with the creation of the WTO.

The GATT's provisions can be grouped into three categories: (1) tariff concessions; (2) trade rules; and (3) administrative provisions.[197] The tariff concessions or permanent reductions are given by each party to the agreement and apply broadly to trade with all other parties.[198] The trade rules discipline both tariff and nontariff barriers to trade in goods. At the heart of the trade rules are the national treatment requirement (which requires that imported products be accorded treatment no less favorable than like domestic products, including in respect of internal taxation and regulation), the MFN provision and the prohibition on quantitative restrictions on exports and

---

[193] *See* "Principles of the trading system, World Trade Organization, available at https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.

[194] Many of these obligations are also included, if not expanded upon, in the recently-concluded Trans-Pacific Partnership Agreement ("TPP").

[195] General Agreement on Tariffs and Trade ("GATT"), Oct. 30, 1947, 61 Stat. A-11, T.I.A. S 1700, 55 U.N.T.S. 194.

[196] *Id.*

[197] *United States Participation in the General Agreement on Tariffs and Trade*, 61 Colum. L. Rev. 505, 508 (1961).

[198] *See id.*

imports.[199] Other rules include freedom of transit, antidumping and countervailing duties, governmental subsidies, valuation for customs purposes, fees related to importation and exports, and marks of origin.[200] However, the GATT does not cover procurement by governmental agencies for governmental purposes.[201]

As with most WTO agreements, the GATT contains a national security exemption in Article XXI, which is discussed in subsection 5 below. To date, member states have not invoked Article XXI in any dispute settlement cases involving challenged restrictions on foreign-origin equipment and software, including where critical technologies and infrastructure were considered or alleged to be an essential security interest. However, Article XXI has been invoked in diplomatic settings to persuade certain governments to narrow measures based on security interests that are overbroad (for example, India's PMA *initiative discussed earlier).*

2. *WTO Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS")*

The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"),[202] which came into effect in 1995, requires WTO Members to provide minimum standards of intellectual property protection and enforcement. TRIPS sets forth baseline standards for areas of IP including patents, copyrights, trademarks, and undisclosed information including trade secrets[203], defines limited exceptions to those rights, and includes obligations related to domestic enforcement procedures and remedies. The TRIPS Agreement is also subject to dispute settlement.

The TRIPS Agreement includes fundamental principles on MFN, national treatment and non-discrimination. For example, TRIPS Article 3.1 states that WTO Members "shall accord to the nationals of other Members treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property."[204] With respect to patents specifically, TRIPS prohibits discrimination based

[199] *See id.*

[200] *See id*. at 509.

[201] *See* GATT Article III:8(a).

[202] Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), Apr. 15, 1994, 1869 U.N.T.S. 299.

[203] The TRIPS Agreement requires protection for information that is secret, has commercial value because it is secret and has been subject to reasonable steps to keep it secret. *See* TRIPS, art. 39.2. However, TRIPS does not include specific enforcement obligations for trade secret theft. TPP is the first international trade agreement to require Parties to establish criminal procedures and penalties for trade secret theft. *See* TPP, art. 18.78.

[204] TRIPS, art. 3.1. Two elements must be satisfied to establish a violation of the national treatment obligation in TRIPS Article 3.1: "(1) the measure at issue must apply with regard to the protection of intellectual property; and (2) the nationals of other Members must be accorded 'less favourable' treatment than the Member's own nationals." Panel Report, *EC-Protection of Trademarks and Geographical Indications for Agricultural Products and Foodstuffs*, ¶ 7.125, WT/DS174/R (Mar. 15, 2005).

on "place of invention, the field of technology and whether products are imported or locally produced."[205]

TRIPS also includes a national security exception.[206] However, this exception does not appear to have been invoked in any dispute settlement cases under TRIPS.

3. WTO Revised Agreement on Government Procurement ("GPA")

The WTO's Revised Agreement on Government Procurement ("GPA") sets out minimum requirements for government procurement systems with the aim of avoiding trade discrimination among the agreement's members.[207] Essentially, the GPA extends the GATT's disciplines on non-discrimination for trade in goods to government procurement. However, the GPA only applies to procurement by covered governmental entities listed in country-specific schedules attached to the GPA, and only to contracts whose value is above the thresholds specifically negotiated by GPA members and reflected in those schedules.

The GPA is a plurilateral trade agreement, meaning it only binds and protects those WTO members that have expressly acceded to the terms of the GPA.[208] The U.S. and many other developed countries have acceded to the GPA, but many countries have not.[209] Notably, none of the big developing countries (BRICs) are GPA signatories; in fact, only 46 WTO members are covered by the agreement.[210] Even if a country has acceded to the GPA, the terms of the GPA only apply to covered procurements.[211] For each country that has acceded to the GPA, a set of annexes are available that describe exactly which entities are covered.[212] For example, the U.S. has acceded to the GPA, but not all states have agreed to be covered by its terms, and many states have agreed to bind only specific state agencies or entities. Most federal agencies are covered by the GPA, but not all transactions by those agencies are covered.

While there is a possibility that the GPA could impact the ability of a governmental agency to purchase goods or supplies from a foreign firm, the applicability

---

[205] TRIPS, art. 27.1.

[206] TRIPS, art. 73.

[207] *See Agreement on Government Procurement*, WTO, https://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm (last visited July 24, 2015).

[208] *See id*.

[209] *See Agreement on Government Procurement: Parties, Observers and Accessions*, WTO, https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm (last visited July 24, 2015).

[210] https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm.

[211] Revised Agreement on Government Procurement ("GPA") Art. II (2012).

[212] *See Agreement on Government Procurement: Coverage Schedules*, WTO, https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm (last visited July 24, 2015).

of the GPA would have to be determined on a case by case basis depending on factors such as the national origin of the firm, the governmental entity at issue, and whether the transaction is covered. Even if a purchase by a governmental entity violated the terms of the GPA, the only recourse available would be for another member of the GPA to file a complaint against the offending party under the WTO dispute settlement procedures, which is very rare.

4. WTO General Agreement on Trade in Services ("GATS")

The General Agreement on Trade in Services ("GATS") imposes both general obligations and specific commitments on its members. The general obligations of the GATS apply to any government measure affecting any service, regardless of whether the member has undertaken a commitment for that particular service.[213] Similar to the GATT, the GATS requires WTO members to extend MFN treatment to service providers from all other WTO members.[214] Additionally, the GATS requires transparency in trade in services.[215] Along with the general obligations imposed by the GATS, each member negotiates specific commitments on a service-by-service basis.[216] The telecommunications sector requires special commitments from the member countries because the use of telecommunications infrastructure for so many other sectors can have large economic and national security implications.[217] Similar to the GPA, the obligations provided in the GATS apply only to the telecommunications services that a member incorporates in their schedules.[218] Accordingly, similar to the GPA, while it is possible that the GATS could impact the procurement of foreign owned telecommunications services, that would have to be determined on a case by case basis. Security-related ICT measures could also implicate service sectors other than telecom—for example, computer and related services.

5. WTO Agreement on Technical Barriers to Trade ("TBT")

Under the WTO Agreement on Technical Barriers to Trade (TBT),[219] WTO members must ensure that their technical regulations and standards, and associated conformity assessment procedures, meet certain requirements so as to not create

---

[213] *See* MARK K. NEVILLE, JR., INTERNATIONAL TRADE LAWS OF THE UNITED STATES ¶ 14.03 (2015).

[214] *See id.*

[215] *See id.*

[216] *See id.*

[217] *See* Taunya L. McLarty, *Liberalized Telecommunications Trade in the WTO: Implications for Universal Service Policy*, 51 Fed. Comm. L.J. 1, 7 (1998).

[218] *Id.* at 9.

[219] *See* WTO Agreement on Technical Barriers to Trade, https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm (last visited July 8, 2016).

unnecessary obstacles to trade. Those requirements include MFN and national treatment.[220] WTO members also must ensure that technical regulations, standards and conformity assessment procedures are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade.[221] Where international standards exist or their completion is imminent, they must be used as a basis for national technical regulations and domestic standards unless deemed ineffective or inappropriate to fulfill the legitimate objectives pursued.[222] Similarly, international recommendations on conformity assessments must be used as a basis for national conformity assessments unless they are ineffective or inappropriate.[223]

The TBT Agreement also contains a number of procedural safeguards to ensure its requirements are met. For example, where a relevant international standard or guide on conformity assessments does not exist or the content of a proposed national technical regulation, standard or conformity assessment is not in accordance with the relevant international standard or guide and the national measure may have a significant effect on trade, then other WTO members must have the ability to review and provide input on the draft national standard or conformity assessment.[224] Any draft standard is subject to comments by other WTO members, which must be taken into account. [225] With security related measures, it is often unclear, at best, whether the regulatory authority even considered comments submitted by industry. In addition, to prevent surprises and ensure timely compliance, WTO members need to promptly publish final technical regulations, standards and conformity assessments.[226]

6. WTO Security Exceptions

While the WTO agreements described above place limitations on the authority of member states to impose discriminatory requirements or prohibitions on trade in ICT products, the so-called "essential security exception" may permit such measures when justified on grounds of national security. A number of WTO agreements including the GATT contain carve-outs that permit WTO members to take actions on national security

[220] *Id.* Art. 2.1, 5.1.1; Annex 3, Par. D.

[221] For technical regulations, this means they cannot be more trade-restrictive than necessary to fulfil a legitimate objective, which include national security requirements; the prevention of deceptive practices; protection of human health or safety, animal or plant life or health, or the environment. For conformity assessments, this means they shall not be more strict or be applied more strictly than is necessary to give the importing Member adequate confidence that products conform with the applicable technical regulations or standards. *Id.* Art. 2.2, 5.1.2; Annex 3, Par. E.

[222] *Id.* 2.4; Annex 3, Par. F

[223] *Id.* Art. 5.4.

[224] *Id.* Art. 2.9, 2.11, 5.6; 5.8; Annex 3, Par. L-O.

[225] *Id.* Annex 3, Par. L-N.

[226] *Id.* Art. 2.11, 5.8; Annex 3, Par. O.

grounds that otherwise would be inconsistent with their obligations under the agreements. For example, GATT Article XXI provides:

> *Nothing in this agreement shall be construed*
>
> *(a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or*
>
> *(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests*
>
> (i) *relating to fissionable materials or the materials from which they are derived;*
>
> (ii) *relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;*
>
> (iii) *taken in time of war or other emergency in international relations; or*
>
> *(c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security*.

Unlike some other exceptions in the WTO Agreements, Article XXI permits states to define their own "essential security interests" and therefore the scope of the provision is potentially quite broad. Article XXI has been used by countries as a justification for imposing trade sanctions against other countries with which political or military tensions had escalated, as it permits all contracting parties to "tak[e] any action which it considers necessary for the protection of its essential security interests,"[227] so long as one of the factors set out in (b)(i) – (iii) also applies. This provision has been invoked, for example, by the United States to justify its blockage of Cuba and to prohibit trade between the United States and Nicaragua.[228]

There has been very limited experience with GATT Article XXI in dispute settlement so the standard of review is subject to debate. Between 1947 and 1995 there was only one case where a GATT panel considered a measure justified under Article XXI:(b)(ii). Measures taken under Article XXI:(b)(iii) were discussed by the contracting

[227] GATT art. XXI.

[228] *See* Bhala, *supra* note 78, at 265.

parties in eight instances. Since 1995 and the formation of the WTO there have been invocations of Article XXI in at least two WTO disputes (Nicaragua in 2000 and India in 2003), which did not reach the panel stage. Both these disputes have stayed at the consultation level.

The U.S. government has taken the position in the past that it has full *and* unreviewable discretion to assert GATT Article XXI. But it is unclear whether this comports with the text of Article XXI(b), which only applies in three enumerated sets of circumstances. Furthermore, at least some WTO members would question an attempt to assert Article XXI in a way that clearly revealed industrial policy motivations. Sweden, for example, tried to use GATT Article XXI to block imports of shoes, arguing it needed to protect its domestic shoe industry in case of war, but eventually abandoned the argument when GATT parties showed their skepticism of its essential security assertions.[229] No WTO member has invoked Article XXI within the dispute settlement process to justify discriminatory treatment of foreign ICT products.

Certain other WTO agreements contain provisions related to national security. The WTO Agreement on Technical Barriers to Trade ("TBT Agreement"), however, has a national security-related exemption that has a different approach and does not vest as much discretion in the government asserting the exemption. The TBT Agreement states, "Members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. For this purpose, technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective," one of which includes "national security" (Article 2.2). Missing from this language is the broad discretion in Article XXI vested in GATT parties on how they can protect the essential security interests specifically listed in that article. Instead, under the TBT Agreement, the Members have the burden to ensure that any technical regulation prepared, adopted or applied for national security purposes is "not more trade-restrictive than necessary to fulfil [that] legitimate objective." To our knowledge, to date no Member State has invoked Article 2.2 to justify a discriminatory regulation, ICT related or not. However, the non-discrimination requirement in the TBT Agreement has been successfully used multiple times to exert pressure on China, India and other WTO members to abandon or refine problematic draft ICT regulatory measures that were allegedly based on security concerns.[230]

---

[229] *See* GATT, L/4250, p.3 (https://www.wto.org/gatt_docs/English/SULPDF/90920073.pdf)
See GATT , L/4254, p. 17-18 (https://www.wto.org/gatt_docs/English/SULPDF/90920091.pdf)

[230] In August 2007, China notified to the TBT Committee a series of 13 proposed technical regulations relating to information security for various information technology products, primarily software. The proposed regulations appeared to mandate the use of Chinese national standards on encryption, which would have likely deviated from recognized international standards. In response to the invocation of TBT Article 2.2, China clarified at the 2009 JCCT that the 13 categories of information security products applied only to products procured by Chinese government agencies. See https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2009/october/us-china-joint-commission-commerce-and-trade

7. OECD Guidelines and Principles

In addition to the binding requirements of the trade agreements described above, the Organisation for Economic Cooperation and Development ("OECD") has promulgated relevant non-binding guidelines that address restrictions on foreign-origin ICT products and investments based on national security grounds. Most relevant, the "Guidelines for Recipient Country Investment Policies Relating to National Security" (the "Guidelines") encourage governments to adhere to the following principles in their laws and policies toward foreign investors:

- **Non-discrimination.** The Guidelines emphasize first and foremost that "government should be guided by the principle of non-discrimination." Accordingly, "governments should rely on measures of general application which treat similarly situated investors in a similar fashion." Where general measures are inadequate to protect national security, "specific measures taken with respect to specific investments should be based on the specific circumstances of the individual investment which pose a risk to national security."

