AEI Economic Studies

Telecoms and the Huawei Conundrum

Chinese Foreign Direct Investment in the United States

Claude Barfield

November 2011

American Enterprise Institute

AEI Economic Studies

Telecoms and the Huawei Conundrum

Chinese Foreign Direct Investment in the United States

Claude Barfield

November 2011

AMERICAN ENTERPRISE INSTITUTE

Acknowledgments

The author would like to thank the following for commenting on parts or all of the manuscript or providing advice and counsel: Adam Lerrick, Theodore Moran, Daniel Rosen, Philip Levy, Mark Groombridge, William Plummer, Lixin Cheng, Derek Scissors, James Mulvenon, Charles Hunnicutt, Nicholas Lardy, Alex Pollock, Peter Wallison, and Richard Suttmeier. The author would also like to thank Robert Fisher and Patrick Schneider for research and fact-checking assistance. Any errors in fact or judgment are mine.

Foreword

In this first paper in the AEI Economic Studies series, we present "Telecoms and the Huawei Conundrum" by Claude Barfield. While the paper traces the historical evolution of a single Chinese company, the backdrop is the role of China itself in the new world economic order. As China grows in power and influence, its opaque and often secretive nature continues to make other countries wary. Often the concern is merely economic, as many worry that Chinese firms receive benefits from the Chinese government that give them unfair advantages in the global economy. A more acute concern is the extent to which the Chinese Communist Party is able to manipulate Chinese enterprises, posing a threat to the national security interests of countries that allow these firms to operate within their borders.

This paper highlights the complex challenge of allowing the free flow of global capital while adhering to the boundaries imposed by legitimate concerns about national security. The narrative details the growth and expansion of the Chinese telecommunications equipment company Huawei. Huawei began operations in 1988 as a privately owned corporate enterprise in Shenzhen, China. By 2010, it had established operations in more than 140 countries around the globe. Today, it is set to overtake the Swedish champion, Ericsson, as the world leader in telecoms equipment. However, US government officials and politicians are wary of the firm's ties to the Chinese military and view its presence in the United States as a security concern. Many officials have accused the company of engaging in espionage on behalf of the Chinese military, stealing intellectual property, and benefitting from subsidized loans from the China Development Bank.

In light of these fears, there has been an attempt to marginalize the company in the US telecom market. In 2010, when Sprint Nextel was considering awarding a multibillion dollar contract to Huawei, political interference from Washington prevented the deal from taking place. In February, the American government even forced Huawei to undo a minor deal: the $2 million purchase of patents from 3Leaf, a bankrupt Silicon Valley startup.

Political interference in investment decisions represents a divergence from the ideal of economic freedom and free markets. But it may be reasonable in telecom and other sensitive sectors where national security trumps free-market priorities. How governments respond to these kinds of conflicts of priorities will determine geopolitical relations going forward. Huawei is therefore a valuable case study because all the accusations levied at Chinese firms—secrecy, economic support from the government, and security concerns—come together in this case. Barfield not only offers analysis and recommendations for how the various parties—Huawei, the Chinese government, and the US government—should respond to the current crisis, but also brings clarity to the bigger issues of how to think about and address difficult questions at the meeting point of economic, political, and national security priorities.

It is my hope that this paper will be thought-provoking and will spur debate, paving the way for a more informed consensus on these issues.

—Aparna Mathur, AEI Economic Studies Editor

Executive Summary

The Chinese company Huawei has emerged as the second-largest telecommunications equipment company in the world. It operates in 140 countries around the globe, providing equipment, software, and services to forty-five of the world's fifty largest telecom operators. It is moving aggressively downstream into the burgeoning smartphones market. As a recent, detailed report on the company concluded, Huawei's "extraordinary range of product offerings supports almost every meaningful segment of telecommunications network architecture."[1]

Despite its global success, Huawei has consistently been rebuffed in attempts to make large investments and land large contracts in the United States. US government officials have intervened on a number of occasions to block potential acquisitions and equipment contracts involving Huawei, citing security concerns (though without specific details). The company has vigorously contested allegations that it has ties to the Chinese military or represents a security risk in the United States. It has vowed to continue its quest to become a significant player in the US telecom market.

All of this is being played out against a background of increasing tension between Washington and Beijing over cyber attacks on US corporations and government agencies that have been traced back to sites and hackers in the People's Republic of China (though not to the government directly). As this study was going to press, the top counterintelligence agency in the United States pointed the finger directly at China, stating, "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[2]

In addition, the White House disclosed that it had commissioned a task force to evaluate the "opportunities, risks and implications" posed by foreign telecommunications companies in the US market. US officials let it be known that while no particular company or country was targeted, Huawei's expansion in the US market was a "key impetus" for the initiative.[3]

At the same time, the Obama administration, faced with the continuing economic drag from the global financial crisis and economic downturn, has been eager to reaffirm America's historic open arms policy toward foreign direct investment (FDI) as a means of enhancing renewed economic growth and prosperity. This includes the potential of large FDI inflows from China over the next decade. To underscore this commitment, Vice President Joe Biden recently urged Beijing to increase investment in the US market, saying, "We are still the single (best) bet in the world, in terms of where to invest." Chinese investment, he continued, "means jobs. American jobs."[4] In turn, Beijing has been quick to protest America's alleged unfair treatment of Huawei and other Chinese telecommunications companies and the "lack of transparency" in US FDI policy. It has also threatened to match purported US investment obstacles with new hurdles of its own.

This study traces Huawei's corporate history, particularly its unsuccessful efforts to gain a foothold in the US market. It analyzes both the economic and security challenges posed by future Chinese investment in sensitive sectors, such as information technology and the broader telecommunications supply chain. The study concludes with recommendations for action by the US government, by the Chinese government, and by Huawei, to accommodate future Chinese investment and contracting in the US telecommunications sector while preserving vital US national security interests and priorities.

These recommendations include:

- The US government should make the investment/security-vetting process (the

so-called CFIUS process) more transparent and should take steps to formulate and publicize a set of guidelines that would explain the rationale behind individual investment decisions. As a number of intelligence officials from several administrations have concluded, Committee on Foreign Investment in the United States (CFIUS) officials can provide more detail on the sources of their security concerns without jeopardizing US intelligence efforts. At a minimum, the results of the White House task force initiative cited above, as they pertain to Huawei, should be made public.

- Efforts to expand CFIUS to cover normal business contracts or joint research and corporate ventures should be resisted. If acceded to, moves to expand CFIUS, whether stemming from congressional sources or private competitors, would lead to an undesirable politicization of the process through an adverse intermingling of national security and private competitive concerns and motives.

- Beijing should renounce trade-investment-distorting credit subsidies that aid Chinese companies competing in overseas markets. It should agree to adhere to the guidelines and specific restrictions set out in the 1978 Organisation for Economic Co-operation and Development (OECD) arrangement on export financing and the 1991 Helsinki Package that clarified rules with regard to tied aid to developing countries.[5] Pending this action, Huawei would be well advised to agree to be bound by OECD rules when accepting subsidized credit arrangements for its customers.

- Huawei should bite the bullet and become a publicly traded company listed on a US stock exchange, most likely the NASDAQ. The company's opaque corporate structure and its obscure decision-making process, abetted by recent governance and accounting scandals involving other Chinese companies that invest overseas, feed suspicions that it is an unreliable business partner and secretly a creature of the Chinese government. As the *Economist* recently stated in criticism of Huawei's resistance thus far to public listing, "Huawei appears to want to have it both ways: remaining a Chinese company . . . while competing with publicly traded Western giants—this is unlikely to work."[6]

- Huawei should continue—and even step up—its efforts to assuage US government agencies' security concerns. It has given global security concerns a top place in its corporate structure, and it should increase and expand programs to provide independent, continuous third-party evaluation of its equipment. Finally, though there are risks involved, the company's recent strategy of instant and highly vocal rebuttal to negative judgments by the US government and by congressional critics and outside interest groups, will pay off in the future—assuming the in-your-face candor is consistently supported with solidly documented facts.

Telecoms and the Huawei Conundrum: Chinese Foreign Direct Investment in the United States

In February 2011, the Chinese telecommunications-equipment giant Huawei published an open letter to the Obama administration flatly denying a series of so-called unfounded allegations and false claims against the company's practices and organization and urging US authorities to "carry out a formal investigation of any concerns" they may hold about Huawei.[7] Though it has emerged as the world's second largest manufacturer of telecommunications equipment (and the third largest maker of equipment for wireless networks), Huawei has been rebuffed repeatedly in its efforts to gain a substantial foothold in the US market. The open letter attempted to rebut charges that Huawei has direct ties to the Chinese military, that purchase of its equipment by US companies would create a major security risk for the United States, that it has received unfair (and by inference, trade illegal) subsidies from the Chinese government, and that is it is a perpetual thief of intellectual property.

In response to the Huawei letter, a US Treasury official (Treasury chairs the interagency committee responsible for vetting foreign direct investment [FDI] for security purposes) brushed off the company's request with a boilerplate response that the United States still "strongly support[s] a longstanding commitment to welcoming foreign direct investment, consistent with national security. This includes investment from China."[8] Meanwhile, an unnamed official from the People's Republic of China (PRC) Ministry of Commerce accused the United States of using "all kinds of excuses, including national security, to engage in obstruction and interference" with Chinese businesses' activity in the United States.[9] In a sign that the PRC may be ready to increase the stakes in the FDI/security tug of war, the Chinese antimonopoly bureau twice postponed clearance of a Nokia-Siemens joint venture's proposed purchase of Motorola's wireless equipment division (a move once contemplated by Huawei, but dropped because of past US government opposition to such purchases).[10] And finally, the PRC State Council announced that it was establishing a new ministerial panel to screen foreign firms for national security issues.[11]

Over the past several months political pressures against Huawei's operations in the United States escalated. On August 9, 2011, four US senators and one US representative wrote to the Secretaries of Energy and Defense and the chairwoman of the Securities and Exchange Commission repeating the early security and subsidy allegations and challenging a recently awarded contract with a University of Tennessee computer engineering research center. The letter was aimed specifically at a subcontract for a joint venture between the US firm Symantec and Huawei to provide data storage and cyber-security equipment. Such a contract is not illegal under current US law, but the congressmen concluded that "Huawei is not an appropriate partner for advanced US research centers."[12]

Huawei in turn responded furiously and in kind, charging that the congressional letter "drags out a series of tired, hackneyed allegations against Huawei derived from several non-authoritative sources."[13] Huawei contended the thesis and specific allegations in the letter "are simply false." The letter concluded by stating that there is no new strategy or "any nefarious aims to penetrate US information systems."[14] In an August 25, 2011, letter to Secretary of Defense Leon E. Panetta, Huawei also challenged a recent Department of Defense report stating that Huawei had "close ties to the PLA [People's Liberation Army]."[15] Huawei states that the report "has no basis in fact and unjustly perpetuates an aura of doubt and distrust."[16]

Telecommunications and information technologies (IT), which undergird both economic and security networks, occupy a no man's land between national defense rules and policies and national commercial, trade, and investment policies. In recent years, cyber attacks, many traced back to hackers and sites in the PRC (though not to the government directly), have greatly complicated—and potentially politicized—US commercial investment decisions and the national security vetting process.[17]

But telecommunications and IT must also be viewed in the larger context of growing cross investment between the two countries through new, so-called greenfield investments and through mergers and acquisitions. US multinationals' push into the Chinese economy is an old story: for almost two decades US firms have taken advantage of a favorable climate in many sectors for FDI, with the total cumulative US investment now above $50 billion.