- **Proportionality.** Restrictions on investments based on national security should "not be greater than needed to protect national security and they should be avoided when other existing measures are adequate and appropriate to address a national security concern."

- **Accountability.** Governments should maintain appropriate procedures, including internal oversight, legislative oversight, regulatory impact assessments, and "requirements that important decisions (including decisions to block an investment) should be taken at high government level should be considered to ensure accountability of the implementing authorities.[231]

- **Transparency and predictability.** Nations' laws and regulations "should be as transparent as possible so as to increase the predictability of outcomes."

These OECD guidelines are helpful but do not appear to be robust enough to address emerging ICT regulatory issues, and to our knowledge, have not been sufficiently or effectively used to preempt or resolve trade issues concerning ICT regulations based on security concerns.

* * *

[231] OECD Guidelines for Recipient Country Investment Policies Relating to National Security, adopted May 25, 2009, *available at* http://www.oecd.org/investment/investment-policy/43384486.pdf.

As the foregoing discussion illustrates, international trade agreements and guidelines reflect important principles that support equal treatment of domestic and foreign ICT goods and services. The trade agreements also include, however, potentially broad exceptions under the guise of "security," which in turn can in some circumstances provide cover to countries seeking to discriminate against foreign-owned ICT goods and services for other domestic policy purposes. The effect of such laws and regulations may be the balkanization of the ICT industry. The question, in turn, is: to what end? If countries get the balance between trade and security in this industry wrong—and err too far on the restrictive side—what are the costs? The next section takes perhaps the most aggressive actor in this area—China—and seeks to examine the costs associated with efforts to develop and enforce localization requirements.

Part II: Assessing the Welfare Costs of Balkanizing the ICT Industry: The Case of China

Globalization facilitated by dissemination of ICT products and services reshaped cross-border economic flows and other interconnections around the world, delivering significant welfare effects and expanded economic growth. Yet, as the foregoing discussion demonstrates, there are significant pressures on the continued expansion of such interconnections, and risk that some countries could seek to retreat to a more "nationalized" Internet and ICT sector. This section of the report seeks to estimate how a reverse of that process specific to the information and communications technology sector would affect economic welfare in China. We chose China as a case study because of its size, rapid transformation, and major pendulum swings in policy orientation. China experienced incredible economic growth for many years, driven by accession to the WTO and opening its doors to foreign investments and products. But today's "growth strategy" appears to include centralized and expansive plans to detach from global ICT supply chains, a policy course we refer to as "ICT deglobalization."

A. The Gains from Globalization

This sections describes the phenomena associated with globalization; the economic flows driven by them—such as trade, investment, cross border R&D, and technology transfers; and the welfare outcomes related to those flows. We examine these dynamics in the context of globalization generally, the role of ICTs in globalization, and with regard to ICTs and globalization in China specifically. In the following section we then employ a quantitative model to explore the magnitude and direction of economic welfare effects in terms of gross domestic product (GDP) and gross domestic consumption ("absorption") caused by an ICT deglobalization scenario for China. There are factors that such a modeling exercise measures only imperfectly, and others that it does not measure at all. After reviewing the quantitative results, we explore these other economic considerations qualitatively.

1. Globalization and Economic Gains

Globalization typically refers to the increased flow of trade, investment, people, technology and intellectual exchange across national borders. Importantly, these flows largely result from two phenomena: (i) a reduction of policy interventions such as tariffs on trade and restrictions on investment and people that impede flows of commerce which would otherwise take place; and (ii) technological innovations that reduce the costs associated with taking advantage of those economic flows. These reductions in policy distortions and increases in technology flows make it possible to access comparative advantages and economic endowments in different parts of the world, and thus incentivize global flows of commerce in pursuit of new commercial advantages and opportunities to profit. Globalization multiplies the potential for economic growth

found within individual nations. It has been a defining global force over the past half century, reshaping the economic landscape, as well as political and security conditions.

Globalization is not a new story: it stretches back well before the modern period. Driven by the interplay between commercial interests and technological development, national trade and investment links expanded far afield in many periods of human history. The patterns of global connectedness evident today can be traced to the industrial revolution of the 1870s,[232] the rise of trans-national merchant banking and foreign investment corporations in 17th century Europe, and even the ancient Silk Road networks maintained by Persian and other middlemen over the thousands of miles between Europe and East Asia. It has not been a one-way process, and at times has reversed.[233] Such reversals have arisen when nations or regions chose to decouple from the rest of the world for ideological reasons (e.g., China after 1949, Iran after 1979), as a result of periods of war or imperial collapse, or due to the devastation wrought by pandemic diseases. As a result, globalization has seen ebbs and flows over the millennia, rather than a constant progression. It is fitting that a comprehensive review of global commerce since the year 1000 describes the post-WWII recovery of international commerce to previous levels not as globalization, but re-globalization.[234]

Since the mid-20th century the economic flows characteristic of globalization have reached new heights, driven by policy convergence toward economic openness and new innovations in information and communications technology, transportation and other sectors. Data on these flows is used to describe the extent of globalization. Figure 1 summarizes the growth of cross-border flows of trade, direct investment, and portfolio investment since 1961 to reflect the acceleration in globalization over the past five decades. The world's advanced economies are generally working to increase economic flows and deepen connections, as demonstrated by the proliferation of international economic agreements (see Figure 2).

---

[232] Ferreira, Pedro Cavalcanti, Samuel Pessôa, and Marcelo Rodrigues dos Santos. "Globalization And The Industrial Revolution." *Macroeconomic Dynamics* 20, no. 03 (2016): 643-666.

[233] Historian Angus Madison's *The World Economy: A Millennial Perspective* is considered a seminal assessment in this literature. http://www.oecd.org/dev/developmentcentrestudiestheworldeconomyamillennialperspective.htm

Also see: Bordo, Michael D., Alan M. Taylor, and Jeffrey G. Williamson, eds. *Globalization in Historical Perspective*. University of Chicago Press, 2007; and Deese, David A., ed. *Globalization: Causes and Effects*. Ashgate, 2012.

[234] Findlay, Ronald, and Kevin H. O'Rourke. *Power and Plenty: Trade, War, and the World Economy in the Second Millennium*. Vol. 51. Princeton: Princeton University Press, 2007, Chapter 9.

Figure 1: Increases in Global Flows[235]
USD Trillions

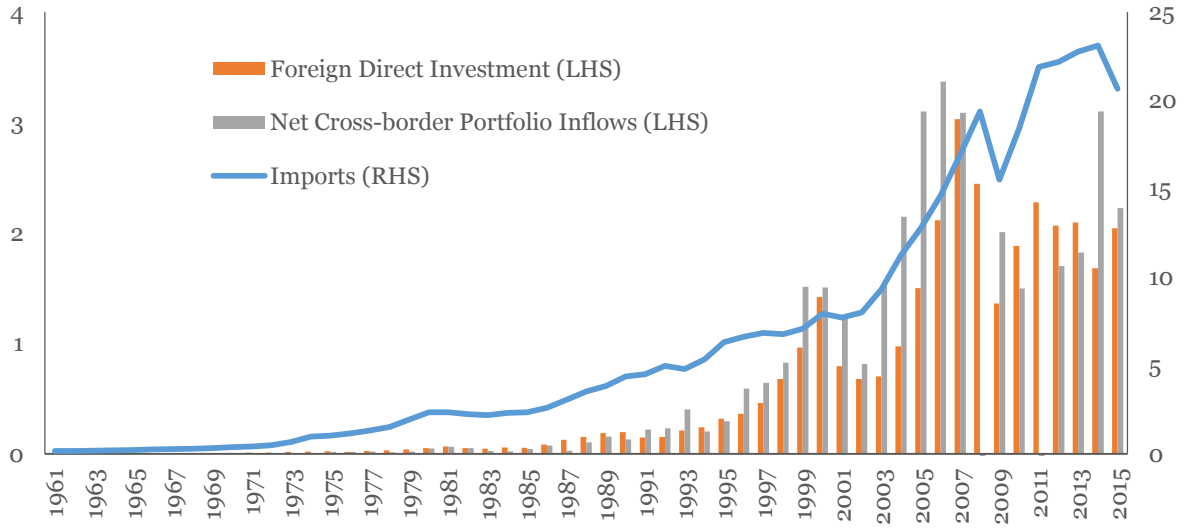
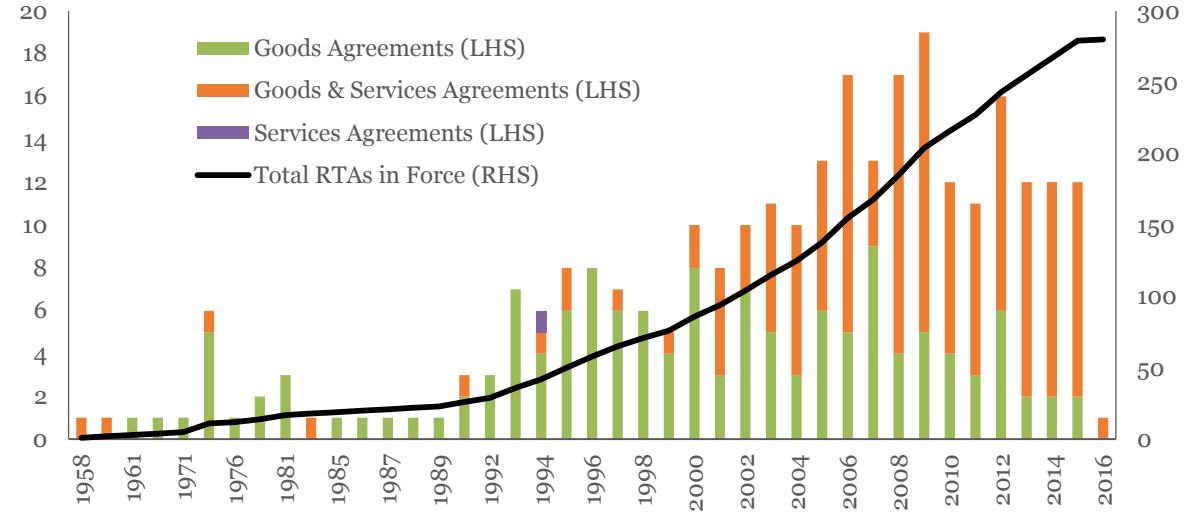


Figure 2: Global Increase in Trade Agreements[236]
Number of Regional Trade Agreements



[235] Source: World Bank, International Monetary Fund. Net cross-border portfolio investment is calculated using IMF Balance of Payment statistics and is a measure of annual global net cross-border debt and equity investment inflows. It is not a measure of market turnover, and excludes financial derivatives and other investments.

[236] Source: World Trade Organization. The bar chart details the breakdown of RTAs brought into force in a given year, while the line is a sum of all RTAs in force. Often, goods agreements are supplemented with a services agreement years later. In these cases, the RTA is classified as a goods & services agreement and counted in the year it was updated.

Policies and technologies evolve, giving rise to new commercial flows and activity, and this in turn leads to a new level of economic welfare. There are competing schools of thought about measuring that economic welfare. An altered flow of trade and investment among nations creates both winners and losers, and inequality in the distribution of gains is hotly debated. Moreover, the environmental, social, cultural and political implications of globalization are difficult to reflect in standard economic models of estimating welfare effects. At the same time, there is strong evidence that broader measures of human development improve along with the standard measures of economic welfare employed by researchers estimating the gains associated with globalization. World Bank economists calculate that less developed nations integrating with the world see per capita incomes rise three-and-a-half times faster than non-globalizing nations, with gains benefitting the poor in those nations, not just elites.[237] A literature review and calculations by a group of private economists estimate that world gross domestic product (GDP) is more than 7% higher—roughly $5.5 trillion better off—thanks to the course of global integration that has prevailed since the apogee of protectionism in the 1930s.[238] It is calculated that more than $9,000 of a typical American household's annual buying power has resulted from globalization.[239]

Our objective in this study is to assess the welfare gains or losses dependent on ICT globalization, but it is important to understand the commercial channels by which globalization gives rise to that welfare. With falling trade tariffs and transactions costs to take advantage of competitive inputs abroad (either products or labor), firms can lower their own production costs and input costs for what they produce, generating more value for consumers. In a global economy there are greater opportunities to specialize on comparative advantages, while embracing far flung supply chains for inputs more efficiently produced by others. As a result, total potential output—or the *production possibility frontier* in economist terms—goes up. Household consumers see lower prices and a wider selection of products. Export opportunities, and the level of investment—especially in innovation—generally rise. Especially for less developed nations, inclusion in globalization means a rapid increase in the introduction of new technologies and management knowhow.[240]

Beyond higher investment and consumption today, technology diffusion and adjustment to it drive improved welfare from productivity effects tomorrow and in the

---

[237] Dollar and Kray present these findings in *Growth is Good for the Poor* (2002), and update them in *Growth Still Is Good for the Poor* (2013, with Tatjana Kleineberg). The International Monetary Fund (2008) summarizes this research and offers a useful *Overview*, available at: https://www.imf.org/external/np/exr/ib/2008/053008.htm

[238] Bradford, Scott C., Paul L.E. Grieco, and Gary Clyde Hufbauer. "The payoff to America from global integration." *The United States and the World Economy: Foreign Economic Policy for the Next Decade* (2005): 65-110

[239] Figures adjusted for inflation.

[240] Keller, Wolfgang. "International technology diffusion." *Journal of Economic Literature* 42, no. 3 (2004): 752-782.; Luttmer, Erzo GJ. "Technology diffusion and growth." *Journal of Economic Theory* 147, no. 2 (2012): 602-622.

future.[241] With larger markets to sell to and more competitive pressure, firms with higher productivity thrive and double down on investment, whereas unproductive firms stop wasting resources, bolstering productivity growth. When technology investments are made they boost GDP through capital formation; thereafter, the absorption of new tools boosts the efficiency of production, swelling output beyond what can be accounted for from mere input growth. This contribution is reflected in what economists call *total factor productivity* (TFP).

Many of the productivity gains characteristic of globalization depend on openness to financial flows and foreign direct investment (FDI), not just trade. While firms will export products from afar, they are unlikely to deploy production technologies if they cannot invest. And global capital flows are enormous today, and can permit a small economy such as Ireland to bat much above its weight based just on locally available capital. Many of the world's most transformative technology companies today resulted from cross border access to capital markets in other nations, such as NASDAQ. For host nation consumers meanwhile, the physical presence of a foreign invested competitor, not just locally branded products, maximizes competition and welfare gains. In sum, FDI increases investment in fixed capital, prompts technology upgrading, redoubles attention to consumer interests, and spurs innovation.[242]

Globalization is no assurance of welfare,[243] any more than a faster car guarantees reaching a destination more quickly and safely: it depends on how it is used. By reducing the costs of shifting production structures and products around a nation or internationally, globalization benefits those with skills and mobility, and consumers; but that doesn't include everyone, and this reality has fueled debates and will continue to do so.[244] Opening up an economy and integrating it with global industries must come with attention to education and adaptability if it is to be more gainful than disruptive.[245] But assuming these well-understood policy imperatives are addressed, the evidence of ultimate gains from globalization is strong: national production (GDP), gross national

[241] McMillan, Margaret S., and Dani Rodrik. *Globalization, Structural Change and Productivity Growth*. No. w17143. National Bureau of Economic Research, 2011.

[242] For a thorough review, see: Hayakawa, Kazunobu, Tomohiro Machikita, and Fukunari Kimura. "Globalization and productivity: A survey of firm-level analysis." *Journal of Economic Surveys* 26, no. 2 (2012): 332-350. Available at: http://www.ide.go.jp/English/Publish/Download/Dp/pdf/252.pdf

[243] Chen, Yu-Fu, Holger Görg, Dennis Görlich, Hassan Molana, Catia Montagna, and Yama Temouri. *Globalisation and the Future of the Welfare State*. Institut für Weltwirtschaft an der Universität Kiel, 2014.

[244] For instance Bradford, Grieco, and Hufbauer, "The payoff to America from global integration," presents a strong summary of various lines of analysis on the gains from globalization and a generous estimate of its value, while [Bivens, Josh. "Globalization, American Wages and Inequality." *Past, Present and Future. Economic Policy Institute Working Paper* 279 (2007).] demonstrates the lines of attack on those analyses and propose more conservative estimates of the gains.

[245] See McMillan and Rodrik (2011), *Globalization, Structural Change and Productivity Growth*.

consumption, and trade-related welfare gains depend to a considerable degree on globalization today.

2. Globalization and the ICT sector

Throughout history the spread of technology has fueled globalization. Technological advances have been both the trigger and means of globalization: consider ship building and other transport innovations, food preservation techniques critical to crossing ancient trade routes, or banking modalities which facilitated commerce across great distances. Technology transfer—intended or not—was also a *result* of this widening interconnectedness, as newly exposed consumers learned of products and innovations they had never imagined, and undertook to acquire or replicate them.

Information and communications technologies have played a predominant role in the modern era. The telegraph and telephone (invented 1835 and 1876 respectively; and both in turn reliant on innovation in electricity production) are the not-so-distant ancestors of todays interconnected world, and demonstrated the transformative power of communications technologies. With each successive generation of ICT, the lag between invention and adoption in less developed locales has shortened. The telegraph didn't play a role in sub-Saharan Africa for 30 years after its debut; the telephone showed up within a decade. Two years after the first cell phone call in 1973 the technology was at work in Africa.[246] This acceleration in the diffusion and uptake of ICT is inseparable from the story of globalization today. This is particularly important because ICT is a general purpose technology that adds not only its own weight to the output of a nation—such as when new semiconductor factories are built or personal computers are sold—but has a powerful multiplier effect on the value and productivity of many other industries. In the case of developing nations this often includes industries that couldn't take root without the enabling benefits of ICT, which reduce information gaps across great distances and make it possible to distribute production chains more broadly.[247]

The ICT sector was (1) the initial trigger for much of today's globalization, (2) a major component of the growth in flows (i.e., investment in ICT production and consumption of ICT products), and (3) the embodiment of elevated societal welfare that has resulted. First, improved capacity and radically lower costs for global communications, coordination, and information transmittal made it possible to conduct business worldwide to a previously unseen degree. Compelled by the opportunities created by falling communication and transportation costs, governments around the world undertook complementary policy reforms, such as tariff reductions, tax

[246] Comin, Diego, and Bart Hobija. "An exploration of technology diffusion." *The American Economic Review* 100, no. 5 (2010): 2031-2059. http://www.hbs.edu/faculty/Publication%20Files/08-093.pdf.

[247] Biniazi, Kourosh, Rohallah Ghahremani, Hamidreza Alipour, S. Z. Talebian, and Samane Akhavan. "Position and role of ICT in supply chain management (SCM)." *Australian Journal of basic and Applied Sciences* 5, no. 8 (2011): 827-831.

incentives, investment opening and current account liberalization. Second, this set the scene for firms to distribute production around the world according to dispersed comparative advantages for each component part or process. This redistribution of manufacturing pushed down prices and amplified distribution of products and hence economies of scale, and the heightened capital investment and consumption around these value-added enhancing products were a boon, especially for dozens of emerging economies which found an on-ramp to global participation.

Third, and at least as important to the global growth equation, were the productivity gains made through worldwide absorption and use of ICTs. Three decades ago leading economists quipped that they could see the computer age everywhere except in productivity statistics.[248] By the early 2000s that paradox had been resolved, and economists could conclude that in the economies where ICTs were put fully into use they were nearly doubling the productivity growth rate, and moreover, most of this improvement was not in the ICT producing industries themselves but in all manner of other sectors that were consumers of ICT goods and services. In the U.S., TFP growth rose from 0.4% in the pre-ICT boom years of the 1970s and 80s to 1.6% after 1995. Since ICTs are general purpose technologies—that is, they are absorbed into and enhance the productivity of most if not all industries, and transform the economy broadly in a sustained manner—these gains were spread far beyond the tech sector—in fact 63% of U.S. TFP gains experienced in these years accrued to non-ICT industries.[249] [250] With a time lag to reflect the upfront investment costs and policy adaption required to accommodate their potential, ICTs delivered a global revolution in productivity gains well beyond the advanced economies. This positive productivity shock is still ongoing. In fact, in many ways it is just getting started. A reverse shock that dismantled the international production chains, economic flows and interconnectedness that were the offspring of globalization would weigh heavily on our dependent variable—the economic welfare that accrues to citizens worldwide today—for a nation that took such a route. And if a departing player were big enough, as China is, the deleterious effects for the system as a whole would be large, and felt in GDP, in national consumption, and terms of trade.

3. ICT Globalization and China

China's relationship to the forces of globalization described above, and especially to the role of the ICT sector, was key; and its stake in the economic welfare effect that resulted was huge. China began in 1978 in virtual autarky from the world economy—

[248] This was Robert Solow's "productivity paradox", observed in 1987. Robert Solow, "We'd better watch out", New York Times Book Review, July 12, 1987, page 36. Available at: http://www.standupeconomist.com/pdf/misc/solow-computer-productivity.pdf

[249] Economic Report of the President (2001), Chapter 1, pp 26-33.

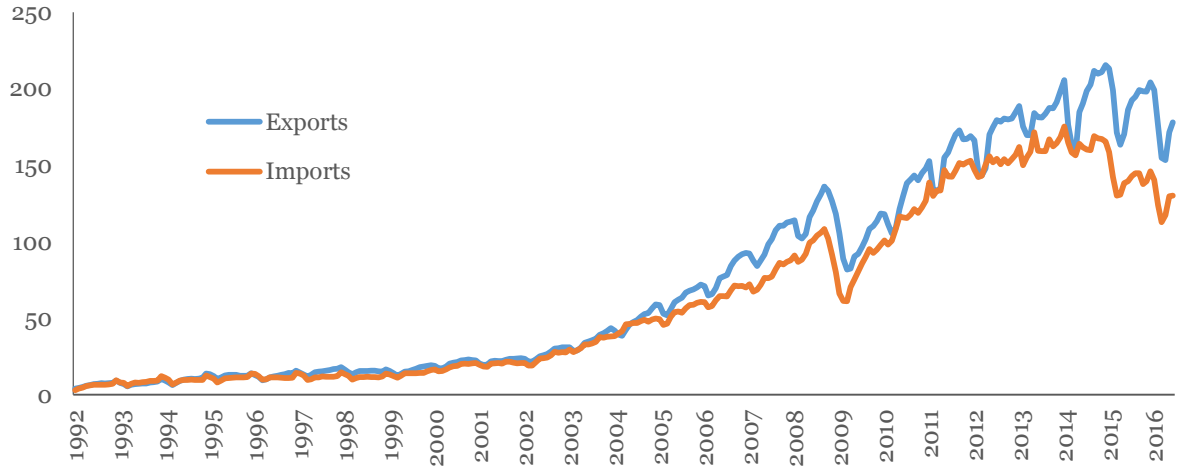
[250] Boyan Jovanovic and Peter L. Rousseau, 2005. "General Purpose Technologies," in: Philippe Aghion & Steven Durlauf (ed.), Handbook of Economic Growth, edition 1, volume 1, chapter 18, pp. 1181-1224, Elsevier.

that is, it maintained policy barriers to the world economy that walled it off from participation, and within those walls it defeated the logic of internal economic flows that could generate economic welfare. In the post-Mao era it reformed domestic policies to permit commercial rationalization, and more importantly for the global context it also reformed border trade and investment policy distortions that prevented outsiders from taking advantage of its enormous endowments of labor—first as a means of reducing low-skill, labor-intensive manufacturing costs, and later as a source of consumer demand and network externalities.

China's policy choices impelled massive international trade and direct investment flows to take advantage of these new factors. The country's timing was propitious, as ICT innovation over the first decades of China's reform both drove international producers to shift assembly and production activities to take advantage of China's labor and other cost advantages, and permitted non-ICT industries such as apparel and other light manufacturing to manage production chains extending into China while keeping transactions costs low, quality control reasonable, and time to market competitive. The backwardness of many high-technology industries in China meant that incumbent firms—few in number at the time—were inclined to enter into joint ventures with foreign players, and to leapfrog generations of ICT infrastructure and move more quickly to the next generation.

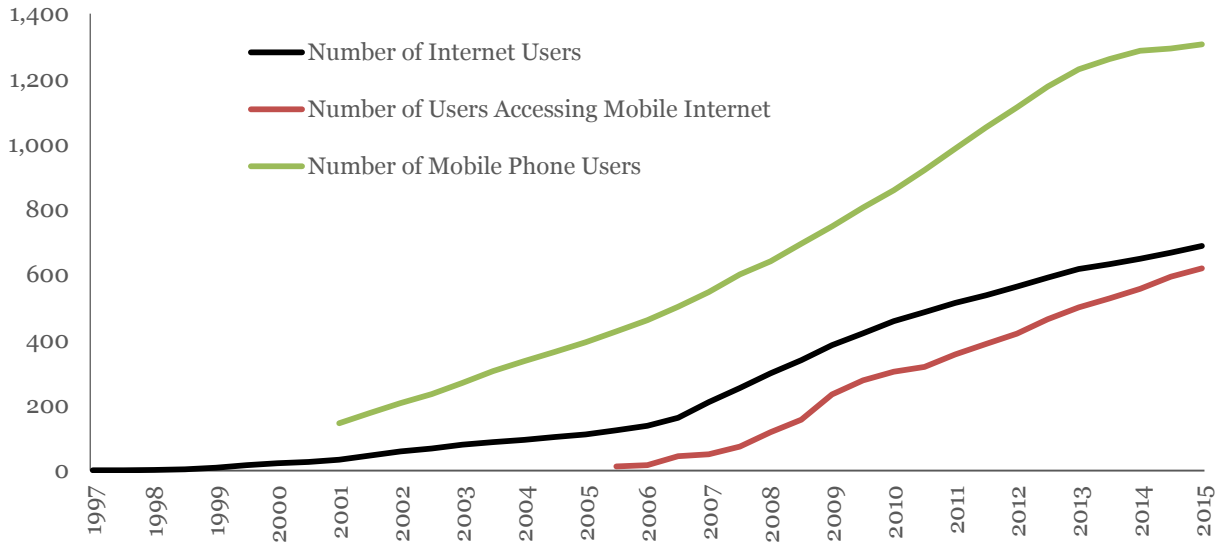
China's rise and the modern era of globalization are inseparable phenomena in many respects. The unprecedented growth in China-related flows of cross-border trade and investment facilitated by policy reform has been endlessly discussed. The prodigious deepening of ICT use and the manner in which it has transformed the marketplace—and society—within China has been the subject of numerous reports.

Figure 3: China's Increasing Trade Flows[251]
USD Billion, Three Month Moving Average



[251] China General Administration of Customs, CEIC

Figure 4: China's Increasing Use of Technology[252]
Millions of Users



Looking back over three decades of Chinese GDP growth averaging 10%, globalization and ICT had a starring role. Figure 5 shows the IMF's attribution of China's growth to annual growth of three factors: labor force growth, capital stock investment and TFP. China's achievement clearly depended on capital deepening and productivity. The build-out of ICT-related capital stock including telecommunications and internet infrastructure, diffusion of computers and control systems, and myriad other assets were significant components of total capital investment. Fixed asset investment in one ICT goods sector alone, Computer, Communication & Other Electronic Equipment, and one service sector, Information Transmission, Software and Information Technology Service, from 2004 to 2015 amounted to more than RMB 8 trillion. Research discussed further below calculates that between 1978 and 2003 ICT investment growth averaged 26% per year.[253] Combined business revenue for the computer and telecommunications industries was roughly RMB 32 trillion over the same period.