What is new today is the arrival of Chinese companies—both private and state-owned enterprises (SOEs)—knocking at the door of the US economy, eager to take advantage of investment opportunities in the United States. As a recent study from the Asia Society underscores, while Chinese investment in the United States is tiny compared with that of other countries (under $12 billion), the Chinese presence is set to explode in the coming decade. According to the Asia Society analysis, more than $1 trillion in direct Chinese investment should flow worldwide by 2020, with a substantial portion directed at the United States and other advanced economies.[18]

Though the authors of the study argue strongly that Chinese FDI can become an important source of jobs and enhanced economic growth for the United States, they also admit that the new investment wave presents difficult questions stemming from strategic tensions between the two countries, security risks and suspicions, and quandaries over competition with state-owned or directed corporations.[19] The goal of this paper is to examine in detail how these challenges and anxieties have played out with regards to Huawei's attempts to enter the US market and to extract lessons from this experience. The paper will conclude with observations and recommendations both for US policymakers and for Huawei and other Chinese companies as they seek to reap advantages from increased FDI in the US economy. The larger issues and questions the study will analyze include:

- The dilemmas inherent in defending long-standing US policies for open investment when the spread of information technology, with attendant networks and structural components, create serious national security risks;

- The limits of security actions when information technology is moving more swiftly than national security defenses;

- The pull to expand the reach of the CFIUS process pitted against the potential downside economic and investment consequences, as well as the threats from politicization of the national security scrutiny.

- The specific challenges posed by Huawei and other Chinese telecoms companies that often began as instruments of government policy but have evolved into highly efficient and innovative multinational organizations.

- The adequacy of US and other countries' securities and investment regulations for publicly traded multinational companies, and the extent to which Chinese companies should be given special scrutiny and stricter oversight.

Huawei, Past and Present

As a result of recent controversies and an expensive public-relations campaign to make the case that it is a normal commercial enterprise, Huawei has made

many aspects of its corporate history known.[20] Ren Zhengfei, a former PLA officer and technician, founded Huawei in 1988 in the city of Shenzhen. It initially distributed imported PBX (private branch exchange) products but almost immediately began producing its own telecommunications equipment. Unusually for a Chinese corporate entity at the time, Huawei was organized as a private company.[21] The management structure is convoluted. The company is employee-owned, with Ren retaining 1.42 percent of the shares, and the rest—98.56 percent—held by some more than 61,000 Chinese employees. Employee shares are not freely traded and must be sold back to the company if an employee leaves. Non-Chinese employees (now numbering over 50,000 worldwide) are not eligible for ownership shares. The employee shareholding arrangement is implemented through the Union of Shenzhen Huawei Investment Holdings Co. Ltd. Company spokesmen state that the Union is the controlling authority for the organization: it governs the policy of the Huawei Technology Co. Ltd, which itself is a wholly owned subsidiary of the Shenzhen Huawei Investment and Holding Co. Ltd. A committee of fifty-one Union members is elected by the shareholders to make decisions for the company. In turn, the committee elects thirteen members to the Huawei board of directors.[22]

Much of the company's early history is explained by two parallel phenomena: first, in its determination to create a modern, technologically advanced military, the Chinese government gave top priority to the telecommunications sector, including building a world-class telecommunications equipment base; and second, whatever its ties to the government, Huawei's relative freedom as a private-sector operation allowed full play for Ren's entrepreneurial instincts and the technical savvy of a group of young researchers assembled around him.

Huawei and the Digital Triangle. In a widely cited 2005 study of the evolution of the Chinese defense/industrial complex, the Rand Corporation identified Huawei (along with other Chinese IT companies) as part of a paradigm shift in "technonationalist strategy."[23] The "digital triangle," as described by RAND, consisted of highly commercial domestic IT companies, state R&D institutes, and the military. "Private Chinese companies such as Huawei . . . represent the new digital triangle model, whereby the military, other state actors, and their numbered research institutes help fund and staff commercially oriented firms that are designated 'national champions,' receive lines of credit from state banks, [and] supplement their R&D funding with directed [targeted project] money. . . . [They] are genuinely commercial in orientation, seeking to capture domestic and eventually international market share."[24]

Certainly, there is evidence to support this theory in Huawei's early history. In the early 1990s, the company received a crucial boost from contracts to develop equipment for the PLA's first national telecommunications network; these contracts were periodically renewed for continuous system upgrade. In 1996, Beijing established an explicit national champion policy for the telecomm equipment industry to forestall future foreign domination, and it gave a direct nod to Huawei, symbolized by a personal visit and endorsement from then–vice premier Zhu Rongji.[25] This opened the way for increased state support from entities such as the Chinese Construction Bank and later the Chinese Development Bank. Further, after promoting joint ventures in the area in the early 1990s, the PRC reversed course after 1997, not only terminating government loans for the importation of digital switching equipment but also levying tariffs on imported communications equipment. Within several years, aided by crucial contracts with the national railway systems and a number of provinces, Huawei had overtaken and passed Shanghai Bell, the joint-venture company that had initially dominated the Chinese telecom-manufacturing market and was the source of key technology transfers.[26]

Further, during the 1990s, Huawei, along with other Chinese telecom companies, had important ties with a group of government research institutes, several of which were sponsored by the PLA. Three organizations that constituted an R&D consortium

were particularly important during these early years. The Center for Information Technology, itself part of a larger research institute of the PLA, led the consortium. Two other research institutes, maintained by the (former) Ministry of Post and Telecommunications, also provided buttressing support. These IT companies further supplemented their R&D resources through support from so-called numbered research programs, particularly the National Defense Program 863 (administered by the Ministry of Information Industry) that aimed to marry the latest university research with private commercial advances.[27]

Huawei benefitted more recently from problems related to government-sponsored industrial policy for high-tech sectors. In 2007, Huawei and several other IT companies were awarded new "national laboratories" by the Ministry of Science and Technology to advance mobile telecommunications technology and standards. The project signaled Chinese officials' dissatisfaction with the meager technological payoff from funding traditional research institutes. As one official complained, "Large quantities of R&D have been spent in vain. Research institutes rate their success by how many R&D projects have been completed, rather than the effectiveness of the final results."[28] In what it called the Next Generation Project, the Chinese government will directly inject a large proportion of the research funds into these companies with the hope and expectation that they would be better able to develop the intellectual property (IP) and a strategy for successfully promoting the technologies under highly competitive market conditions.

Commercial Entrepreneurialism. Though undoubtedly aided by government support, Huawei, under Ren's leadership, early on displayed entrepreneurial traits and a gritty determination to succeed in international competition far beyond the confines of the large Chinese market. From the outset, the company paid high wages and recruited top-flight technical and engineering talent (often from competing companies and often with a talent for reverse engineering),[29] and it has consistently plowed back over 10 percent of sales into R&D.[30]

Huawei devised a growth strategy for the Chinese market that it successfully transformed into a competitive strategy for global markets. Aware that Huawei could not compete initially with larger, more advanced telecom-equipment companies, Ren adopted an economic variation of Chairman Mao's military strategy: occupy the countryside and surround the cities.[31] In more formal economic terms, Huawei exploited market segmentation, first in the Chinese market and later in the global market.

Domestically, it initially focused on rural areas with simple, easy-to-use products that could withstand adverse conditions, such as erratic electricity, poor transmission quality, or "rats chewing the wires."[32] It attempted to compete with foreign multinationals with more advanced equipment in China's booming urban markets only later.

Huawei successfully adopted the same strategy in international competition. Technology and marketing executives fanned out to a number of backward, developing economies throughout Africa, South America, and Asia. (Russia was also a successful early target.) Starting with simple, low-priced equipment, the company filled a competitive niche that allowed it to take commanding positions later in these markets as the demand grew for more sophisticated switches, circuits, and a broader portfolio of wireless technology.[33] Because it specialized in wireless network equipment, Huawei was also able to take advantage of the fact that many developing economies had little investment in ground-based infrastructure and were ready to skip ahead to wireless networks.[34]

While an integrated technology-marketing plan is essential for an international strategy, there were many other potential challenges in growing a small, insular Chinese company into a globally competitive multinational. These relate to internal decision making on a host of issues, ranging from establishing local management in diverse markets to coordinating among various internal departments to effective communication and service to key customers to tailoring specific technologies to local needs and requirements.

For these challenges, traditional government support—subsidy or favoritism by Beijing bureaucrats—had little relevance. Instead, Huawei turned to Western management specialists. For a decade, beginning in the late 1990s, it enlisted IBM's management skills and experience to construct an organization and structure that could manage and control increasingly complex supply chains that included multiple sourcing across a number of national borders. The result streamlined the production process and, of equal importance, reshaped the corporate culture.[35] Additional advice came from leading consultants such as PricewaterhouseCoopers, the Hay Group, and Towers Perrin in areas such as financial management, quality control, human resource management, and employee stock-option plans.[36] Openness to outside advice started at the top. Ren traveled to the United States in 1997, where he spent weeks interviewing US corporate executives seeking guidance on how to succeed in foreign and international markets.[37]

In the early years, Huawei took pride in a lone-wolf mentality and modus operandi, but more recently it has shifted to a less aggressive, more cooperative stance with other telecom-equipment firms and system operators. Over the past decade, it has established a large number of cooperative R&D and joint-product ventures with many telecoms and IT companies, including IBM, Texas Instruments, Qualcom, Microsoft, Intel, Siemens, NEC, and Motorola, among others. It also joined the major international telecom-standards organizations such as the ITU (International Telecommunication Union), ISO (International Organization for Standardization), and the IEEE (Institute for Electrical and Electronics Engineers). Finally, Huawei established joint ventures with both equipment companies and operators to manufacture products in China for sale under other corporate names (Verizon, T-Mobile, Motorola) in Western markets.[38] Huawei has also attempted to balance the competitive pressures from international competition against bureaucratic pressures within China. Thus, while it bowed to bureaucratic pressures to push a national standard for 3G (third generation) and 4G (fourth generation) wireless devices, it developed equipment that comported with other international wireless standards to maintain a competitive advantage.[39]

The company achieved its first breakthrough in a Western, developed country in 2001 when it concluded a deal in the Netherlands to supply a wireless station that could run several communications technologies more efficiently and inexpensively than competing firms.[40] It went on to negotiate key contracts and alliances in France, Germany, England, and Belgium, as well as in Eastern Europe. Today Huawei sells equipment, software and (more recently) services to forty-five of the world's fifty largest telecom operators. Over the past decade, it has rapidly climbed the technology ladder, becoming a key player in the build out of advanced 3G and 4G wireless equipment networks. It is now moving aggressively downstream into the burgeoning smartphone market.[41] In 2010, in alliance with Google, it launched its own IDEOS smartphone; by 2015, Huawei aims to be among the top three mobile handset brands.[42]

Already, Huawei has exerted a major impact on price competition in the markets in which it competes. For instance, before Huawei began bidding for large European telecom-equipment contracts in 2004, gross profit margins for major players such as Ericsson and Alcatel-Lucent reached 45–50 percent. They fell to 30–35 percent immediately after Huawei appeared on the scene, according to an analysis by the Barenberg Bank in Hamburg.[43] Another recent detailed report on the company concluded that Huawei's "extraordinary range of product offerings supports almost every meaningful segment of telecommunications network architecture."[44]

This places the company just behind Ericsson and in close competition with Nokia-Siemens as the second largest telecommunications-equipment company in international competition, with $28 billion in global revenues in 2010.[45] It operates in 140 countries and employs some 110,000 workers and technicians worldwide. Over 65 percent of its sales are outside of mainland China.[46] It has established over 100 international branch offices and operates

twenty R&D centers in China and around the world. In both a symbolic and practical step, the company reorganized its corporate structure in 2005, with the China department becoming one of nine regional departments for global marketing.[47]

Clawing to the Top: Fierce International Telecom Competition

As a latecomer to international telecom-equipment competition, Huawei faced particularly daunting hurdles, and its response to these challenges revealed a capacity to learn and adjust swiftly—and to cut legal and competitive corners when necessary.

Allegations of bribery and trapping clients through trial-period misinformation have at times plagued the company's operations in Latin America and Africa. A report for the US Army's Strategic Studies Institute details purported unfair business practices in Argentina, including framing customers for activities undertaken during fully paid business trips to China and using monetary presents for extortion. While admired for its technological prowess, Huawei also acquired a reputation as a ruthless and cunning competitor among Argentinean businessmen.[48] More recently, Motorola has charged in a lawsuit that Huawei bribed a number of Motorola employees to steal and pass along proprietary technology that directly aided product development.[49] Court records in this suit have a James Bond element, including the 2007 arrest of a Chinese-born Motorola employee at Chicago's O'Hare airport. She was carrying 1,300 stolen Motorola documents and Chinese military catalogues and was traveling on a one-way ticket to the PRC.[50]

Intellectual Property and Telecom Competition. While there are a number of reasons Huawei has failed to penetrate the US market, a bad stumble and miscalculation early on set back its initial efforts. It first mounted an aggressive marketing strategy that challenged established US vendors suddenly and directly. In 2003, market leader Cisco Systems filed a wide-ranging suit against Huawei, charging wholesale infringement on Cisco's copyrights, including "blatantly" copying router technology and source codes, among other allegations.[51] In July 2004, Cisco dropped the lawsuit after the two parties reached an agreement that saw Huawei withdraw the named products from the US market.

This was a humiliating defeat for the company, and the episode has often been cited as evidence of Huawei's shoddy business tactics. The reality is a bit more complicated. Intellectual property lawsuits are actually common currency in the telecoms sector.[52] Huawei's real mistakes related to timing and depth of patent portfolio—it lacked a large backlog of patents as weapons for countersuits. Since 2004, Huawei has systematically worked to rectify this situation.

From 2003 to 2009, Huawei's patent filings grew by 26 percent per year. In 2008, it filed more international patents than any other firm in the world. By 2011, the company had applied for more than 49,000 patents, and had been granted 17,765 patents.[53] In 2010, it paid some $220 million in license fees to Western telecom companies. Also in 2010, Huawei received a coveted innovation award for corporate use of innovation from the *Economist*, which stated that the award challenged the notion that "Chinese firms are merely imitators rather than innovators."[54] In truth, there were complementary reasons for Huawei's patent drive. For strategic defense (countersuits) in IP warfare and offensively, as a natural outgrowth of the company's climb up the technology ladder. By 2011, Huawei had a lot of technology to defend.[55]

It also was in a much better position to counter legal maneuvering by its competitors. Thus, over the past eighteen months, a very different IP litigation story has unfolded. Because of expected US government opposition, in 2010 Huawei allowed a leading rival, Nokia Siemens Networks (NSN), to scoop up Motorola's substantial wireless assets. But then Huawei immediately sued (and won an injunction) to stop Motorola from transferring certain IP to NSN as part of the deal. Through a joint venture, Huawei had supplied Motorola with telephonic equipment that was sold under a Motorola label. Prior to the merger negotiations, Motorola had sued Huawei,

charging industrial espionage. In a settlement announced on April 13, 2011—and a victory for Huawei—Motorola and Huawei settled all of their IP disputes, including Motorola's withdrawal of the industrial espionage charge.[56]

In the larger competitive arena, Huawei's drive to amass a sizeable patent portfolio was fortunate, though the company probably could not have foreseen current developments. Over the past year, major patent wars have erupted in the high-end electronics sector, particularly over the thousands of patents related to smartphone production. Google has been subjected to a number of suits from companies such as Apple, Microsoft, and Oracle, charging patent infringement in the development of its Android smartphone.[57] In a defensive response, Google first bid and lost an auction for Nortel's patent portfolio but then triumphed by winning control of Motorola's 17,000 patents for a whopping $12.5 billion. Many economists have severely criticized the patent "arms race" as costly and devoid of any spur to real innovation.[58] But for Huawei, which aspires to enter the low end of the smartphone market, the 17,000-patent cushion represents an arsenal in waiting.

Continuing Subsidies: Unfair Practices?

As noted above, Huawei has received substantial R&D support from the Chinese government—and from organizations tied to the PLA—over the course of its history. It continues to receive such R&D support, as the company stated in its February open letter to the US government. In 2010, it received public R&D funds amounting to about $90 million. In addition, and of much larger significance, Chinese commercial banks, particularly the China Development Bank, have made credit lines available to Huawei's customers since 2004. Huawei serves as an intermediary, but the customers are responsible for paying principle and interest directly to the banks. The buyer's credit line is up to $40 billion, with some $10 billion made available to Huawei's customers.[59]

The key questions regarding both the R&D funds and the credit line are whether they represent unfair public support and, more specifically, whether they violate China's obligations under the World Trade Organization (WTO).[60] Public R&D support is not likely to become a major issue: many nations have substantial research programs and the trade rules governing permissible programs to advance national technologies are not well defined (as the ongoing brawl between the European Union [EU] and United States regarding support for Boeing and Airbus demonstrates).

The legality of the credit line is potentially a much greater problem. Huawei has benefitted enormously from the $10 billion laid out over the past decade to entice international customers to buy its products; this has been particularly true for the company's astounding rise in developing countries.[61] But many countries have programs and institutions to support domestic corporations in the global competition for large contracts. For instance, the US Export-Import Bank dispenses some $15 billion in loans and loan guarantees each year to aid US companies, such as GE, Boeing, and Caterpillar, in bidding for international contracts.[62]

Whatever the legal technicalities, Huawei is likely to face greater scrutiny and challenges regarding alleged unfair subsidies. In June 2010, at the request of a small wireless modem producer, Option SA, the European Commission began a countervailing duty investigation based upon charges of unfair research and credit-line subsidies granted to Huawei by various elements of the Chinese government. Subsequently, Huawei effectively bought off Option SA with $40 million contracts to purchase software and buy out the company's semiconductor unit. Though the commission terminated the proceeding, it announced that it would continue to investigate unfair subsidy allegations against the company as well as potential dumping (selling below cost) charges. EU trade commissioner Karel De Gucht stated, "I expect that there will be more and more complaints . . . it will become a trend."[63] He followed by openly inviting EU companies to request a case,

stating that the commission was prepared to "support EU companies in seeking a legal solution to the problem, including recourse to WTO dispute settlement."[64] Recently, the EU has given notice that it will launch a broader campaign against alleged PRC government subsidies in other areas. In explaining the rationale, one EU official stated, "We are going to the heart of their system" of export subsidy.[65]

The initial reaction in the United States was more cautious. In the May 2011 semiannual US-China Strategic and Economic Dialogue, the United States raised the issue of export credit finance with the Chinese delegation with the purpose of pressing the PRC to abide by export financing guidelines laid down by the Organisation for Economic Co-operation and Development (OECD). The two sides agreed to "exchange views" on export financing in future meetings.[66] These future talks may be overtaken by events, as some US interest groups are pressing the Obama administration to follow in the footsteps of the EU and initiate countervailing duty proceedings against Chinese companies.

For its part, the Chinese government may be preparing ammunition for any future negotiations over export subsidies. In late February, the PRC Ministry of Commerce leaked an internal (unofficial) report that concluded that the EU has provided WTO illegal R&D funds, export credits, and loans to Europe's largest telecom-equipment vendors. As one security analyst sees it, this is clearly a defensive measure by the PRC, "essentially a gesture and signal of its intention to help Chinese manufacturers obtain a better operating environment in Europe."[67] And in a more direct move, the PRC has formally launched countervailing duty investigations against certain EU agricultural products, leading a prominent European think tank to speculate that "a new trade war is looming."[68]

The Security and Political Challenge

Looming much larger than IP and subsidy obstacles to Huawei's penetration of the US market are difficult and, thus far, intractable issues stemming from deep national security concerns and from a continuing climate of mutual distrust. Since the fall of 2010, members of Congress have increased pressure on the Obama administration with a series of bipartisan letters to the president, cabinet secretaries, and chairpersons of independent regulatory bodies, warning against allowing Chinese investment in the telecom sector or awarding contracts or subcontracts to Huawei (or ZTE). The effort has been spearheaded by Sen. Jon Kyl (R-AZ), but a number of other senators and House members have joined him on particular letters, including Sens. James Webb (D-VA), Sherrod Brown (D-OH), Susan Collins (R-ME), James Inhofe (R-OK), Tom Coburn (R-OK), and Richard Burr (R-NC) and Reps. Sue Myrick (R-SC) and Darrell Issa (R-CA).[69] The letters combine both commercial fears and allegations (unfair subsidies and IP theft) with deeper security fears (ties to the PRC military and possibility of penetrating US security networks). As one letter states, Huawei's position as a supplier could "create substantial risk for US companies and possibly undermine US security."