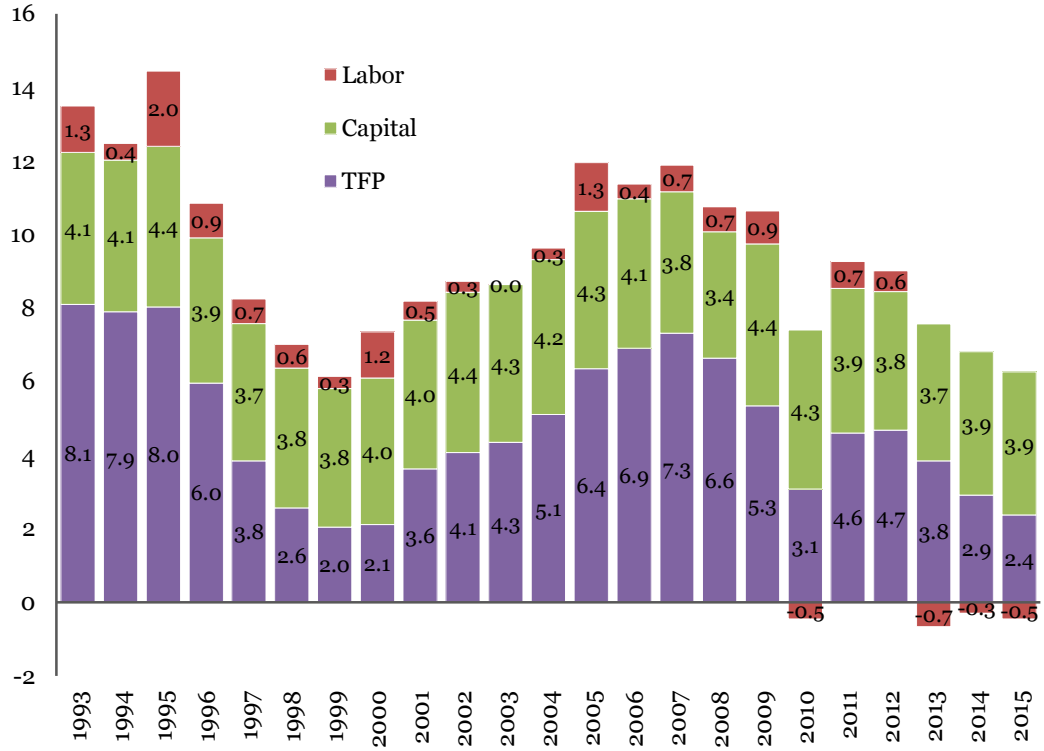
Investment in ramping up factory output of ICTs has played an important part. But an insight from research in advanced economies is critical for understanding China as well: the biggest welfare impacts from ICT come not from making advanced products

[252] Source: China Internet Network Information Center, CEIC. Note: For magnitude depiction only. Chinese data likely reflect multiple accounts held by one person.

[253] Heshmati, Almas, and Wanshan Yang. "Contribution of ICT to the Chinese economic growth." *The RATIO Institute and Techno-Economics and Policy Program, Seoul National University* (2006): 1-17., p. 14

to export to others, but from adopting them and using them at home.[254] ICT is valuable in places open to reform, where leaders permit ICT to reshape the productivity and potential of their economies. The research literature validating this insight for Asia and for China in particular is copious.[255] The majority of China's output growth over the past two decades came not from putting more inputs through the doors of factories and offices, but in squeezing higher output from existing resources – TFP growth. This TFP value reflects a number of factors, but foremost among them is the level of technological prowess embedded in an economy.

Figure 5: Factor Contributions to China's Growth[256]
Percent



[254] Atkinson, R.D. and Stewart, L.A., 2013. "Just the facts: The economic benefits of information and communications technology." *Washington, DC: The Information Technology & Innovation Foundation*. Available at: http://www2.itif.org/2013-tech-economy-memo.pdf

[255] Ezel, Stephen J. and Atkinson, Robert D., 2014. "How ITA Expansion Benefits the Chinese and Global Economies," *Washington, DC: The Information Technology and Innovation Foundation*. Available at: http://www2.itif.org/2014-ita-expansion-benefits-chinese-global-economies.pdf

[256] Source: IMF, Rhodium Group

Total-factor productivity has immense implications for the future of China's growth. With a rapidly shrinking demographic dividend and increasingly unproductive uses of capital absorbing a lion's share of investment, sustaining technology-driven productivity growth in China is more important than ever. This is why many researchers have looked closely at the role of ICT in Chinese TFP growth.

Heshmati and Yang (2006) estimate that each 1% increase in China's capital investment in ICT 1978-2003 resulted in a 0.076% increase in TFP. Based on average annual ICT investment growth of 26.4%, they find that the ICT-related subcomponent of TFP growth accounted for 2% of the 5.3% total annual average TFP contribution to GDP.[257] This means about 2/5 (38%) of total TFP growth is attributable to ICT-spurred productivity, or 21.2% of *all* Chinese GDP growth. This is a big number, but it is not surprising considering that it not only includes the capital deepening effect and technology improvement but also includes the effects of resource reallocations, and reorganization effects in both ICT and non-ICT sectors. In other words as a general purpose technology, the productivity enhancing welfare impact of ICT spills over into most if not all sectors.

A number of questions remain. Is the attribution of the ICT share in Chinese TFP 1978-2003 accurate for the years since, during which informatization grew but other industrial investment went through the roof as well? Whatever the ICT share of TFP, is aggregate TFP itself still contributing close to 5 percentage points to China's GDP growth (which now hovers below 7%, instead of the near-10% earlier average)? Further, what share of China's TFP and especially ICT-related TFP is dependent on China's interaction with *foreign* firms and economies, given that some of those interactions are under strain? In order to estimate the welfare cost of ICT deglobalization for China we must first explore these questions.

There is no off-the-shelf assessment of recent changes in the weight of ICT-related factors in Chinese TFP. However, Wang and Lin (2013) show a consistent weight of 20% in total GDP growth through 2007,[258] a five year extension beyond the Heshmati and Yang analysis. Using fixed asset investment (FAI) shares as a rough proxy for China's changing sectoral intensity in the years since, we can approach this question. The ratio of FAI in manufacturing of computers, communications devices and other electronic equipment to all secondary sector (industrial) FAI has changed surprisingly little over the years, ranging from 3.8 to 4.2% between 2005 and 2015 (except for an anomaly in 2009). Relative to FAI in steel smelting and pressing (a non-ICT industry seen as the epitome of over-investment in these years) this ICT cluster has

[257] Heshmati and Yang. "Contribution of ICT to the Chinese economic growth," p. 14. There are important debates about these estimates. For example, if you believe the proper depreciation rate for China is higher than 7% (the estimate Heshmati and Yang select), then capital deepening is smaller and implied TFP growth is even higher. Based on our analysis we believe the depreciation rates and other inputs used by Heshmati and Wang are reasonable.

[258] Wang, Cassandra C., and George CS Lin. "Dynamics of innovation in a globalizing China: regional environment, inter-firm relations and firm attributes." *Journal of Economic Geography* 13, no. 3 (2013): 397-418.

seen its weight boom over these years: at the end of 2005 computer FAI was 52% the value of steel manufacturing FAI, this grew rapidly and consistently to a current ratio over 200%—computer FAI is now more than twice the annual value of steel investment. Based on these patterns it is reasonable to assume that the weight of ICT-related TFP to all TFP is today at similar or greater levels as in previous periods.

To gauge overall TFP, the IMF's 2015 Article IV evaluation for China offers a perspective on 2010-2014 trends. The IMF concludes that the TFP contribution to GDP growth has fallen off in recent years in line with headline growth, from around 3 ½ points of annual contribution to the vicinity of 2 points, down significantly from the earlier period average. This TFP decline makes sense: previous TFP levels were very high, and reflected the unusual abundance of high-impact measures readily available to policymakers, including reforms to permit private enterprise, foreign trade and investment liberalization, and capacity expansions. Regression to the mean was to be expected.[259] In addition, China's reform momentum dropped off after the early 2000s, and especially after the global financial crisis, as a combination of vested interests, self-satisfaction with high-growth, and disorientation following the global financial crisis set in. Other researchers believe current Chinese GDP growth is much lower than the officially stated 6.9%, and that a steeper fall in the TFP contribution—to near zero—is the cause.[260]

Putting these lines of inquiry together, we believe that the relative weight of ICT-factors in China's TFP performance is higher than ever, due to the fall-off in other sources of TFP growth, but that on the whole TFP growth has subsided, to levels reflected in the IMF's estimates. It is assessed that TFP is contributing 3 percentage points to GDP over the business cycle presently, with risks to the downside going forward and dependent on the quantity and quality of reform. It is estimated that 2/3 of this downsized TFP contribution depends on ICT related activity.

Finally, China's TFP has relied heavily on interaction with foreign firms and economies. This is apparent from both the record of technology transfer programs that foreign firms and governments have announced in China for decades, and also in the records of international trade and investment dispute proceedings documenting technology transfers gone awry. Disputes are not unusual for developing countries, but in China global firms were more likely to be required or pressured to transfer technology in order to facilitate their business interests there than in other, smaller economies, and so the stakes, and interdependence, are high. Research in recent years has attempted to put a more robust estimate on the weight of international technology contributions in China's rapid growth. Work by Yueh (2013) argues that in the 2000s "one-off" TFP

[259] Pritchett, Lant, and Lawrence H. Summers. *Asiaphoria meets regression to the mean*. No. w20573. National Bureau of Economic Research, 2014. Available at: http://www.nber.org/papers/w20573

[260] Wu, Harry Xu. "China's Growth and Productivity Performance Debate Revisited." The Conference Board working papers, EPWP1401, 2014. Available at: https://www.conference-board.org/pdf_free/workingpapers/EPWP1401.pdf

boosters like factor reallocation were the part that dried up, reducing growth (the off-mentioned stall in reform under Hu and Wen), while ICT-related sustained efficiency improvements (technology deepening) held up.[261] In a separate study she finds this depended on Sino-foreign joint ventures transferring technology, and that overall growth would have been 0.43 to 1% lower per year without foreign contributions to TFP.[262] That translates into roughly one-half of the ICT-related TFP growth China has enjoyed.

The IMF pegs the recent contribution of TFP to China's growth around 3%.[263] As discussed, the ICT-related part of that appears to be about 2%, 2/3 of the total. The foreign-driven share of that, in turn, is half: if all of it dried up, headline TFP would be reduced by 33%; if half the foreign ICT contribution evaporated, headline TFP would fall 17%; and if one-quarter were removed, an 8% TFP reduction could ensue. These deductions are used in the following section to calibrate a model to explore the impact of ICT deglobalization—the exclusion of foreign ICT players from China's capital stock and market—on Chinese welfare.

B. Estimating the Welfare Costs of Chinese ICT Nativization

The previous section reviewed economic welfare gains associated with globalization, and how deeply connected this process has been to innovations in information and communications technologies (ICTs). China's economic growth particularly benefited from this confluence of forces; in fact, China was the epitome of it. But just as ICT globalization has generated large economic welfare gains, reversing that integration is likely to subtract from welfare. This is not a theoretical notion: globalization has worked in reverse before—indeed, within living memory of many Chinese who lived through the intentional autarky pursued by the Communist Party during its first three decades holding power, sometimes partial, sometimes nearly-complete.

Trade economists use economic models to gauge the benefits of globalization, estimating the positive and negative welfare effects that result from lower tariffs, increased investment in ICT, and other elements of deepening economic interconnection. Over the past few decades, there has been little reason to use these models to estimate the same effects in reverse. At the beginning of the 21st century there was little reason to believe that countries would willingly close themselves off.

[261] Yueh, Linda. "What drives China's growth?" *National Institute Economic Review* 223, no. 1 (2013): R4-R15.

[262] Van Reenen, John, and Linda Yueh. "Why Has China Grown So Fast? The Role of International Technology Transfer." *CEP discussion paper* 1121 (2012).

[263] Staff Report for the 2015 Article IV Consultation (2015). *People's Republic of China*. International Monetary Fund, p. 39. Available at: https://www.imf.org/external/pubs/ft/scr/2015/cr15234.pdf

The political and economic developments, however, have led many to question whether or not international economies were "deglobalizing," actively breaking down the networks that had spurred growth in the past and directly increased the welfare benefits of their citizens. In light of the pressures on the ICT sector and the policies being pushed in China to "nativize" all ICT production and services, as described in Part I above, this paper uses trade models to explore the increasingly less hypothetical: what would happen if policies that shield domestic suppliers led to the secession of ICT engagement between China and the rest of the world?

1. Modeling China in Global ICT production

To analyze the impact of ICT nativization, we employ the data and computable general equilibrium (CGE) model for the world economy available through the Global Trade Analysis Project (GTAP).[264] GTAP is a global network of researchers and policy makers conducting quantitative analysis of international policy issues. The network maintains a consistent set of global economic data and Input-Output tables. The current release, the GTAP 9 Database utilized for this analysis, features 2004, 2007, and 2011 reference years as well as 140 regions for 57 GTAP commodities.[265]

This database is used to calibrate the standard GTAP CGE model which is a multi-region, multi-sector, CGE model, assuming perfect competition and constant returns to scale. Bilateral trade is handled via the Armington assumption.[266] A CGE model is best suited to analyze the impact of trade policy shocks as it can capture not just the direct impact of trade policy changes, a shift in the trade pattern of affected sectors and regions, but also the indirect effect on other sectors and broader economic consumption and welfare. The main channels for policy shock transmission in the model are changes in the relative prices of goods and service, and in income flows to consumers.