The congressional pressure also reflects the larger context of increasing cyber attacks on US corporations and government agencies, many of which have been traced back to Chinese sources (though not directly to the Chinese government, which strenuously denies involvement). Fears of industrial espionage merge with more traditional defense espionage to produce a poisoned climate.[70]

Recently, Huawei's presence in the US market has spilled over into the 2012 presidential race. On August 15, two days after he rolled out his presidential campaign, Governor Rick Perry (R-TX) faced criticism for having "welcomed" Huawei investment in Texas. A *Washington Post* news article recited a number of the security concerns surrounding the company, and included a negative question from a member of the bipartisan US-China Economic and Security Review Commission, asking, "Was he [Perry] willing to put short-term economic interests ahead of broad national security concerns?"[71]

Access Denied. On at least three notable occasions over the past several years, Huawei has been denied US acquisitions or contracts based upon security concerns.[72] In its present form, the US security review process for FDI is presided over by an interagency Committee on Foreign Investment in the United States (CFIUS), chaired by the Treasury Secretary but composed also of a combination of commercial/trade agencies and key representatives from defense and intelligence agencies and departments.[73] The committee has broad powers of review and action, including the power to self-initiate a proceeding at any time and to reopen a case if circumstances change after an initial positive vetting. As a practical matter, some corporations have taken advantage of a prefiling, informal CFIUS review to avoid surprises later.

Huawei and 3Com. In February 2008, Bain Capital Partners, an asset management and venture capital company, agreed to withdraw an application for security approval for a $2.2 billion acquisition of 3Com, a network equipment manufacturer. The acquisition, which would have given Huawei a 16.5 percent minority stake, failed to gain a CFIUS go-ahead after extensive discussions between the companies and the government. While CFIUS officials give no explanations for any of their actions, press reports pointed directly to fears that Huawei's ties to the PLA would compromise US security through the introduction of backdoor technology that could monitor or disrupt wireless communications. Classified information was said to link the company directly to the PLA. In the aforementioned open letter and in numerous public comments, Huawei executives have strenuously denied links to the PLA and separately have offered to establish independent "security cells" through which software codes can be compiled and monitored independently.[74]

Whatever the reality of the security threat, the corporate history leading to the 3Com reversal is replete with competitive ironies and twists. After great early success in the modem market, 3Com had difficulty adapting to the rapidly changing wireless equipment scene after 2000, when it had exited the high-end router business as a result of tough competition with Cisco. Struggling without direction among the new consumer applications markets—initial handheld mobile computers—3Com found a new start through a joint venture (H3C) with Huawei whereby it would rebrand and sell its ethernet switching and routing technology and gain access to the growing market for wireless equipment in China. As a part of the deal, H3C created a highly skilled Chinese workforce, mainly from existing Huawei engineers and skilled technicians, and technology sharing was an essential element of the joint venture. The joint venture later gained about one-third of the Chinese market for data-center networking gear. One commentator has stated that 3Com became "primarily a Chinese vendor with an American façade."[75] In 2006, 3Com bought out Huawei, reportedly paying $1.26 billion for H3C's assets and technology, most of which remained located in mainland China. 3Com still struggled in the larger competitive marketplace, and in 2007 Bain Capital proposed to buy the company for $2.2 billion, with minority equity financing (16.5 percent) by Huawei. Throughout the entire period, 3Com had retained important US government contracts for servers, routers, and security equipment. There was speculation at the time that Huawei planned later to move for a complete 3Com takeover, while agreeing to shed defense-related assets.[76] It was at this point that CFIUS stepped in to oppose the deal.

Two years later, in November 2009, Hewlett Packard (HP) acquired 3Com for $2.7 billion, largely as a counter Cisco's aggressive move into its traditional territory. One analyst described the evolving competition, saying, "HP is attacking Cisco's dominance of the market for gear that connects computers just as Cisco move more aggressively into the market for computer systems, where HP is strong . . . 3Com's products, which connect computers inside corporate data centers, complement HP's . . . networking equipment which is used to link PCs to corporate networks."[77] Bizarrely, while Huawei was cut out of a minority stake in the earlier transaction, HP will utilize products designed and produced through

3Com facilities in China. One reason for HP's move was also to shore up its relatively weak position in the Chinese market.[78]

For this study there are two salient points about the CFIUS/3Com episode. First, though not intended, security investment interventions can have a profound impact on global telecom competition, altering the playing field in important ways. Secondly, given complex technological interconnectedness, it is often difficult to hit the precise security target when attempting to seal off a national economy. The US government had not intervened to stop substantial technology sharing in the H3C joint venture that gave 3Com a lucrative share of the PRC market, yet it had in response to a mere 16.5 percent share of a venture in the US market.

3Leaf Patents. In May 2010, Huawei purchased the patent portfolio of 3Leaf, a near-bankrupt Silicon Valley company, for $2 million and hired some of its staff. 3Leaf had developed cloud computing technology that allowed groups of computers to work together as a more powerful system. At the time, Huawei did not file a notice with CFIUS. Only in December 2010, after it discovered that CFIUS was investigating the acquisition and seven months after the assets had been transferred, did the company belatedly give formal notice of its purchases. In February 2011, CFIUS informed Huawei that it would recommend to the president that the company divest itself of all 3Leaf assets.[79]

Given the background of distrust and security suspicions—and given the large amount of money Huawei had expended to learn the ropes of the US political and regulatory system—it is astonishing that the company stumbled so badly again. By early 2010, it was aware that foreign companies routinely played it safe by consulting with CFIUS well before bidding for a property even remotely security related. Huawei officials have argued that they did not think that a $2 million patent purchase rose to the level of CFIUS. To underscore their point, the company's top management briefly considered another extraordinary action: appeal of the CFIUS decision directly to the president, who has final authority in the process. After quick reconsideration, Huawei backed down and accepted the CFIUS divestiture mandate.[80]

Once again, the security and technological results of the government's action are ambiguous. Though Huawei divested itself of the patent portfolio, it had no doubt already reaped technological benefits during at least six months' ownership. It is likely the CFIUS action is best explained for reasons that actually have little to do with the security risks. One, given the background of distrust for Huawei's motives, CFIUS wanted to teach the company a lesson: don't even think of skirting regulatory boundaries. Two, on a more basic political level, CFIUS wanted to assure US political leaders (particularly US senators who had strongly protested the 3Leaf acquisition) that it was tightly monitoring Huawei's corporate activities in the United States.

Beyond CFIUS: The ATT and Sprint Contracts. CFIUS authority does not extend beyond mergers and acquisitions to private contracts or equipment-supply arrangements, yet in the past two years, US government officials have intervened to stop such contracts and equipment-supply deals.

In late 2009, AT&T was considering a large contract to upgrade its network to accommodate 4G technology, and Huawei was a leading contender. AT&T received a call from the head of the National Security Agency informing the company that if it wanted to keep highly profitable contracts with US government agencies, it must exclude Huawei from the bidding. The contract was subsequently divided between Swedish-based Ericsson and French-based Alcatel-Lucent.[81]

In October 2010, Huawei seemed close to winning a similar network structure upgrade contract with Sprint Nextel, the third-largest US carrier. Though the Obama administration had no legal means of stopping the contract, it took the extraordinary step of having Gary Locke, the secretary of Commerce, personally call Sprint's chief executive to express opposition to the pending Huawei contract and to warn that government contracts would be

jeopardized. The award was divided among Ericsson, Alcatel-Lucent, and Samsung, none of which, observers have claimed, matched Huawei in either price or quality in the specific technologies.[82]

The Investment Chilling Impact. There is also a further negative impact of the continuing standoff between Huawei and CFIUS: the unquantifiable, but potentially significant, chilling effect on investment and other transactions. In August 2010, Huawei failed to reach agreement to purchase two US assets, even though the company offered at least $100 million more in each instance.[83]

Motorola had placed its wireless equipment unit on the market. Though it offered substantially less than Huawei, Nokia Siemens Networks bought the unit for $1.2 billion. To bridge the gap with the Huawei offer, which was about 10 percent higher, Nokia Siemens kicked in an additional $150 million in accounts receivable, cash, and some other assets—a gesture that still left the offer shy of Huawei's more solid, clear-cut bid.

A month earlier, in July 2010, Pace Pic, a UK television and top-box manufacturer, announced plans to buy 2Wire, a San Jose, California, based company. Again, Huawei reportedly had the higher offer but was turned down because of fears that the transaction would be slowed (or even vetoed) by the US government review process.

As this study was being completed, the Department of Commerce dealt Huawei another blow when it excluded the company from participation in a project to build and test a national wireless emergency network. The network will be used in future emergencies by police, firefighters, and other emergency personnel. Huawei immediately complained that it had become a pawn in a "geopolitical chess game" and, specifically, that the decision would have a "chilling effect" on its future business plans. In response to queries, an anonymous Commerce Department official said this was a "national security decision" and added, "The specific concerns won't be elaborated on, because we don't conduct national security analyses in public."[84] It is impossible to know how many contracts or potential sales have been aborted due to fears of getting caught up in regulatory morass or of being vetoed at the end of a contractual negotiation. In response, Huawei has mounted a strong, even defiant, counterattack over the past year.

Huawei's Counterattack

Despite the frustrations and failures to date, Huawei officials remain determined to compete in the US market, and they have mounted a sustained and expensive campaign to achieve their goals—including greater transparency regarding its corporate structure, recruitment of high-powered technical executives from competing telecom firms and among the politically connected, an extensive public relations campaign and pushback against business practice and security allegations, and a stepped-up effort to become an important R&D player in the US telecoms sector. Over the past several years, Huawei has attempted to introduce more clarity into its business operations and structure. Though a private company, it has published much greater detail concerning its financial situation. And the recently released 2010 annual report made public the names and (partial) biographies of the company's board of directors.[85] The company's most important US move to get public traction has been the appointment of William E. Plummer as vice president for external affairs for Huawei Technologies (USA). Plummer has quickly emerged as the feisty public face of Huawei in the United States, both politically and tech-savvy.[86]

Plummer is just one of a number of high-profile executive recruits in recent years. Huawei is in process of establishing a worldwide ring of advanced R&D centers, with a key facility planned for Silicon Valley. The Silicon Valley operation is headed by John Roese, former Nortel executive. According to Roese, the US facility will no longer merely augment research in China but will also be tasked with forging ahead with frontier projects, particularly with regard to cloud-computing technology.[87] In addition to

Roese, the company recruited Matt Bross, former chief technology of British Telecom, as copresident of Huawei North America. It also picked up the former sales head of Motorola's European wireless division.

Even in the recent moves, however, Huawei has made miscalculations. Last year, the company sought the advice of the Cohen Group, headed by former Defense Secretary William Cohen. Shunning the Cohen Group's recommendation to establish a wholly separate US company with an independent board and decision-making authority, Huawei opted to establish a new startup, Amerilink Telecom Corp. The new startup ostensibly was created to distribute Huawei equipment software, but in reality it was an (unsuccessful) vehicle to ease the way for the hoped-for Sprint Nextel contract (the company was largely staffed by former Sprint Nextel employees).[88] Amerilink's board is led by William Owens, a former vice chairman of the US Joint Chiefs of Staff, and includes former congressman Richard Gephardt, former World Bank president James Wolfenson, and former deputy Defense secretary Gordon Englund.[89] As the Cohen Group had predicted, however, the US government was not impressed with the startup's capability and independence or with its offer to independently check Huawei's equipment for security risks.[90]

On a more positive front, Huawei has taken a series of internal steps that may pay off over the longer term. In the wake of the 3Leaf standoff, the company appointed a permanent CFIUS compliance officer charged with the responsibility of overseeing a continuous dialogue with the US government to overcome existing distrust and build confidence in the company's motives and intentions in the future. In a very recent move, Huawei has created a global cyber security office and snagged a high-ranking British security official, John Suffolk, to be its first head. Suffolk was previously chief information security officer for the British government, and his new appointment had to be cleared by Prime Minister David Cameron. He will be based in Shenzhen and report directly to CEO Ren.[91]

The company has also taken more specific steps to assure customers (and governments) of the independent security of its equipment. In the United Kingdom, Huawei persuaded the British government and its cyber-security agency, the Government Communications Headquarters (GCHQ), to approve and participate in a new Cyber Security Evaluation Center. At the center, independent analysts will evaluate and scrub down wireless equipment for security risks, including compiling security codes and placing them in escrow. This will be an ongoing process that will scrutinize later upgrades and patches in original equipment. In a similar move in Canada, Huawei has partnered with Electronic Warfare Associates (EWA) to provide third-party verification of the company's products sold in that market. It is in the process of teaming with EWA to establish a security evaluation lab in the United States. It also has offered US customers third-party installation and evaluation of Huawei's products through outside companies (such as Bechtel), again including both original equipment and all upgrades and patches.[92]

Partially in response to the security frustrations and partially in response to a rapidly evolving telecom competitive environment, Huawei has reorganized itself into three separate divisions. The first continues the company's production and sale of infrastructure to networks, the second will build upon recent moves into consumer products and mobile phones, and the third will move the company more rapidly into corporate services and data processes (a move that will bring Huawei into direct competition with broader technology firms such as Cisco and HP).[93]

General Observations

Before setting out specific recommendations, there are several relevant general observations that can provide a context and setting.

The US Investment Landscape and the CFIUS Process. First, beyond the particular challenges in the telecoms and IT sections, Chinese investment in the United States seems set to take off—though from a

very low base. The Rosen and Hanemann study identified some 230 Chinese investments between 2003 and 2010, split almost equally between greenfield projects and acquisitions. They estimate the value at around $11.7 billion, distributed among 35 of the 50 US states. About 170 (74 percent) of the 230 investments originated with private companies, though in value SOEs accounted for 65 percent of the total. One-third of the Chinese investments are in services, with two-thirds going to industrial sectors, including industrial machinery; electronic equipment; and components, energy (coal, oil, gas), automotive components, and medical devices. There has been a substantial increase in these deals since 2007. Chinese investment has not been systematically excluded from the US market.[94]

Further, the two authors conclude that the CFIUS process, in general, "works well to screen out security risks, and most Chinese investments in the United States happen without drama . . . there is no indication that Chinese firms were formally discriminated against when their investments were subject to CFIUS screening."[95] That said, there are troubling incidents and trends. Political pressures on the CFIUS process are rising, fueled by a combination of factors. These include heightened media interest in any PRC investment, competing private interests that stand to gain from blocking a particular investment, and political interests—particularly in the US Congress. Such political motives are a mixture of specific and genuine security concerns and a more general distrust of the PRC, not necessarily rooted in fact. The result has been instances of seemingly random, illogical intervention. These include blocking the Chinese firm CNOOC from acquiring Unocal but allowing a $1 billion Texas oil-shale investment; opposition from policymakers and unions to investment plans in wind power by the Chinese manufacturer A-Power but allowing a $1.5 billion stake in the power utility AES by the Chinese sovereign wealth fund with barely any dissent; and strong opposition to a Chinese investment in a Mississippi new-steel mill, while another Chinese steel company won praise for a sizeable investment in Texas.[96]

CFIUS has extended the erratic incidence to Huawei, which has by no means been totally shut out of the US market. In a continuation of its earlier "surround the cities" tack, the company—without provoking Sprint-like *ex parte* political interventions—has steadily gained contracts with second- and third-tier wireless operators. One such customer is LEAP, a spinoff from Qualcom, and the seventh largest US wireless operator. Since 2006, LEAP has successively purchased base 3G equipment and base stations from Huawei, and it sells Huawei's affordable Android-based smartphone, the Ascend (Best Buy and T-Mobile also sell inexpensive versions of Huawei's Android-based smartphones). Of even greater interest, the Internet wireless provider Clearwire (broadband 4G network that reaches millions of people in the United States) is another large customer. This is ironic, in that Clearwire is majority-owned by Sprint. Clearwire has a contract with Sprint to provide its 4G traffic—at least in part with Huawei equipment.[97]

Security Quandaries and the CFIUS Process. In an analysis published in July 2010, two *Financial Times* reporters posited that US officials were divided over how to handle Huawei and sensitive acquisitions and contracts in the US market through the CFIUS process or other means.[98] So-called pragmatists argue that the United States should approve future transactions because it would allow the government to enforce mitigation agreements that would include security and other strict conditions, including employee screening, third-party audits, and even access to source codes. The pragmatists also argue that US officials cannot cut off all technology interchange, pointing to security alliances and already large sales of products (smartphones) to US customers under other brand names (Motorola, Verizon).

On the other side, many security officials doubt that the United States would gain enough, on balance, to warrant such easing. They also worry that even with stricter safety measures the security of government systems cannot be assured. Though this skepticism stems in part from a visceral distrust of

Huawei as part of China Inc.—whatever the nominal corporate governance—it is also rooted in the primitive state of the art at this point regarding cyber security.

At a recent Washington conference, two noted cyber-security experts—James Mulvenon, one of the authors of the Rand study previously cited, now with the Center for Intelligence Research and Analysis; and James Lewis, a senior fellow at the Center for Strategic and International Studies—presented revealing and important insights into the evolved challenges and dilemmas presented by Chinese telecom companies' global telecommunications supply chains and threats to the security of national communications systems. Though they do not speak for the entire security community, their presentations opened important windows into current thinking. Distilling their comments and conclusions, the following realities stand out as relevant to this study.[99]

- From the outset, global IT infrastructure has been flawed from a security perspective: "The architecture . . . was designed by a group of cyber-punk libertarians who never thought the network would be used for malicious purposes. They thought it would be for scientific communication. . . . They didn't build security into the network. At the fundamental levels, things related to authentication and security were never built into the network, and we've been gluing it onto the network ever since" (Mulvenon).

- Blocking Huawei or other Chinese companies from the US telecom equipment market is defensible but "in the end it's all an illusory exercise" (Mulvenon).

- Given the current state of technology and the pervasiveness of global IT supply chains, a new mind-set must emerge for dealing with cyber-security challenges. "We are going to have to deal with the fact that the old way of thinking about security no longer makes sense. . . . We are going to have to think about new defensive strategies that tolerate the fact that the enemy is inside the wire" (Lewis).

- "There is now a recognition, a painful recognition, that we are going to have a persistent threat inside the network that cannot be removed. There's going to be compromised hardware and software inside the network persistently. . . . We have to be able to figure out how to operate a flawed architecture despite the intrusions. . . . [The] buzzword . . . is active defense, fight through the intrusion, fight through the attack" (Mulvenon).

- The imperatives of the global supply chain dictate technological interdependence. "The global supply chain is not going away. We are all going to be dependent on foreign suppliers. Every product you have in the room includes pieces that were made in Europe, in Asia, In North America, and the question is, how do you know you can trust them?" (Lewis).

- "It is impossible . . . to prevent Huawei from getting inside the US telecommunications market. They have not only surrounded the United States, they are in the United States. So our strategy can't be predicated on building a higher fence and having a more stringent CFIUS process" (Mulvenon).

- Both experts were skeptical that attempts by Huawei (or any other company) to reassure governments or customers that their equipment was immune from malware would pass muster. "Companies will say, 'Inspect us, we're willing to be inspected by a third party.' Of course they are, because the third party isn't going to

find anything. The contamination will come later through updates, through managed services" (Lewis).

- "The issue is not solved by third-party inspection. The industry standard is moving to constant and continuous remote maintenance and upgrades. And that will be impossible to police effectively as time passes" (Mulvenon).

- Finally, though generally skeptical about Chinese motives, both men agreed that, long-term, some sort of global cooperative system is the only answer to the cyber-security challenges. The problem for dealing with the Chinese is twofold. First, while they cannot admit it, Chinese officials fear that the United States is far ahead in cyber technology. Secondly, they are also think that we are "symmetrically more vulnerable" to attack then they are.

- "So people know that their supply chain is potentially vulnerable, and they've sought ways to control it. But the only way we're going to be able to do this over the long term is through some sort of global cooperative system. . . . [Common criteria is] an effort to get suppliers to agree with standards for security that would let them trust products up to a certain level. . . . [But] the Chinese are not quite ready to trust common criteria" (Lewis).

- "There is still a perpetual blind spot on the Chinese side about their own dependencies and their own vulnerabilities on the network. . . . There is still a sense among many . . . that somehow the United States is asymmetrically invulnerable on these issues while China is not. Well, the US is asymmetrically vulnerable. We are more wired, more digital. . . . But every day that goes by, China asymptotically is becoming more of a status-quo power just like we are. And [with] the same blind spots: they are building a smart electric grid that is plugged into the Internet. . . . Security—what security?" (Mulvenon).

Recommendations

Given the extraordinary technological complexity of the cyber-security landscape, the importance of maintaining an open investment policy for the United States, and the difficulty of defending against increased politicization of the investment/security process, this study recommends the following short- to medium-term actions.

Proposals to Expand CFIUS: Proceed with Caution. For the US government, the least defensible actions regarding Huawei have been the *ex parte* interventions to prevent US companies from granting contracts to the company (or, by implication, any other Chinese company) for key portions of the telecommunications sector. Threatening phone calls from the Secretary of Commerce or the head of the National Security Agency contradict and vitiate US demands that other countries adhere to the rule of law and due process. As scholars from the Heritage Foundation (certainly not known as being soft on the PRC) have written, "Determination of a national security risk should not be communicated behind closed doors on unstated grounds by seemingly random government actions. Nor should it be communicated by letters from groups of US Congressmen and Senators, which are appearing with greater frequency."[100]

To rein in congressional ad hoc meddling in Chinese FDI, and to avoid situations such as the Sprint contract intervention, Heritage has recommended expanding the authority of CFIUS to included oversight of equipment supply contracts. The goal is to place authority with a clearly identified government body on the basis of "transparent standards." The

proposal is certainly worth considering, but this would be a very large expansion of CFIUS's reach and authority. Thus, there are difficult issues that must be defined and clarified before going down this pathway.