This paper utilizes the 2011 reference year data and aggregates the 140 regions in GTAP to four regions—China, EU, United States and rest of world (ROW)—in order to make the modeling work easier. This choice reflects our interest here in impacts on China, rather than on China's trading partners. Despite incorporating production and consumption for 57 product groups and commodities, GTAP does not have a dedicated information and communication technology (ICT) good & service subcategory in its standard database. Instead, ICT is distributed among three groups of products in GTAP:

1. Electronic equipment, which includes all ICT related goods

[264] GTAP is coordinated by the Center for Global Trade Analysis in Purdue University's Department of Agricultural Economics. For more details see here https://www.gtap.agecon.purdue.edu/default.asp

[265] See Appendix 5 for the list of sectors and regions in our version of the model.

[266] Further model documentation can be found here. https://www.gtap.agecon.purdue.edu/models/current.asp

2. Business Services, which includes ICT-related services

3. Communication, which includes ICT-related services

As shown in Table 1, these categories are not perfectly aligned with an ideal definition of what belongs in the ICT category, but one is able to filter in most of what is important for this exercise, and filter-out what is extraneous. The technical appendix has more detail on the sectorial and product calibration.

Table 1: Breakdown of ICT-related Sectors

	Level 1 (GTAP Sectors)	**Level 2** (ICT and non-ICT)	**Level 3** (Further breakdown of ICT)
Goods	**Electronic goods** (includes office, accounting and computing machinery, radio, television and communication equipment and apparatus)	ICT-related electronic goods (includes computer and peripherals, communication equipment, consumer electronics, and ICT-related electronic components)	Computer and peripherals
			Communication equipment
			Consumer electronics
			Other ICT-related electronic equipment
		Non-ICT related electronic goods	Non-ICT related electronic goods
Services	**Communications** (post and telecommunications)	ICT-related services (includes telecommunications, software and information)	Communications
	Other business services (real estate, renting and business activities including software)		Software and information
		Non-ICT related services	Non-ICT related services

2. Calibrating the Model to Mimic Deglobalization, and Measuring the Results

Part 1 of this assessment described what Beijing has said about ICT deglobalization and the range of policies and practices both in China and in international use that could be involved in such a campaign. The question of how partial or complete such a digital divorce would be is unanswerable. Moreover the models available to explore the consequences of such a scenario do not offer a fine-grained ability to approximate a partial and nuanced closure of the sector. To simulate the effects of ICT nativization through our CGE model, we apply three shocks to the baseline picture of business as usual. First, we reset China's ICT import tariffs to very high levels to reflect the stoppage of ICT-related goods and services inflows associated with "de-Ciscoizing" the country with an aggressive anti-foreign ICT policy. (A search for "de-Cisco campaign" [or *Qu Sike Hua Yundong* in Chinese] on the micro-blogging service Weibo produces hundreds of results.[267]) This largely closes off China to importing foreign made ICT.

[267] See Rosen, Daniel H. and Beibei Bao, "Eight Guardian Warriors." *Rhodium Group*. Available at: http://rhg.com/notes/eight-guardian-warriors-prism-and-its-implications-for-us-businesses-in-china-2

Second, we look at the effect on China's economic performance after that trade shock, in light of assumptions about trade elasticity of substitution. Trade elasticity reflects how easy or hard it is for a nation to switch to a domestically produced alternative if denied the ability to import a like foreign made product. If denied imported garments, China could switch to domestic substitutes fairly easily; if denied foreign bauxite, the task of switching would be far harder because domestic supplies are finite. The substitutability between Chinese and foreign ICT is unclear: policy rhetoric from Beijing suggests China is close to the cutting edge, while many observers are skeptical. We model two trade elasticity scenarios to explore the difference: a *differentiated* ICT scenario, in which China cannot easily replace foreign inputs; and a *homogenous products* scenario, in which it can.

Third, as noted above much of the gain from ICT globalization has been shown to come not from output of technology products themselves but from subsequent productivity benefits that accrue across the whole economy. The family of CGE model we use does not calculate these productivity shocks based just on the tariff and trade elasticity variables, but rather requires us to set productivity assumptions from "outside" the model, or *exogenously*. As with trade elasticity, the question of how Chinese productivity—as reflected in TFP—would be effected by excluding foreign participation is debatable. Once again we offer a selection of scenarios, based on the literature on the relationship between Chinese TFP and foreign ICT sector participation, to promote discussion and capture the reasonable range of outcomes.

These shocks, along with the base modeling inputs, result in a variety of different outputs, two of which we feature here:

1. Gross Domestic Product (GDP): a measure of the value of all final goods and services produced in a country during a time period.

2. Absorption: a measure of an economy's gross domestic *consumption* of final goods and services within a time period. Because this reflects the consumption ability of domestic parties, and not just how much the nation can send abroad to benefit consumers elsewhere, this is a better measure of aggregate *welfare*.

The GTAP model suggests changes in exports, but intentionally nets them out with changes in imports (part of what is referred to as macroeconomic closure) in order to "squeeze" the impacts of policy changes into the domestic welfare in the forms of output (GDP) and consumption (absorption). While we do not therefore focus on the absolute value of China's trade, we can make two common sense statements: China's overall exports would be much less over time if it nativized ICT; and within trade, high-tech activity would plummet in both directions while trade in less sophisticated goods and services would make up part of the difference.

In each case below, we compare the results for China under the initial baseline scenario to economic performance after the policy shock of ICT deglobalization is imposed, under a variety of assumptions.

3. Quantitative Results

Table 2 summarizes key results from our modeling exercises exploring the impact on China from ICT deglobalization. There are four productivity shock scenarios, ranging from *no impact* to a 16% reduction in the contribution of TFP to China's headline GDP growth (in 2011—the base year—China grew 9.4%, roughly half of which resulted from productivity growth rather than growth in capital and labor inputs). In each of those scenarios, we offer both the high product substitutability case and the low elasticity case. For each of these runs of the model, we show results for GDP and absorption.

The first observation is that China ICT deglobalization affects all regions negatively in GDP and domestic consuming power terms, as the benefits of specialization around comparative advantage go into reverse. Second, these negative impacts are much more pronounced for China than for the other regions in our model. Third, impacts are quite significant in absolute value terms, not just relatively speaking. Even leaving aside likely damage to China's productivity over time, China sees a -1.77% to -3.44% reduction in GDP depending on how much foreign ICT can really be substituted by domestic producers easily. Economists would consider effects of that size to be very significant indeed. By comparison, Chinese economists have estimated the negative effect on the nation from non-participation in the TPP FTA arrangement to be –2.2% over four years;[268] and a model of China's inclusion in its biggest regional trade agreement to date, the China-ASEAN FTA, suggest output benefits of just 0.5%. As policy shocks to economic performance go, a decision by Beijing to purge foreign ICTs would be huge and costly.

Moreover it is likely that ICT nativism would have well more than a zero impact on Chinese productivity growth. Scenarios 2, 3 and 4 explore the range of likely TFP impairment. Even with homogenous ICT goods that China could quickly turn to making wholly at home (albeit at higher cost), GDP is reduced by 3.4-10.7%; if ICTs are more difficult to indigenize than Beijing thinks, a 5-12.3% reduction in trend GDP is projected. In today's US dollars, these damaged-productivity scenarios translate to between $354 billion of *annual* lost output in the 3%/homogenous products case to $1.28 trillion in the high-productivity shock scenario with hard to substitute products. The range of scenarios and assumptions permits readers with differing points of view to find results they believe to be reasonable.

[268] Vanderklippe, Nathan (2015). *For some businesses in China, the cost of exclusion from TPP is too high*. The Globe and Mail. Accessed February 22, 2016. Available at: http://www.theglobeandmail.com/report-on-business/international-business/asian-pacific-business/exclusion-from-tpp-to-cost-china-central-bank-official-warns/article26734745/

Table 2: Modeling Results of China's "Deglobalization"

		%GDP	%Absorption
No productivity shock			
Regionally Differentiated ICT products	China	-3.44%	-3.59%
	World ex China	-0.21%	-0.21%
	US	-0.34%	-0.32%
Regionally Homogenous ICT products	China	-1.77%	-1.85%
	World ex China	-0.04%	-0.04%
	US	-0.09%	-0.09%
3% productivity shock			
Regionally Differentiated ICT products	China	-5.03%	-5.25%
	World ex China	-0.22%	-0.22%
	US	-0.34%	-0.32%
Regionally Homogenous ICT products	China	-3.38%	-3.52%
	World ex China	-0.05%	-0.05%
	US	-0.09%	-0.09%
8% productivity shock			
Regionally Differentiated ICT products	China	-7.74%	-8.08%
	World ex China	-0.23%	-0.23%
	US	-0.34%	-0.32%
Regionally Homogenous ICT products	China	-6.13%	-6.39%
	World ex China	-0.07%	-0.07%
	US	-0.10%	-0.09%
16% productivity shock			
Regionally Differentiated ICT products	China	-12.30%	-12.84%
	World ex China	-0.26%	-0.26%
	US	-0.34%	-0.32%
Regionally Homogenous ICT products	China	-10.74%	-11.21%
	World ex China	-0.09%	-0.09%
	US	-0.10%	-0.09%

The other modeling output from our model to consider is absorption, or gross domestic consumption. The model suggests that for China the loss of domestic consumption power is moderately worse than output shrinkage. Deglobalization will mean, among other things, higher average prices for ICT products in China, and hence the basket of goods and services households, governments and business can acquire for the same amount of income is lower. As output goes down in the ICT industries, some resources (capital and labor) could migrate to other industries, making those products cheaper and more competitive. Many a Chinese farmer's child went from agriculture and garment stitching directly into high-tech assembly over the past decades, and that has pushed down electronics unit costs and generally lifted wages lately in other segments, hence costs of production. The reversal of that trend might be good for farming and making socks, but that is not where Beijing had intended to take the nation. Moreover, because those industries pay much lower wages, overall consumption power suffers even if a few segments see benefits.

4. Projections to 2025

These shocks, while modeled as one-off production and absorption effects, would also have long-lasting effects on the continued growth of the Chinese economy. To get a rough idea of the effect over time we use a simple methodology to cumulate impacts to 2025. In Table 3 below we compare a business as usual projection of GDP to 2025 to a pattern of growth reduced by the least disruptive scenario from our model (no productivity hit, highly substitutable ICT products). We leave aside any consideration of exchange rate changes or inflation here. For each year to 2025 in the ICT shock column, we grow prior year GDP by the baseline growth rate but then reduce the product by 1.77%. Finally, we measure the cumulative reduction from the GDP position China would have achieved if not for this annual hit on performance. The 2025 difference – almost $3 trillion – is huge. And this is assuming the most modest reduction of China's growth: a productivity shock and trade elasticity problems would very likely add to the problem. Over the course of a full decade Beijing would be paying at least $14 trillion for whatever security benefit it achieves. Perhaps only China can decide whether that is a reasonable price to pay, but one imagines that many Chinese should like to know that this is the price tag, would contemplate whether there is a cheaper way to achieve the same result, or consider whether there is a way to get more security benefit for that much money.

Table 3: Cumulating the Impacts on China's GDP to 2025

	Baseline Growth (%)	Pre-shock GDP (2015 $ billion)	Post-shock GDP (2015 $billion)	Cumulative GDP Loss (%)
2015		10,426	10,426	0.00%
2016	6.50%	11,104	10,907	-1.77%
2017	6.25%	11,798	11,384	-3.51%
2018	6.00%	12,506	11,853	-5.22%
2019	5.75%	13,225	12,313	-6.89%
2020	5.50%	13,952	12,760	-8.54%
2021	5.50%	14,719	13,224	-10.16%
2022	5.25%	15,492	13,672	-11.75%
2023	5.25%	16,305	14,135	-13.31%
2024	5.00%	17,121	14,579	-14.85%
2025	5.00%	17,977	15,037	-16.35%

5. Qualitative Comments and Unquantifiable Effects

Economic modeling is highly imperfect. The exercise undertaken here is meant to illuminate the magnitude and direction of impacts from a program of extreme ICT deglobalization. We do not claim to offer precise implications for specific technology segments. Beijing may wall off just a subset of the technology segments included in our calibrations, or permit exceptions for "qualified" foreign firms that are willing to meet certain national security standards. Rather than closing to the world as in our model, China may attempt to maintain production linkages to some nations and not others; or those nations might take the initiative and offer to choose China's side in a global ICT standards bifurcation between a U.S.-centric and China-centric platform. All of these scenarios are conceivable,[269] and could mitigate the welfare impacts for China that we project. At the same time, it should be noted that even half of the value of the middle productivity loss scenario means a 3-4% hit on China's GDP – enough to merit careful cost-benefit review in Beijing or any other capitals where such a pathway might be contemplated.

There are numerous economic elements not reflected in our modeling effort, and we point these out in order to avoid misperceptions, suggest avenues for additional research, and indicate how we think these factors might change our results. First, our modeling is not capturing dynamic effects over time. Our 2025 cumulation exercise is just adding the same sorts of impacts in the base year to subsequent years. In reality, the

[269] As noted in Part I, President Xi Jinping's speech in April of this year indicates a desire to segment foreign technologies depending on whether they are "secure and controllable," whether they can be reverse engineered, jointly developed with others, or fully developed domestically.

changes to prices, competitiveness and other factors in year one would change patterns of investment in year two, and so on. As noted above, there might be a tendency for consumers to shift consumption to product segments that did not see rising prices due to deglobalization, leading to a diversion of China from a high-tech future to a less advanced one. Such dynamic modeling was beyond the scope of this study, but is doable, and indeed worthwhile given the magnitude of expected impacts.

Second, we have not explored the employment implications of a Chinese ICT nativization program. The "foreign" products at risk from such a campaign often involve manufacturing in China, so it is not clear that "kicking them out" would create more jobs in the sector in China. In fact we assume that profound reciprocal closure to Chinese products would ensue abroad as well, reducing the potential for China's ICT sector export-oriented employment. We consider the jobs question to be an important and interesting one, and difficult to form a simple hypothesis around without more formal estimation.

Third, our modeling-set up and analysis here has focused on China, and not the effects on other countries, scenarios involving rival blocks of nations instead of just China v. World (three regions). We note that the U.S. takes a hit in this modeling as well, though much smaller than China's because it remains open to the rest of the world. The regional and global implications of nativization are not limited to choices made in China however. As discussed in the first portion of this study, other nations are contemplating retrogressive policies as well, and some may initiate or accelerate such steps in light of what China does.[270]

Fourth, it is entirely likely that we are underestimating the degree of service sector loss bearing down on China if it chooses to go this route. It is generally understood that CGE models, including GTAP, are mediocre at capturing the dynamics of the services industries, which make up a large part of the ICT cluster story. Much of the value found at the ICT cutting edge is difficult to estimate in national income accounting data making up GDP itself, let alone the trade data fed through GTAP. Both as an engine of jobs, output and innovation itself and a general purpose technology machine benefitting all sectors, ICT services are hugely important to China's future and are subject to severe impairment if a better-red-than-competitive mindset comes to dominate Chinese policymaking.

Fifth, there is a question of capital stock deterioration which we have a limited ability to address in the modeling we have done. In standard GTAP modeling, a nation's capital stock of existing assets is held constant in projecting the effect of a policy shock. However, China's discussion of secure and controllable ICT infrastructure implies that a

[270] South Korea and Taiwan already have regulations in place specifically restricting Chinese investment in some of their most prized domestic technologies, and are contemplating various other measures to help their domestic ICT companies better compete against China's increasing ICT strength.

non-trivial part of the *existing* capital stock would be *torn out and abandoned*. How to model this is a question.

Finally, the discussion above shows that ICT autarky would raise consumer prices, reduce GDP, and undermine productivity growth in China. But that is not the whole picture. The model described above cannot capture political and security consequences of a breakdown in ICT-related trade and investment. The culture of ICT innovation has thrived in environments of openness and adaptability. What impact on the global cultural scene, especially in the business community, such an assault on non-native participation would have is impossible to tease from a spreadsheet. And yet, it may be the biggest variable of all.

Part III: Conclusion and Recommended Principles

The adverse economic impact of the increasing number of deglobalization policies being promulgated underscores the need for a new approach designed simultaneously to promote national security and national and global economic development. Ill-conceived rules seeking to exclude or restrict ICT products based on country of origin promote neither objective. Rigid, all-or-nothing legal regimes also are not necessary. Instead, the economic data analyzed above demonstrate the need for new thinking about national security in ICT procurement in order to forestall long-term damage to deglobalization.

A more sophisticated approach can provide governments with the tools to protect a nation's security while still realizing the vast economic benefits that globalization of the ICT sector continues to bestow. The authors recognize the value in legitimate and targeted actions to protect national security, and that aspects of the ICT sector may well implicate national security considerations. A "one-size-fits-all" approach is inappropriate for different countries, with different economies and national security needs. Instead, we suggest that national policies should be based on a common set of principles, as described further below.

A. Embrace a Globalized ICT Sector

National policy approaches to the ICT sector should embrace globalization—not fight it. Thus national policies should be consistent with the foundational principles underlying the global trade regime enshrined in the WTO agreements. Consistent with the most-favored nation principle, nations generally should not discriminate among their trading partners in ICT technology standards and procurement policies. Procurement policies should not be discriminatory. Likewise, locally produced goods and services generally should be afforded equal treatment to imported goods and services (or goods and services provided by local subsidiaries of foreign firms).

To the extent that governments must deviate from these general principles for legitimate national security purposes, such deviations should be limited, proportionate and narrowly tailored to the risk that they are designed to protect against. Deviations should be considered appropriate only where a demonstrable risk to national security cannot be addressed in a non-discriminatory manner. Moreover, regulations should be imposed only to the extent necessary to protect national security and not any further. Overbroad regulations risk being misused to distort a market and limit competition, resulting in the economic disadvantages modeled above.

B. Promote Market Competition

Government policies should encourage both domestic and cross-border competition. The modeling demonstrates the devastating effects policies limiting cross-border competition can have on national GDP and economic welfare. The interconnected nature of the ICT sector with other sectors and total factor productivity underscores how limiting competition can have widespread—and often difficult to predict—effects across both a national and global economy. To counter this potential, policies across a range of areas— including intellectual property, antitrust, standards setting, export financing, and the use of domestic subsidies—should promote competition.

Further, competition promotes—not impedes—national security. When there is competition in the marketplace, procurers benefit from increased product options. Those ICT products perceived as less secure will be at a competitive disadvantage, which in turn reduces their demand. In a post-Snowden world where consumers are increasingly basing their choices on the strength of a product's information security, competition inherently hastens the development of more secure products on the global marketplace. In other words, it is perfectly reasonable for both customers in the private market and government organizations to evaluate ICT products and services on the basis of security, but in doing so they should promote competition on this basis rather than limit it.

C. Promote Transparency

The laws and regulations enacted to govern companies in pursuit of national security should be transparent. Nations can—and should—use a corporation's transparency as one standard by which to determine the security of its ICT products. Conversely, failure to be transparent is a legitimate basis for security concern, and therefore a principled and appropriate basis on which to exclude a company's products from procurements.

In this context, transparency includes a number of facets:

- First, companies should operate in an open and transparent manner, including with respect to ownership, governance, design, manufacturing, and other business practices. An emphasis on transparency encourages companies to compete on the basis of their legitimate practices, including around security, and enables customers to make more informed decisions about their vendors. By comparison, it may be reasonable to question the security bona fides of a company that cannot transparently describe its ownership structure and sources of finance; the countries and customers whom it serves; or its product development, sales and services practices.

- Second, companies should be transparent with respect to their products' supply chains, as well as the security practices they apply to those supply chains. Increasing transparency in this regard will better enable both commercial and government customers to evaluate vendors on the basis of objective security criteria and may help support the further establishment of a accepted norms for developing and providing reasonably secure products to customers, regardless of their origin.

- Third, state owned and controlled enterprises should be subject to transparency disciplines that permit procurers of ICT to determine whether those state owned and controlled enterprises are acting for commercial reasons. This is important because SOEs may be subsidized conduits of deglobalization plans promulgated by their governments.

- Finally, governments should be transparent in the criteria and process utilized in regulating "foreign" transactions. Although there are sometimes legitimate reasons for withholding the information that led to a particular course of action on a transaction, a transparent process can add legitimacy to these conclusions. Further, by disclosing the objective criteria utilized in the evaluation process, companies can work to self-mitigate risks and advance information security.

D. Allow Commercial Procurers to Set Requirements

While governments can set broad policies and encourage open and transparent business practices, commercial entities should be allowed to set their own requirements for the equipment and software they purchase. These entities are in the strongest position to determine their needs, and place corresponding requirements on suppliers. Further, security needs are highly case-specific and therefore require an individualized approach. Commercial entities can achieve transparency, consistency across transactions, and efficiency by establishing a well-defined set of procurement rules.

* * *

Building on those general principles, the Chamber calls upon like-minded governments to work toward a voluntary, global agreement on security in the ICT industry, which requires security-related regulatory measures to adhere to the following standards:

1. **Security measures should be developed in a fully transparent manner and in partnership with the private sector**. The ICT industry has extensive experience in providing leadership and resources in every aspect of security, and can help governments ensure its security measures are effective and adaptive to rapidly changing circumstances. Product security is a function of how a product is made, used and maintained, not where it is made – a reality that would be made clear by robust partnerships between governments and the private sector.

2. **The governmental authority promulgating the security measure should demonstrate that it is not more trade restrictive than necessary to fulfill a legitimate security objective(s)**. The exercise should require a detailed explanation of the measure's security objective(s) and robust evaluation of feasible alternatives considered, including those proposed by the regulated community and other stakeholders.

3. **The security measure should be consistent with the global trade requirements enshrined in the WTO agreements, including most-favored nation and national treatment principles**. Deviations from these general rules should be rare, thoroughly explained and supported, and regulations inconsistent with these principles should be proportional to the national security risk they seek to address.

4. **The security measure should be fully consistent with existing globally recognized, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes**. This principle improves security because 1) will help ensure procurement determinations are made on the basis of objective criteria, not solely on artificial definitions of country of origin; 2) nationally focused efforts may not have the benefit of the best peer review processes traditionally found in global standards bodies; 3) proven and effective security measures must be interoperable as they are deployed across the entire global digital infrastructure; and 4) the need to meet multiple, conflicting security and conformity assessment requirements in multiple jurisdictions raises enterprises' costs, demanding valuable security resources.

5. **Security requirements should be technology-neutral**. Mandates requiring certain technologies, including a preference for domestically made technologies, decrease security because the country can no longer access leading-edge security solutions that could be developed anywhere in the world. Procurers should require their suppliers to be transparent regarding their ownership, business practices, and security policies practices.

6. **Security requirements should not require forced technology transfer or review of intellectual property (IP) such as source code**. Such IP is business proprietary information that is essential to a company' ability to innovate and remain economically competitive.

7. **Any prescriptive security requirements should be limited to areas of the economy that are highly sensitive, such as government intelligence and military networks**. Many governments justifiably have very stringent requirements for security technologies sold into intelligence and military networks.

Government procurement requirements for such systems should not extend to other government networks, government-licensed networks, or privately run infrastructure or commercial companies.

The Chamber recommends that like-minded governments voluntarily commit to abide by the foregoing principles through a formalized agreement. This non-binding agreement should establish an annual review mechanism to determine the benefits of applying the principles, whether any refinements or additions to them need to be made, and how to encourage other governments to adopt those principles. Based on the data in this study and related information, those economies which abide by the foregoing principles will be both stronger and more secure than those that do not.

APPENDIX 1: Chinese National ICT Policies and Administrative Regulations

Title of Policy or Administrative Regulation	Effective Date
Notice of the State Council on Issuing Several Policies on Further Encouraging the Development of the Software and Integrated Circuit Industries 国务院关于印发进一步鼓励软件产业和集成电路产业发展若干政策的通知	2011.01.28
Several Opinions of the State Council on the Vigorous Promotion of Informatization Development and Effective Protection of Information Security 国务院关于大力推进信息化发展和切实保障信息安全的若干意见	2012.06.28
Notice of the State Council on Issuing the 12th Five-Year Plan for the Development of the National Strategic Emerging Industries 国务院关于印发"十二五"国家战略性新兴产业发展规划的通知	2012.07.09
Administrative Measures for Credit Reference Agencies 征信业管理条例	2013.01.21
Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development of the Internet of Things 国务院关于推进物联网有序健康发展的指导意见	2013.02.05
Notice of the State Council on Issuing the "Broadband China" Strategy and Implementation Plan 国务院关于印发"宽带中国"战略及实施方案的通知	2013.08.01
Several Opinions of the State Council on Promoting Information Consumption to Expand Domestic Demand 国务院关于促进信息消费扩大内需的若干意见	2013.08.08
Outline for Promoting the Development of the Nation's Integrated Circuit Industry 国家集成电路产业发展推进纲要	2014.06
Opinions of the State Council on Promoting the Innovation and Development of Cloud Computing and the Cultivation of a New Situation in the Information Industry 国务院关于促进云计算创新发展培育信息产业新业态的意见	2015.01.06
Opinions of the State Council on the Vigorous Development of Electronic Commerce to Accelerate the Cultivation of New Economic Power 国务院关于大力发展电子商务加快培育经济新动力的意见	2015.05.04

Guiding Opinions of the State Council on Accelerating Construction of High-Speed Broadband Network to Promote Increased Network Speeds and Lower Fees 国办关于加快高速宽带网络建设推进网络提速降费的指导意见	2015.05.16
Notice of the State Council on Issuing "Made in China (2025)" 国务院关于印发《中国制造2025》的通知	2015.05.08
Guiding Opinions of the State Council on Promoting the Healthy and Rapid Development of Cross-Border E-Commerce 国办关于加快高速宽带网络建设推进网络提速降费的指导意见	2015.06.16
Several Opinions of the State Council on Using Big Data to Strengthen Services and Supervision of Market Entities 国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见	2015.06.24
Guiding Opinions of the State Council on Actively Advancing "Internet+" Action 国务院关于积极推进"互联网＋"行动的指导意见	2015.07.01
Opinion of the State Council on Reforming the Examination and Approval System for Pharmaceuticals and Medical Devices 国务院关于改革药品医疗器械审评审批制度的意见	2015.8.09
Notice of the State Council on Publishing the Promotion Plan for the Three Network Integration 国务院办公厅关于印发三网融合推广方案的通知	2015.08.25
Notice of the State Council on Issuing the Outline for Action to Promote the Development of Big Data 国务院关于印发促进大数据发展行动纲要的通知	2015.08.31
Opinions of the State Council on Speeding Up the Innovative Development of and Upgrading of Business Circulation for both Online and Offline Promotion 国务院办公厅关于推进线上线下互动加快商贸流通创新发展转型升级的意见	2015.09.18
Several Opinions of the State Council on Promoting the Development of the Express Delivery Industry 国务院关于促进快递业发展的若干意见	2015.10.26
Guiding Opinions of the State Council on Promoting the Rapid Development of Rural E-Commerce 国办关于促进农村电子商务加快发展的指导意见	2015.11.09
Regulations on the Management of Mapping 地图管理条例	2015.11.26

Notice of the State Council on Publishing the Development Plan (2016-2020) for Establishing the National Standardization System 国务院办公厅关于印发国家标准化体系建设发展规划（2016-2020年）的通知	2015.12.17
Notice of the State Council on Publishing the 2016 Major Work Items for Administrative Affairs 国务院办公厅关于印发2016年政务公开工作要点的通知	2016.04.18
Opinions of the State Council on Deepening the Implementation of the "Internet+ Distribution" Action Plan 国务院办公厅关于深入实施“互联网+流通”行动计划的意见	2016.04.21
Notice of the State Council on Publishing an Action Plan on Promoting the Transformation of Scientific and Technological Achievements 国务院办公室关于印发《促进科技成果转移转化行动方案》	2016.04.21
Outline of the National Innovation-Driven Development Strategy 中共中央国务院印发《国家创新驱动发展战略纲要》	2016.05.20
Guiding Opinions of the State Council on Deepening the Integration and Development of Manufacturing and the Internet 国务院关于深化制造业与互联网融合发展的指导意见	2016.05.20
Guiding Opinions of the State Council on Promoting and Standardizing the Application and Development of Healthcare Big Data 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见	2016.06.24
National Informatization Development Strategy Outline 中共中央办公厅国务院办公厅印发《国家信息化发展战略纲要》	2016.07.27
13th Five-Year Plan for Science and Technology Innovation “十三五” 国家科技创新规划	2016.07.28