First, there is the question of where all of this ends. When one moves beyond incoming investments in existing US companies, there is potentially a large universe of transactions that could be included under the same rationale. What about greenfield investments, where there is no US company involved but where security implications are present? What about joint ventures? Should the 3Com-Huawei alliance have been vetoed or the Huawei-Symantec technology transfers in the area of network security? Similarly, should the government become involved in decisions of US carriers to sell rebranded smartphones manufactured in the PRC by Huawei or ZTE?[101] The market for IT equipment and services today is a global market, and this raises the question of how much domestic regulatory decisions really add to US security. What should be the reach of the US government's security process abroad? All of the major players in the telecommunications equipment market—Ericsson, Cisco, and Alcatel-Lucent—manufacture substantial portions of their output in mainland China.[102] Should CFIUS attempt to assess the security dangers from hundreds, even thousands, of these Chinese-produced components and finished products?

Underlying all of these possible extensions is a more fundamental question. As now constituted and employed, does CFIUS have the combination of technical expertise (delivered in a timely fashion) and market foresight to stay on top of a rapidly evolving Internet and IT world? Further, given the state of the art described above by cyber-security experts Lewis and Mulvenon, are these interventions themselves "illusory"?

Heritage acknowledges that standards for increased government oversight do not now exist. (It proposes that the Department of Defense take the lead in formulating new standards.) Such a process will likely be protracted and contentious, raising fundamental divisions over traditional US open-investment policies and potentially new security imperatives.

The bottom line for this study is that, on balance, at this point the downside of expanding CFIUS outweighs the uncertain security gains.

Increased CFIUS Transparency. Pending the outcome of a debate over new powers for CFIUS, the current CFIUS process should be made more transparent. A number of intelligence officials from several administrations have acknowledged that, in the words of former NSA and CIA director Michael Hayden, information on cyber threats is "overprotected."[103] Many analysts believe that without giving away major security secrets CFIUS could provide more detail about the sources of the security concerns, particularly in areas where the government has already attempted to negotiate a mitigation agreement. As a specific case, CFIUS could have explained just what it was about the 3Leaf patents— patented technology is, by nature of the patenting process, public knowledge—that constituted a security threat. Overall, as Heritage scholars again have written, "Some material will be classified. But the tradeoff between security classifications and the ability to promptly and adequately respond to a threat should be weighted more heavily to the transparency side than it is at present."[104]

CFIUS should also consider publishing a more general set of guidelines that would explain the rationale behind its deliberations and decisions.[105] Beyond this, public seminars and conferences explaining the underlying legal framework and CFIUS' interpretation of its role in this framework would help to clear the air and avoid needless future conflict.

There is one factor that gives some urgency to moves to clarify CFIUS rationales in individual cases: the PRC's announced intention, along with new provisional regulations, to screen new foreign investment on security grounds. The US government and key US-China business organizations, such as the US-China Business Council and the US Chamber of Commerce, have protested the vagueness of the proposed new rules, as well as the lack of transparency

in the regulatory process. US action to clarify and provide greater detail on the rationale behind CFIUS decisions would greatly strengthen the hand of US negotiators with relevant Chinese agencies such as the Ministry of Commerce (MOFCOM) and the State Council on Legislative Affairs.[106]

Finally, as this report was going to press, the White House revealed that it had established a task force to evaluate the "opportunities, risks and implications" posed by foreign telecommunications companies in the US market. Unnamed US officials also revealed that while no particular company or country was targeted, Huawei's expansion in the US market was a "key impetus" for the initiative. The decision to establish a White House project moves the process beyond CFIUS. When the task force has completed its work, its conclusions, as they pertain to the controversies surrounding Huawei, should be made public.[107]

Huawei's Role. Huawei, likewise, must be more forthcoming in meeting legitimate US government security concerns. As noted, the company has appointed a compliance officer to work directly and continuously with CFIUS, and it has given global security concerns a top place in its corporate structure. As the analysis in this study has illustrated, however, given the quality of cyber security, it will not be possible to achieve 100 percent safety from present and future malware and system subversion. Still, Huawei would be well advised to build upon the security systems and actions it has already undertaken and to continue to push the frontier with new security technologies as they come onstream.

The British Cyber Security Evaluation Center is one model that can be replicated in other markets. Similarly, use of third-party mechanisms and institutions, such as the Canadian company EWA, could serve as an alternate model. It will also be important for the company to mount an aggressive effort to publicize its new security policies and actions through the media and through technology forums and standard-setting organizations.

In the United States, though rebuffed by key congressional elements, Huawei must persevere by quietly continuing to build alliances with third-tier customers for its products and with state and local officials, like Governor Perry, who are seeking job-creating FDI from Chinese and other international companies.

In addition, though there are risks involved, Huawei's recent strategy of instant and highly vocal rebuttal, both to negative decisions by the US government agencies and to criticisms from members of Congress and outside interest groups, has merit and should be stepped up. As candidates for office in the United States have learned, allowing a negative allegation or aspersion to go without rebuttal, even for a short period, can make it difficult, if not impossible, to gain traction later in the political discourse. The caveat in all of this: Huawei better have its facts correct and solidly documented right out of the box.

The Investment Framework. Huawei has moved to become more open in regard to its governance and its financial structure and condition. It still has a ways to go before the critics will be quieted, though. While it revealed names of its board of directors in the recent annual report, it neglected to note that two board members are members of Ren's immediate family—his daughter and his brother—or that the board's chairwoman is rumored to have worked for the Ministry of State Security.[108] Though this omission itself may not be important, it highlights larger succession questions. Will Ren attempt to keep insular family control over an increasingly complex multinational operation? Or will the company follow the path of other successful international corporations and recruit and reward management excellence through a meritocracy?

Beyond questions of succession, it is also true that very little is known about the internal decision-making apparatus and process outside of Ren's role. As noted earlier in the study, central issues, such as the qualifications and actual powers of the board, have never been disclosed, nor is there any public disclosure of the relations between the Huawei holding company (the so-called shareholders union run by an undisclosed committee) and Huawei Technologies Inc. The company has also declined to make public the criteria by which shares are allocated to Chinese

employees or the share value of stock with which they are compensated if they leave the company. While touting the principles of shareholder equity for its employees, the fact is that its non-Chinese managers and workers (now almost half of the employees) are second-class corporate citizens.

Given the current unanswered questions concerning Huawei's governance and internal operations, the rocky history of Huawei in the United States, and the growing controversies in the United States and other countries over dubious financial and accounting practices of Chinese corporations, Huawei will have to attain the purity of Caesar's wife in order to succeed finally in the US market. In the end, its best course of action is to bite the bullet and take the company public and list it on a US stock exchange, most likely the tech-oriented NASDAQ.

Highly successful multinational companies—Cargill is an example—remain private and unlisted, so taking the company public is not a panacea. But it may constitute a highly significant and important step in the company's drive to convince both investors and public officials that it is just a normal commercial enterprise. Abiding by US or European rules mandating an independent board, transparency for decision making and for compensation, and universally agreed auditing regulations, among other things, would also signal that Huawei was prepared to accept the norms and rules of multinational competition and investor protection.

Huawei officials have been coy about when or if the company will go public, stating vaguely that the current structure has been adequate for present growth. They also advance more specific reasons for maintaining the private status, none of which is entirely credible. First, they argue that public listing will introduce "distractions" and limit the company's flexibility.[109] This answer reveals nearsightedness about the current and future circumstances under which Huawei will operate. Highly successful multinational companies from many countries have benefitted and thrived as a result of greater investor and public confidence based on adherence to regulatory disciplines and transparency associated with public listing. Indeed, Huawei's sister IT company, ZTE, has been listed on the Hong Kong stock exchange for some years.

Huawei argues that there are very practical downsides to public listing for a company owned by its employees. A public listing would make many employees instant millionaires, potentially resulting in a huge loss of talent as many would retire or leave.[110] This is certainly a danger, but there are many ways to structure a public offering that would avoid or lessen this problem. Benefits and stock redemption could be stretched out over time, or even put off entirely until some future date—as is done with compensation for high-tech executives in Western economies. Huawei's argument here seems disingenuous; a bit of creative thinking can solve this in an entirely legal manner.[111]

In the end, as blogger and Indiana University China expert Scott Kennedy has opined, "If Huawei had to comply with SEC disclosure laws and subject itself to the scrutiny of shareholders, CNBC's Squawk Box and Bloomberg, that might give the US government and others the confidence they need to allow Huawei to sell its products in the US without regulatory obstacles or political intrusion."[112] Further, the *Economist* pointedly concluded in a recent analysis, "Huawei appears to want to have it both ways: remaining a culturally Chinese company, perhaps even family run, while competing with publicly traded Western giants. This is unlikely to work."[113]

Behind both of the above comments is a larger doubt concerning Huawei that public listing might assuage, though not totally erase: that is, that behind-the-scenes elements of the Chinese government still pull the strings and that even Huawei could well be subject to arbitrary interventions. As Adam Segal, China expert at the US Council on Foreign Relations, has noted: "Private companies in China are always wondering what the government is going to want next."[114] As a publicly listed company on one or more international stock exchanges, Huawei would not be immune from such subventions, but Beijing might be more cautious, given the blow such a move would inflict on Huawei's reputation as a reliable partner and competitor.