APPENDIX 2: Chinese Non-ICT Industry-Specific Policies and Departmental Rules Affecting ICT

Industry Sector (Agency)	Title of Policy or Administrative Regulation	Year Effective
Agriculture (Ministry of Agriculture)	Notice of the Ministry of Agriculture on Issuing the 12th Five-Year Plan for the Nationwide Development of Informatization in Agriculture and Rural Areas 农业部关于印发《全国农业农村信息化发展“十二五”规划》的通知	2011
Forestry (State Bureau of Forestry)	12th Five-Year Plan for the Nationwide Development of Informatization in Forestry (2011-2015) 全国林业信息化发展“十二五”规划（2011-2015年）	2011
Manufacturing (Ministry of Science and Technology)	Notice on Issuing the 12th Five-Year Plan for the Scientific and Technical Project of Informatizing the Manufacturing Industry 关于印发“十二五”制造业信息化科技工程规划的通知	2012
Water Preservation (Ministry of Water Resources)	Notice of the Ministry of Water Resources on Issuing the Outline for the Development of the Informatization of Water and Soil Preservation 水利部关于印发全国水土保持信息化发展纲要的通知	2008
	Plan for the Informatization of Water and Soil Preservation (2013-2020) 全国水土保持信息化规划（2013～2020年）	2013
Construction (Ministry of Housing and Urban-Rural Development)	Notice on Issuing the Outline for the Development of Informatization in Construction Industry for 2011-2015 关于印发《2011-2015年建筑业信息化发展纲要》的通知	2011

Transportation (Ministry of Transport)	Notice of the Ministry of Transport on Issuing the 12th Five-Year Plan for the Development of Informatization in Road and Waterway Transportation 交通运输部关于印发公路水路交通运输信息化“十二五”发展规划的通知	2011
Financial Services (People's Bank of China, China Banking Regulatory Commission, and China Insurance Regulatory Commission)	Notice of the People's Bank of China on Issuing the 12th Five-Year Plan for the Development of Informatization in China's Financial Industry 中国人民银行关于印发《中国金融业信息化“十二五”发展规划》的通知	2011
	Notice on the Issuance of (Trial) Management Guidelines for the Protection of Insurance Company Information Systems 关于印发《保险公司信息系统安全管理指引(试行)》的通知	2011
	Acceptance Guidelines for Opening an Insurance Company 保险公司开业验收指引	2011
	Notice of the People's Bank of China on Improving Work Related to the Protection of Personal Financial Information by Banking Financial Institutions 人民银行关于银行业金融机构做好个人金融信息保护工作的通知	2011
	Administrative Measures for Credit Reference Agencies 征信业管理条例	2013
	Notice of the People's Bank of China on Issuing the Industrial Standards on the Information Security Standards for Credit Reporting Institutions 中国人民银行关于发布《征信机构信息安全规范》行业标准的通知	2014
	Guiding Opinions of the China Banking Regulatory Commission on Strengthening the Banking Network Security and Information Technology Construction through the Application of Secure and	2014

	Controllable Information Technologies 中国银行业监督管理委员会关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见	
	Notice on the Promotion Guidelines for Banking Applications of Secure and Controllable Information Technology (2014-2015) 银行业应用安全可控信息技术推进指南（2014—2015年度）	Currently suspended
	Interim Measures for the Supervision of Internet Insurance Businesses 互联网保险业务监管暂行办法	2015
	Regulation on Supervision and Administration of Informatization on Insurance Organization (Draft for Comments) 保险机构信息化监管规定（征求意见稿）	Released for comment in China 2015; released for comment at WTO TBT
	Administrative Measures for the Online Payment Business of Non-Banking Payment Institutions 非银行支付机构网络支付业务管理办法	2016
	Notice of the People's Bank of China on the Administrative Measures for Bank Card Clearing Institutions 中国人民银行关于《银行卡清算机构管理办法》	2016
Education (Ministry of Education)	Notice of the Ministry of Education on Issuing the Ten-Year Plan for the Development of Informatization in Education (2011-2020) 教育部关于印发《教育信息化十年发展规划（2011-2020年）》的通知	2012

	Notice of the Office of the Ministry of Education on Publishing the 2016 Major Work Report on Education Informatization 教育部办公厅关于印发《2016年教育信息化工作要点》的通知	2016
	Notice of the Office of the Ministry of Education on Launching Acceptance Work on the First Informatization Pilot 教育部办公厅关于组织开展第一批教育信息化试点验收工作的通知	2016
Healthcare (National Health and Family Planning Commission, State Administration of Traditional Chinese Medicine)	Guiding Opinions of the Ministry of Health and the State Administration of Traditional Chinese Medicine on Strengthening the Building of Informatization in Health 卫生部、国家中医药管理局关于加强卫生信息化建设的指导意见	2012
	Guiding Opinions of the National Health and Family Planning Commission and the State Administration of Traditional Chinese Medicine on Accelerating the Building of Informatization in Population Health Information 国家卫生和计划生育委员会、国家中医药管理局关于加快推进人口健康信息化建设的指导意见	2013
	Measures for Administration of Population Health Information (Trial) 人口健康信息管理办法(试行)	2014
Land Resources (Ministry of Land and Resources)	Notice of the Ministry of Land and Resources on Issuing the 12th Five-Year Plan for Informatization in National Land Resources 国土资源部关于印发《国土资源信息化“十二五”规划》的通知	2012
State Administration of Press and Publication, Radio, Film and Television	Provisions on Administration of Online Publishing Services 网络出版服务管理规定	2016

APPENDIX 3: Chinese Provincial and Municipal Administrative Policies and Regulations

City/ Province	Agency	Title of Policy or Administrative Regulation	Year Effective
Beijing	Beijing Municipal Government	Notice of the Beijing Municipal Government on Issuing Several Policies Concerning Further Promoting the Development of the Software Industry and the Integrated Circuit Industry in Beijing 北京市人民政府关于印发北京市进一步促进软件产业和集成电路产业发展若干政策的通知	2014
	Beijing Municipal Commission of Economy Informatization	13th Five-Year Plan for Software and Information Services Industry Development 北京市“十三五”时期软件和信息服务业发展规划	2016
Shanghai	Shanghai Municipal Government	Notice of the Shanghai Municipal Government on Issuing Several Policies Concerning Further Encouraging the Development of the Software Industry and the Integrated Circuit Industry in Shanghai 上海市人民政府印发《关于本市进一步鼓励软件产业和集成电路产业发展的若干政策》的通知	2012
	Shanghai Municipal Commission of Economy and Informatization	Notice of the Shanghai Municipal Commission of Economy and Informatization on Issuing the Action Plan for Advancing the Development of the Internet of Things Industry in Shanghai (2010-2012) 上海市经济和信息化委员会关于印发《上海推进物联网产业发展行动方案(2010－2012年)》的通知	2010
		Notice of the Shanghai Municipal Commission of Economy and Informatization on Issuing the Action Plan for Advancing the Development of the Cloud Computing Industry in Shanghai (2010-2012) 上海市经济和信息化委员会关于印发《上海推进云计算产业发展行动方案(2010－2012年)》的通知	2010
Tianjin	Tianjin Municipal Development and Reform Commission, Tianjin Municipal Commission of Economy and Informatization	Notice of the Tianjin Municipal Development and Reform Commission and the Tianjin Municipal Commission of Economy and Informatization on Issuing the 12th Five-Year Plan for the Development of the Software Industry in Tianjin 天津市发展和改革委员会、天津市经济和信息化委员会关于印发天津市软件产业发展“十二五”规划的通知	2011
		Notice of the Tianjin Municipal Development and Reform Commission and the Tianjin Municipal Commission of Economy and Informatization on Issuing the 12th Five-Year Plan for the Development of the Internet of Things Industry in Tianjin 天津市发展和改革委员会、天津市经济和信息化委员会关于印发天津市物联网产业发展“十二五”规划的通知	2011

Chongqing	Chongqing Municipal Government	Opinions of the Chongqing Municipal Government on Accelerating the Development of the Internet of Things 重庆市人民政府关于加快推进物联网发展的意见	2011
		Opinions of the Chongqing Municipal Government on Issuing the Action Plan for Big Data Development in Chongqing 重庆市人民政府关于印发重庆市大数据行动计划的通知	2013
		Implementation Opinions of the Chongqing Municipal Government on Promoting the Innovative Development of Cloud Computing and Fostering New Businesses in the Information Industry 重庆市人民政府关于促进云计算创新发展培育信息产业新业态的实施意见	2015
Guangdong	General Office of Guangdong Provincial Government	Notice of the General Office of the Guangdong Provincial Government on Issuing the Plan for the Development of the Internet of Things in Guangdong Province (2013-2020) 广东省人民政府办公厅关于印发广东省物联网发展规划(2013—2020年)的通知	2013
	General Office of Guangdong Provincial Government	Notice of the General Office of the Guangdong Provincial Government on Issuing the Plan for the Development of Cloud Computing in Guangdong Province (2014-2020) 广东省人民政府办公厅关于印发广东省云计算发展规划(2014—2020年)的通知	2014
Shenzhen, Guangdong	Shenzhen Municipal Government	Notice of the Shenzhen Municipal Government on Issuing Several Measures Concerning Further Accelerating the Development of the Software Industry and the Integrated Circuit Design Industry in Shenzhen 深圳市人民政府印发深圳市关于进一步加快软件产业和集成电路设计产业发展若干措施的通知	2013
Xiamen, Fujian	Xiamen Municipal Government	Notice of the Xiamen Municipal Government on Issuing the Plan for the Application of Big Data and Development of the Big Data Industry (2015-2020) 厦门市人民政府关于印发大数据应用与产业发展规划(2015—2020年)的通知	2015

APPENDIX 4: Chinese Laws related to National Security and Cybersecurity

Title Law	Effective Date
Guarding State Secrets Law 中华人民共和国保守国家秘密法	2010.10.01
National Security Law 中华人民共和国国家安全法	2015.07.01
Counter-terrorism Law 中华人民共和国反恐怖主义法	2016.01.01
Cybersecurity Law 中华人民共和国网络安全法	Pending

APPENDIX 5: Comparison of Chinese and U.S. National Security and Cybersecurity Approaches to Foreign ICT

Comparison of Chinese and U.S. National Security and Cybersecurity Approaches to for Foreign ICT		
	China	**United States**
1. Scope of Laws Related to Foreign ICT Companies	China's approach to regulating foreign ICT companies explicitly includes both protecting national security and fostering domestic champions. Although the latter is sometimes advocated as necessary for the former, China's industrial policy in this area has also been phrased in ways to achieve economic advantages in the sector. Examples of this can be seen in 12th Five-Year Plan.[271]	The United States does not explicitly incorporate industrial policies to advance domestic champions in its laws regulating foreign ICT companies. While some inadvertent effects of heavy regulation of the ICT sector through the CFIUS process may create a number of strong U.S.-based corporations, country or origin requirements are not explicitly within the scope of U.S. laws. In government procurement, however, the United States does advance the interests of U.S.-based corporations through a preference for American goods in direct government purchases.
2. Regulatory Review Process and Criteria	China maintains a wide range of legal tools to regulate the ICT sector. Most recently, China's antitrust authorities at China's National Development and Reform Commission advanced the government's industrial goals	CFIUS is the central regulator of foreign ICT companies seeking to invest in the United States. Voting Members of CFIUS include Treasury; Departments of Commerce, Defense, Homeland Security, Justice, State, and Energy; the

[271] *See supra*, Part A.1.b.1.

	by requiring Qualcomm to (1) pay $975 million for violations of China's antimonopoly laws and (2) reduce the costs to domestic manufacturers using Qualcomm's technology.[272] In addition, Chinese regulators have established a five-level scale to classify information systems based on their impact to national security, social order, and economic interests. Regulators require any IT security products used at or above a Level 3 to be purely domestic companies. Other laws covering cybersecurity and data privacy requires a security review if they may affect national security.[273] Further, China also maintains a process for reviewing investments on national security grounds. Such reviews are increasing and the definition of "foreign" has been expanded to increase the number of transactions subject to review.[274] The list of review criteria for these national security reviews are broad and vague.[275]	U.S. Trade Representative; and the White House Office of Science and Technology. Criteria analyzed to determine whether or not to approve a transaction include: (1) whether a foreign person has the capability or intention to exploit or cause harm (i.e., the "threat" associated with the buyer); (2) the vulnerabilities associated with the U.S. assets at issue (i.e., whether there are weaknesses or shortcomings in the assets that create a susceptibility to impairment of U.S. national security); and (3) the transaction's potential consequences, which relates to the "interaction between threat and vulnerability."[276] The process is intended to be a transparent review of the transaction. However, the ad hoc group of federal law enforcement agencies known as "Team Telecom" who review telecommunications transactions as part of the FCC's licensing requirements is notoriously opaque in its operations. There is little transparency in the group due to its informal nature.

[272] *See supra*, Part A.1.c.

[273] *See supra*, Part A.2.b.

[274] *See supra*, Part A.2.a.

[275] *See supra*, Part A.2.a.

[276] *Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States,* U.S. DEPARTMENT OF TREASURY, 73 Fed. Reg. 74567, 74569 (Dec. 8, 2008).

3. Implementation & Domestic Champions	Although China maintains a regulatory process similar to the United States, the implementation of China's goals in the ICT sector also include support in the form of subsidies to foster domestic champions. In addition, target domestic production rates are becoming increasingly more common in China's laws affecting the industry.	The United States primarily relies on the CFIUS process to promote domestic cybersecurity and national security requirements. The United States has been reluctant to turn to country-of-origin requirements, instead seeking a position consistent with its longstanding policy of openness to foreign investment.