Trade: Subsidies. In the world of international competition, neither Huawei nor its Chinese competitor, ZTE, can be classified as infant companies. Indeed, they are lusty, brawling adolescents. Pressure is mounting in both the United States and Europe to take countermeasures to ensure that their companies are not shut out of contracts and markets as a result of outsized exports credits and subsidies. The US Export-Import Bank has begun tracking export credits and subsidies granted by China (and other large developing countries such as Brazil and India). In its *2010 Competitive Report*, the bank warned that "the Chinese export team [is] a $40–50 billion-a-year behemoth that is regularly competing with the OECD/G-7 exporters in third markets."[115] In a June 15, 2011, speech, Export-Import Bank CEO and chairman Fred Hochberg took direct aim at Huawei and Chinese export subsidies, saying, "One of the central reasons [Huawei's] growth is so strong is they're backed by a $30 billion credit line from the Chinese Development Bank. This allows Huawei to have a far lower reduced cost of capital and, importantly, offer financing to their buyers at rates and terms that are better than all their competitors around the globe. This financial model not only affects the bottom line of companies trying to compete, but also affects the bottom line of our economy. . . . None of the G-7 countries provide levels of financing anywhere near those of the Chinese Development Bank." Hochberg concluded his remarks with a warning, saying we will "send a clear message to China . . . we are not going to sit by idly and play by a certain set of rules that other countries don't play by."[116]

On August 9, 2011, five members of Congress signed a letter to the secretaries of Defense and Energy and the chairwoman of the SEC protesting an award by a University of Tennessee computer engineering center to a company that would utilize Huawei security technology. Though the letter raised major security concerns regarding Huawei, the congressional group specifically cited Hochberg's speech and condemned Chinese government export subsidies as unfair trade practices. The letter notes, "As Huawei continues to increase its share of the global market, the US government has not yet pursued trade actions against Huawei for the massive support it enjoys from the government of the PRC. However, if Huawei's government support and artificially low prices appear to be the company's lynchpin for expanding its footprint in the United States, then our nation will have no choice but to seek appropriate trade remedies."[117]

As noted in the introduction to this study, Huawei responded with exasperation to the new allegations, calling them tired and hackneyed. At the same time Huawei belatedly provided more information about the credit lines in letters to select US officials. It now acknowledged that a total credit of $40 billion had been made available to Huawei customers through memoranda of understanding with the China Development Bank; but it then claimed (for the first time) that Huawei customers have only tapped $2.9 billion from this credit pool since 2005. In the February letter cited at the outset of this study, Huawei stated that "$10 billion had been loaned to our customers from the China Development Bank." It also listed the total available for credits lines as $30 billion.[118]

Besides changing the numbers, dates, and terms of reference, the company undermined its own defense by stating that this type of vendor financing "is not unique to Huawei, but is standard and accepted practice in the international telecommunications industry." This is disingenuous in that the very size of the credit potential ($40 billion for one company) and the potential of an open spigot can and has constituted a highly potent allure for equipment and network buyers—particularly resource-stretched developing economies. In January 2011, Chen Yuan, chairman of the China Development Bank, boasted of the bank's central role in China's high-tech competitive rise, saying, "Our support for Huawei, ZTE, and other high-technology companies has opened up the overseas market. We have become the principal source of finance for our country's overseas investments."[119]

One could debate the exact amount of the subsidy endlessly; but the fact is that given the protests of US and European companies and rising political

pressures overall, it is increasingly likely that the United States and the EU will take unilateral countervailing duty actions against Huawei (and ZTE) if the PRC continues to provide large-scale export-credit subsidies to their customers. Alternatively, they could bring a WTO case charging violation of China's obligations under the WTO subsidy code.[120] Preliminary gestures from Chinese agencies may indicate that the PRC is preparing a tit-for-tat campaign. Even as a tactical move, this would be unwise, particularly in light of the PRC's announced goal of huge increases in outward investment.

Under the circumstances, given the strong worldwide competitive positions of both Huawei and ZTE, the PRC would be well advised to signal that it is ready to negotiate terms for joining the OECD disciplines on export subsidies and buyer credits. Specifically, the PRC should join the 1978 Arrangement that set forth restrictions on export financing and the 1991 Helsinki Package that clarified certain rules with regard to tied aid for developing countries.[121] While an unusual action for a corporation, it would also be wise for Huawei, in its quest for acceptance in the US market, to signal that it no longer needed access to the $40 billion slush fund for buyers of its equipment and services.

Conclusion

The 2005 Rand study described Huawei as an essential element of the Chinese military/industrial complex—the digital triangle—allied in turn with the PLA and with high-level research institutes whose mandate was to provide funds and resources to budding "national champion" firms in the telecommunications and information technology sectors. As this study has noted, there is great plausibility to the Rand thesis in explaining the early history of Huawei and other Chinese IT companies.

But since 2000, the story has become ever more complex and the future less predictable. Whatever the combination of government support and entrepreneurial grit that explains Huawei's first decade, the company has emerged as a major player in international competition, with deeply embedded roots in an often arbitrary, authoritarian polity and ambitions to compete toe-to-toe with the top telecom firms from around the world.

Both the Chinese government and Huawei's corporate leaders have moved into unknown territory. Two broad future paths seem equally possible. On one course, Huawei will take on the attributes of other successful multinational corporations with publicly traded stock, the transparency mandated by developed countries' regulators, and both research facilities and corporate management dispersed throughout the world. It will abide by OECD subsidy guidelines and operate within broader WTO disciplines, much as a General Electric, a Siemens, or a Samsung competes today. All of this assumes that the PRC government will stay its hand, recognizing that globally competitive telecom companies further its goal of peaceful development and prosperity for China's citizens.

Alternatively, either from an insularity and failure of corporate vision or as a result of dictates from the still-dominant Communist Party bureaucracy, Huawei could hold back, remain a privately-held corporate entity, retain an opaque decision-making apparatus, and attempt to hold onto government favors. Skeptics argue that, given the Chinese government's dependence on advanced cyber technology for both defensive and offensive military strategies, it will always hold IT companies on a short rein, whatever these companies' outward legal status.

In the end, much will depend upon the broader trajectory of US-China relations. Should cyber incidents escalate or bilateral relations deteriorate from increased tensions in the Taiwan Straits, the South China Sea, or other strategic areas around the world, this will undoubtedly redound into high-technology investment and contractual relations, particularly in the IT sector. Similarly, should there be an escalation of the politicization of the CFIUS resulting in a sweeping expansion of China-targeted investment and contract restrictions, Huawei and other Chinese IT companies will find it hard to

compete in the US economy—and the PRC will undoubtedly retaliate in kind.

All of this will be played out against the reality that for the foreseeable future both China and the United States will operate in a cyber-security world where certainty is unattainable and common standards for cooperation are elusive for both technological and political reasons. This may not be satisfactory, but it is a basic fact that both sides must accept and somehow work through.

Appendix:
The Endless, Porous Telecoms Supply Chain

Even without political pressures, Chinese investment in the US telecoms, wireless, and Internet sectors presents huge challenges in balancing national security threats against the benefits of an open economy. In the recent US-China Economic and Security Commission's report on national security, the telecom sector, and the PRC (cited throughout this paper), there is a fascinating section that describes the manifold potential security risks along the entire communications supply chain. Starting with long-haul fiber (cables), the report traces the growing multinational corporate alliances, joint ventures, research alliances, and international-standards procedures that undergird development of routers, switches, and hubs; WiMAX/WiFi (network and network control devices and protocols for wireless networking); applications software; network security products; handsets and smartphones; and wireless headsets, earpieces, and Bluetooth (an open wireless technology that allows devices to exchange data over short distances).[122]

Given the context and the commission's longstanding skepticism about the motives and impact of Chinese government policies, the section was likely written to sound the alarm against PRC incursions into both US defense and economic institutions. But the total impression conveyed by a close reading of this analysis is that attempts to intervene or bar access at any single segment of the telecom supply chain are likely to be futile and self-defeating.

For this paper, two illustrative examples will suffice: network security products and software, and smartphones. Along with other European and American companies, Huawei has recently moved into the area of network security software and manufactured products. In 2008, it entered into a joint venture with Symantec, a major US security and storage software vendor that controls the widely used Norton antivirus and security technology. A new company, Huawei Symantec, was established with 51 percent ownership by Huawei and 49 percent by Symantec. The headquarters are in Chengdu, China, and the company has since created four R&D centers in the PRC with the aim to marry Huawei's expertise in telecoms infrastructure with Symantec's leadership in security software. The new company quickly established itself as a global competitor in the security and storage appliance market, with 4,000 employees and a presence currently in more than forty countries. In 2010, it claimed over 1,000 customers and global revenues of $500 million, including security solutions crafted for a number of American companies.[123]

Separately, in Britain, Huawei has developed close commercial relations with British Telecomm (BT), the leading IT vendor. Beginning with an initial multimillion dollar deal in 2005, Huawei evolved as a major supplier for key elements of BT's advanced communications networks, including BT's current £10 billion upgrade of its networks. This all has transpired despite continuing concerns expressed by elements of the British intelligence establishment. In an attempt to mollify security critics, Huawei—with the blessing of Britain's top IT risk regulator—created a Cyber Security Evaluation Center in 2010 to test equipment and software to be used in the British market and by the British government. It will work in close cooperation with GCHQ, the government's main cyber-security agency.[124]

Explaining the rationale and the dilemma Britain and most other countries face, one analyst noted that absolute security certainty could be obtained only "if BT was to manufacture and install all the hardware and all the software itself"—clearly an impossibility.[125] The United States faces the same dilemma on

a larger scale in that US global security responsibilities and the US defense establishment dwarf those of Great Britain. But as this and other illustrations underscore, there are no easy answers. For instance, should CFIUS have intervened to stop the Huawei-Symantec joint venture? Conversely, should the US government encourage Huawei, either alone or with Symantec, to establish a cyber-security evaluation center on the model of the British unit? For all its wealth of information relating to security products and software, the US-China commission basically punted on recommendations regarding the Huawei/Symantec alliance. It expressed worry at the lack of transparency with regard to the operations and management of the joint venture, stating rather lamely that "this could raise concerns in some quarters regarding potential national security issues." But it then admitted that "no specific allegations have been made against the [joint venture], and it has emerged as a significant competitor in the network security field."[126]

Along with a number of other IT companies, Huawei and ZTE have moved rapidly forward in the handset/mobile-phone sectors and are accruing significant market share particularly in Asian markets, which have been early adopters of 4G technologies. They are competing with Motorola, Ericsson, Samsung, and Apple for both hardware and software products (Huawei's new Android open-source phone is a recent, quite competitive example). In addition, both companies have introduced new lines through relabeling products for established phone companies such as Verizon and T-Mobile.[127]

The China commission staff report describes the risks and vulnerabilities of smart phones to "malicious activity" such as "Trojan horse" programs that can infect a phone, turn it into a "zombie," and in turn infect the underlying computer system.[128] But because the use of smartphones not manufactured in the United States is already ubiquitous, the report in effect admits that there are no practical solutions to systemic attacks through the thousands of individual sets. Interestingly, in terms of government security needs, the report suggest that the most important defense will be multiple and flexible hardware and software purchases that can operate across numerous spectrum types. It says, "By using a broad spectrum purchasing approach, security can be enhanced by having utilization capabilities across a wide variety of hardware and data transmission protocols . . . mobile devices are relatively inexpensive and easily moved from region to region." The alternatives of proprietary hardware and closed networks are both "costly and ineffective from an economic and mobility standpoint."[129]

In this instance, no doubt maddeningly for those deeply suspicious of the PRC or Chinese IT companies, there are no CFIUS interventions available.

Notes

1. US-China Economic and Security Review Commission (USCC), "The National Security Implications of Investment and Products from the People's Republic of China in the Telecommunications Sector," January 2011, 34–35, www.usc.gov?REP/2011/FINALREPORT:TheNationalSecurityImplicationsofInvestmentsandProductsFromThePRCintheTelecommunicationsSector.pdf (accessed October 25, 2011).

2. "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, Office of the National Counterintelligence Executive, October 2011, Washington, DC.