APPENDIX 6: Economic Model

The Model

1. CGE Modeling

We simulate a scenario in which China stops contributing to the global supply chain of ICT goods and services, and assess the general equilibrium impacts of this trade restriction to both China and its trade partners. In such a scenario, China restricts imports of ICT goods and services, effectively engaging in a trade war with its major ICT trade partners. China's declaration of autarky and violation of WTO agreements is expected to bring about circumstances in which the rest of the world (RoW) countries such as the US, strategically impose restrictive import tariffs on Chinese ICT goods. In the following trade-war simulations, we drive both exports and imports close to zero in the Chinese ICT sector using a quota instrument. In addition to loss of physical access to foreign ICT goods and services, Chinese ICT sector will also lose access to knowledge embedded in foreign ICT goods and services and lag behind in technology development, leading to further productivity losses. We model the above effects using a range of exogenous negative productivity shocks in all the sectors of the Chinese economy.

Such cross-sectorial nature of impact necessitates analysis through the lens of *general equilibrium theory*, which is used widely in economics to study the cross-sectorial, cross-regional impacts of policy; i.e., how policy choices in one market can affect another. Approaches to analyzing general equilibrium impacts consist largely of Input-Output (IO) and Computable General Equilibrium (CGE) analysis. An IO model represents the inter-sectorial relationships within an economy, which is simply defined by the notion that output of a sector is used for production in another sector. Given *n* sectors, the relationships among sectors are represented by an n-dimensional input-output table that specifies how each sector provides *output* to other sectors in the form of *intermediate goods*. Given a traditional demand driven model, an IO model can then show how an additional dollar of final demand in a given sector leads to direct and indirect effects across sectors.

CGE models offer a more comprehensive approach in terms of the models' specificity; they are categorized as *completely specified models of the economy,* specifying micro and macroeconomic components from investments and government expenditures to the use of factors in all production activities. We note that IO models are deemed as a specialized version of general equilibrium models, fixed coefficients, no supply constraints, and a perfectly elastic labor supply" [McGregor et al., 1996]. Where international, inter-regional behavioral considerations play a crucial role in assessing policy scenarios, CGE analysis is an especially powerful tool [Rose, 1995].

2. GTAP Framework

The Global Trade Analysis Project (GTAP) database records the flow of goods and services of the global economy at the benchmark years (2004, 2007 and 2011). The database covers 57 sectors, 5 factors (land, skilled labor, unskilled labor, natural resources and capital), and employs both static and dynamic CGE models that primarily analyze global trade and energy policies [Walmsley et al., 2012]. GTAP'S core CGE model (henceforth referred to as the GTAP model) is a static, multi-regional model, which tracks the production and distribution of goods in the global economy. The model used in this study is based on GTAP9 and is implemented using the *GTAP6inGAMS* framework introduced in [Rutherford, 2005]. In the GTAP framework, the world is divided into 140 regions, which for the purpose of this project are aggregated into the following four regions:

- *CHN:* China (including Hong Kong)
- *USA:* United States
- *EUR:* European Union and EFTA
- *ROW:* Rest of World

For each of the four regions, the final demand structure consists of public and private expenditure across goods. The optimizing behavior of the competitive equilibrium is based on is characterized by the consumer and producer's problem; namely, consumers maximize welfare subject to budget constraints with fixed levels of investment and government expenditure; and producers minimize total cost while aggregating intermediate inputs, and primary factors (labor, land, resources and physical capital), given technology [Rutherford, 2005]. We use the 2011 GTAP dataset as the benchmark, which includes a full set of bilateral trade flows with associated transport costs, export taxes and tariffs.

3. Disaggregation of ICT Sectors

To disaggregate the ICT sector, we first identify the sectors available in GTAP database that include ICT. The following sectors are deemed ICT heavy and are disaggregated into ICT and non-ICT subsectors:

- *EEQ:* Electronic Equipment
- *OBS:* Business Services
- *CMN:* Communication

The following tables show the trade flows in the benchmark 2011 GTAP:

Hundred Million USD	**CMN**		**EEQ**		**OBS**	
Exports_BAU	**cmn**	**cmnn**	**eeq**	**eeqn**	**obs**	**obsn**
CHN	2.6	1.3	391.3	14.9	8.8	40.4
EUR	14.1	7.0	73.0	4.4	34.2	165.0
ROW	20.1	9.9	370.3	22.6	33.8	154.3
USA	9.3	4.6	91.8	3.5	18.8	96.0

Hundred Million USD	**CMN**		**EEQ**		**OBS**	
Imports_BAU	**cmn**	**cmnn**	**eeq**	**eeqn**	**obs**	**obsn**
CHN	2.8	1.4	179.4	12.7	3.0	27.3
EUR	19.2	9.4	184.5	13.7	32.9	166.3
ROW	15.1	7.5	288.9	12.0	36.4	184.4
USA	9.0	4.4	273.7	7.1	23.2	77.7

As it is clear from the data in Table 1, EEQ sector dominates the trade in ICT sector between China and its trading partners. So we take a more nuanced approach to disaggregate Chinese EEQ sector with the help from *China's 2007 Benchmark Input-Output table*.

For the remaining three regions, the disaggregation process includes bilateral trade flows of applied and bound tariff rates for 200 countries and 5000 HS6 goods. Most importantly, the trade flows are consistent with the GTAP7 database. For each region, the ICT portion of EEQ is determined by the ratio of ICT exports to total exports within the MAcMapHS6 dataset.

4. Trade Restrictions

Trade restrictions are imposed in the form of a quota on imports and exports of ICT goods and services. For this, we simply introduce quota commodities, *XQ* and *MQ*, which respectively enter the aggregation structure as perfect complements of exports and imports. The aggregation structure in production and imports are displayed in *figures 1 & 2*. In this setting, levels of *XQ* and *MQ* are both fixed to near zero values (< 0.1%).

For a more comprehensive analysis of the effects, we perform sensitivity analysis by changing both the elasticity of substitution between domestic and foreign goods in the production function, σ_d, and the elasticity for imported goods in the import aggregation function, σ_m. Results of this sensitivity analysis are presented in the results section of this report.

Note that by imposing restrictive quota on trade in GTAP, we are in turn assuming a high trade tariff that will bring about near-zero trade activity levels. As a result, one technical challenge arises in specifying this scenario. Due to the *Armington aggregation assumption* of domestic and imported varieties of trade, under which goods are differentiated by region of origin), it is infeasible to drive down imports without having import prices rise to infinity. To overcome difficulties in obtaining both realistic and feasible numerical solutions, we have introduced a backstop alternative to imports; when imports become too costly, domestic production is used to substitute foreign goods. This way we can drive down trade to near zero values without running into numerical problems.

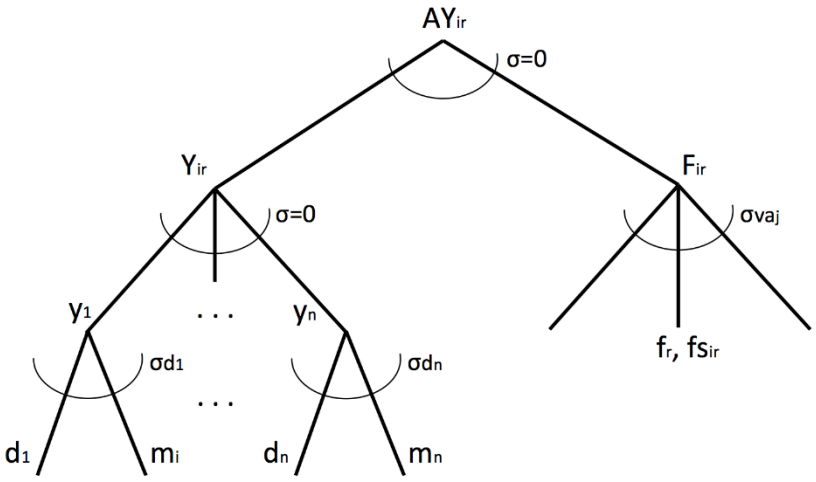


Figure 1. Production Function

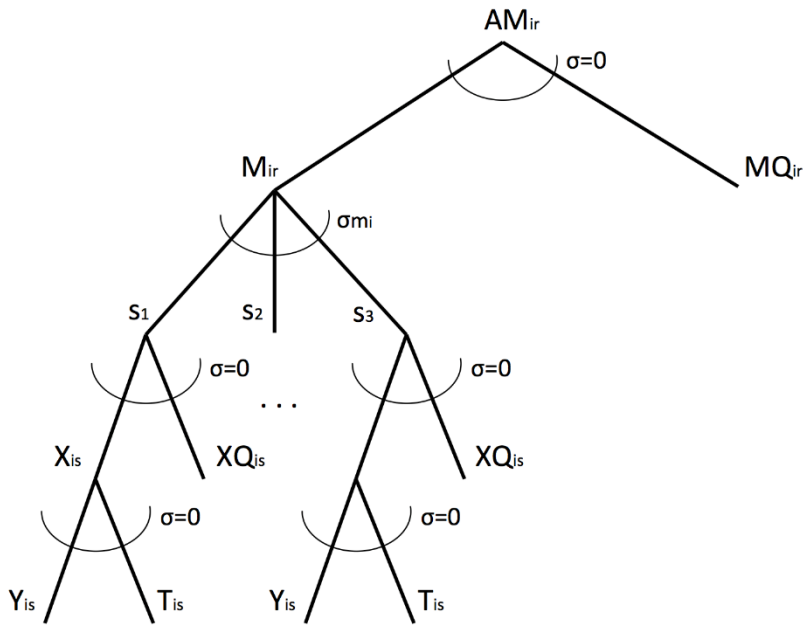


Figure 2. Import Aggregation Function

- *AY:* Production Function
- *Y*: Domestic Output
- *AM*: Import Aggregation Function
- f_r: Primary Factors
- fs_{ir}: Sector-specific Primary Factors
- *d*: Domestic Intermediate Goods
- *m*: Foreign Intermediate Goods
- *M*: Imported Goods
- *MQ*: Import Quota
- *X*: Exported Goods
- *XQ*: Export Quota
- *T*: Transport Services

5. The Steady-state Model

We follow the steady-state model extension of the static GTAP model in Rutherford and Tarr [2003], based on the original work of Hansen and Koopmans [1972]. The objective of this extension is to assess the upper bound on GDP impacts in a Solow type model.

The essence of the steady-state implementation is the following: in equilibrium, we assume that the capital stock in each region is optimized based on the rate of return on capital and the cost of replacing a unit of capital (or producing a unit of the investment good). If for example, the rate of return on capital is *greater* than the cost of replacing a unit of capital due to policy, then investment would *increase* until the ratio of the rate of return on capital to the cost of producing the capital good returns to its equilibrium state.

In this study, a restriction in trade policy will produce a new equilibrium, where the rate of return on capital decreases relative to the cost of investment due to inefficient allocation of resources. Under steady-state conditions, the fixed capital stock in the initial benchmark (static model) is no longer optimal and investment (and hence the capital stock) *decreases* until the marginal productivity of capital (MPK) restores the relative return on capital to its initial value. To implement this, we allow the capital stock to be determined endogenously, while holding constant the price of capital. Note that in the static model we took the opposite approach; while holding constant the stock of capital, the price of capital was endogenously determined.

Equilibrium Conditions for Steady-state

To endogenize the stock of capital, K, we add a capital stock multiplier, τ_K, to the static model, which equals unity in the benchmark equilibrium. This variable alters the supply of physical capital:

$$\sum_i K_i = \tau_K \bar{K}$$

for which investment demand is scaled proportionally:

$$D_i = \sum_j X_{ij}^D + c_i^D + g_i^D + \tau_K I_i$$

where D_i corresponds to domestic output and X_{ij}^D, domestic demand of intermediate goods. Both effects enter into the representative agent's budget constraint:

$$\max U(c^D, c^M) \quad s.t.$$

$$r_K \tau_K \bar{K} + p_L \bar{L} + p_N \bar{N} + \sum_i p_i^R \bar{R}_i = \sum_i (p_i^D c_i^D + p_i^M c_i^M)(1 + t_i^C) + \sum_i p_i^D \tau_K \bar{I}_i$$

where $\bar{L}, \bar{N}, \bar{R}_i$, respectively denote benchmark levels of labor, land and sector-specific resources. Let the cost of replacing a unit of capital be represented by q, for which the cost function takes the form:

$$q = \sum_i a_i^I [\beta_i^M (p_i^M)^\rho + (1 - \beta_i^M)(p_i^D)^\rho]^{1/\rho}$$

where p_i^D and p_i^M each denote the prices of domestic and imported output. In the steady- state model, the capital stock adjusts so that the ratio of the rental rate on capital to the cost of producing a unit of the capital good is constant:

$$\frac{r_K}{q} = \rho + \delta$$

implying that in the long-run equilibrium, the return to capital is equal to the sum of the discount rate on future consumption plus depreciation. When this ratio falls in response to a shock, a decrease in the capital stock take places to *increase* the marginal productivity of capital and to ultimately restore equilibrium. An increase in this ratio, however, will induce an increase in the long run equilibrium capital stock.

As the model employs the *Armington assumption*, in which imported and domestic goods are imperfect substitutes, the capital good is produced by both domestic and imported inputs as well as labor and capital as indicated in the cost function above. A trade restriction will hence *increase* the price of imported inputs and there is a general presumption that q will rise. Even when the trade restriction shifts resources to capital intensive industries and induces an increase in the rental rate of capital relative to the wage rate, the price of a unit of capital, q, could increase more inducing a fall in the capital stock. As a result, r_K/q, and consequently the capital stock, decreases. Since we observe a decrease in the rental rate of capital relative to the cost of the investment good, the capital stock must decline in the steady-state model to keep the ratio at its benchmark value. This reduction of the capital stock then works through the trade model similar to an "endowment effect", generating a larger welfare loss since there are less resources to be utilized.

U.S. CHAMBER OF COMMERCE
International Affairs

U.S. Chamber of Commerce
1615 H Street NW | Washington, DC 20062
Phone: 202-463-5525 | www.uschamber.com