3. Siobhan Gorman, "U.S. Works to Counter Electronic Spy Risks," *Wall Street Journal*, November 12, 2011.

4. Kandaswami Subramanian, "Joe Biden's Visit to China—Analysis," Eurasia Review, www.eurasiareview.com/24082011-joe-biden%E2%80%99s-visit-to-china-analysis (accessed November 8, 2011).

5. Organisation for Economic Co-operation and Development (OECD), *The Export Credits Arrangement: 1978–2008* (Paris: OECD, 2008). See also Gary Clyde Hufbauer, Meera Fickling, and Woan Foong Wong, "Revitalizing the Export-Import Bank" (Policy Brief 11-6, Peterson Institute for International Economics, Washington, DC, May 2011).

6. "The Long March of the Invisible Mr. Ren," *Economist,* June 4, 2011.

7. Robert Olsen, "Huawei's Open Letter to US Investigators," *Forbes*, February 24, 2011. For a recent analysis of Huawei's frustrated effort to break into the US market, see Kathrin Hille, Stephanie Kirchgaessner, and Paul Taylor, "Access Denied: China and the US," *Financial Times,* April 8, 2011.

8. David Barboza, "China Telecom Giant, Thwarted by US Deals, Seeks Inquiry to Clear Name," *New York Times*, February 26, 2011.

9. Chris Buckley and Zhou Xin, "China Decries US Investment 'Obstruction,'" Reuters, February 21, 2011.

10. Diana ben-Aaron, "Nokia Siemens Postpones $1.2 Billion Motorola Deal Again," Bloomberg, March 9, 2011, www.bloomberg.com/news/2011-03-09/nokia-siemens-motorola-deal-won-t-close-in-first-quarter.html (accessed June 13, 2011); and Geoff Duncan, "Chinese Regulators Put Brakes on Motorola/Nokia Siemens Deal," Digital Trends, March 9, 2011, www.digitaltrends.com/mobile/chinese-regulators-put-brakes-on-motorolanokia-siemens-deal (accessed June 13, 2011). The deal was finally cleared at the end of April: see Owen Fletcher and Aaron Back, "China Approves Motorola-Nokia Siemens Deal," Dow Jones Newswires, April 21, 2011.

11. Tan Yingzi, Zhong Nan, and Meng Jing, "M&A Plan Worries US Experts," China Daily, February 18, 2011, http://usa.chinadaily.com.cn/epaper/2011-02/18/content_12038880.htm (accessed October 25, 2011).

12. Letter from Senators Jon Kyl (R-AZ), James Imhofe (R-OK), Tom Coburn (R-OK), and James DeMint (R-SC), and Rep. Sue Myrick (R-SC) to Secretary of Energy Steven Chu, Secretary of Defense Leon Panetta, and Securities and Exchange Commission chairwoman Mary Shapiro, Washington, DC, August 9, 2011. According to congressional staff, the objective of the letter was for the contract to be rescinded: for details, see Eli Lake, "Computer Lab's Chinese-Made Parts Raise Spy Concerns," *Washington Times*, August 16, 2011.

13. William Plummer to Secretary of Energy Steven Chu, August 16, 2011 (in possession of author).

14. Plummer to Chu, August 16, 2011; Lake, "Computer Lab's."

15. US Department of Defense (DOD), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: US Department of Defense, 2011). The reference to Huawei in the DOD report deserves further explanation and background.

The phrase "close ties to the PLA" seems first to have appeared in the 2008 version of the same annual report. As with the rest of the statements in annual reports on PRC military and security developments, the phrase is not accompanied by a source or explanation of just what the "ties" entail (though there is reference in earlier reports to R&D connections). Critics of Huawei in the United States have repeatedly referenced this phrase and assertion as if it were dispositive. With Huawei's direct challenge to the veracity of the statement, the DOD should document the "ties to the PLA" statement, or at least give some detail as to the alleged connection between the company and the PLA.

16. William E. Plummer (Huawei) to Secretary of Defense Leon E. Panetta, August 24, 2011 (Contained in e-mail from Plummer to the author, September 9, 2011). Plummer stated in the letter that Huawei generated only 0.1 percent of its 2010 revenues from PLA contracts and less than 0.5 percent of its revenues from the Chinese government.

17. John Tkacik Jr., "Trojan Dragon: China's Cyber Threat," *Backgrounder*, no. 2106 (Washington, DC: Heritage Foundation, February 8, 2008), www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat (accessed October 25, 2011). See also relevant sections of USCC, "National Security Implications."

18. Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York: Asia Society and Woodrow Wilson International Center for Scholars, May 2011), www.bizjournals.com/sanfrancisco/pdf/FDI_FINAL.pdf (accessed October 25, 2011).

19. Ibid.

20. It should be noted that Huawei has a smaller, sister Chinese telecommunications company, ZTE Corporation. Though this study will deal with ZTE only in passing, its history both parallels and contrasts with Huawei's. A group of companies associated with the Ministry of Aerospace Industry established ZTE in 1985. It is now a publicly traded company and listed on both the Shenzhen and Hong Kong stock exchanges. In 2010, it had revenues of about $10.5 billion, about one-third the size of Huawei's revenues. Like Huawei, ZTE first specialized in producing network gear that was cheap but reliable. It has since branched out into the mobile-phone handset market, and is among the top ten makers of handsets and one of the top six wireless equipment manufacturers today. Generally, it markets its handsets to other companies without branding them with its own name. ZTE has been called the quiet giant, and it typically shuns the spotlight. It has a prickly relationship with Huawei (they have sued each other over alleged patent violations), and ZTE is said to be irritated at what it considers Huawei's highly public political blunders in the United States. For details on ZTE corporate history, see USCC, "National Security Implications"; and ZTE Corporation, *Annual Report*, 2010, wwwen.zte.com.cn/en/about/investor_relations/circular/201103/P020110328621200621489.pdf (accessed October 25, 2011).

21. Two journalists have provided recent in-depth analyses of Huawei's rise and current challenges. See John Pomfret, "History of Telecom Company Illustrates Lack of Strategic Trust between US, China," *Washington Post,* November 10, 2010; and Sheridan Prasso, "What Makes China Telecom Huawei So Scary?" *Fortune,* July 28, 2011. See also USCC, "National Security Implications." This study will only take note of, without delving into, the debate over whether there are truly private companies in the PRC. Studies by the Asia Society and the USCC staff, cited throughout this paper, accept the distinction between SOEs and private corporate entities in China, but others are skeptical. Derek Scissors of the Heritage Foundation is doubtful that truly private companies exist, particularly in the telecommunications sectors. In comments on the paragraph containing this note, Scissors stated: "Relative freedom, maybe. Private sector operation, no. . . . Huawei can deny formal state ownership of shares, but it wouldn't be tolerated as a truly private company." Comments to the author, July 9, 2011. Scissors points to the 2006 PRC ownership guidelines that list telecommunications as one of the sectors where the state must have "absolute control." See Zhao Huanxin, "China Names Key Industries for Absolute State Control," China Daily, December 19, 2006, www.chinadaily.com.cn/china/2006-12/19/content_762056.htm (accessed October 25, 2011). As demonstrated in the text above, however, Huawei has tackled the challenges of international competition by adopting advanced tactics typical of successful multinationals, seemingly unencumbered by bureaucratic hindrances.

22. Huawei, "We See beyond Telecom," *Annual Report*, 2010, www.huawei.com/en/about-huawei/corporate-info

/annual-report/annual-report-2010/index.htm (accessed October 25, 2011); Juha Saarinen, "Analysis: Who Really Owns Huawei?" ITnews, May 28, 2010, www.itnews.com.au/News/175946,analysis-who-really-owns-huawei.aspx (accessed October 25, 2011). A recent unclassified Central Intelligence Agency report has provided more details, using Chinese press sources, on Huawei's corporate structure. A new board of directors was elected in December 2010, at which time the number of directors was increased from nine to thirteen. In addition, a five-member supervisory board was also was chosen by the employee representatives. See "Huawei Annual Report Details Directors, Supervisory Board for First Time," Open Source Center, US Central Intelligence Agency, October 5, 2011, www.fas.org/irp/dni/osc/huawei.pdf (accessed November 9, 2011).

23. Evan S. Madeiros et al., *A New Direction for China's Defense Industry* (Santa Monica, CA, and Washington, DC: Rand Corporation, 2005), ch. 5, www.rand.org/pubs/monographs/2005/RAND_MG334.pdf (accessed October 25, 2011).

24. Ibid., 206.

25. Xu Huio, Wan Yiqian, and Pei Degni, "A Study on Risk Perception and Risk Identification in the Internationalization Process of Chinese Hi-Tech Enterprises: A Case Study of Huawei Technologies," *Frontier Business Research on China* 2, no. 3 (2008): 458–81. For more on the government connections, see Bruce Gilley, "Huawei's Fixed Line to Beijing," as seen in Silicon Investor, posted December 26, 2000, from *Far Eastern Economic Review*, December 28, 2000–January 4, 2001, www.siliconinvestor.com/readmsg.aspx?msgid=15084108 (accessed October 25, 2011).

26. Qing Mu and Keun Lee, "Knowledge Diffusion, Market Segmentation and Technological Catch-Up: The Case of the Telecommunication Industry in China," *Research Policy* 34, no. 6 (August 2005): 759–83. In 1997, the PRC was not yet a member of the World Trade Organization and thus still had freedom to change tariff rates at will. In the late 1990s, the Ministry of Posts and Telecommunications began organizing annual "coordinating conferences" that encouraged the use of indigenous equipment to selected domestic manufacturers. Through these "assignments," Huawei gained millions of digital automatics switching orders in succeeding years.

27. Ibid., 773–79. See also Madeiros et al., *A New Direction*, 206, 231–51. The Rand study states, "Through Program 863, the state sought to intensify government-university partnerships in particular, as well as to link centrally directed money with smaller-scale, commercially driven innovation by public-sector spin-off firms at the local level," 333.

28. Ming Shuliang and Ouyang Changzheng, "Wiring China for the Next Telecom Era," Caijing.com (English edition), December, 2007, http://english.caijing.com.cn/2008-02-25/100049440.html (accessed October 25, 2011). The backstory regarding this support for Huawei and other companies reveals a more complicated set of factors. It was part of an effort, thus far unsuccessful, by the Chinese government to establish a national standard (TD-SCDMA: TD for short) for third-generation (3G) mobile phones that would compete against other standards in international competition. Three competing standards championed by the United States and EU are the CDMA/2000 and the WCDMA, and WiMAX, which utilizes the same frequency base as the TD. China's attempts to force-feed the TD standard in international competition have been analyzed by Richard Suttmeier. See US-China Economic and Security Review Commission, *Hearing on China's Industrial Policy and Its Impact on US Companies, Workers, and the American Economy*, 111th Cong., sess. 1, March 24, 2009, www.uscc.gov/hearings/2009hearings/written_testimonies/09_03_24_wrts/09_03_24_suttmeier_statement.php (accessed June 13, 2011).

29. Mu and Lee, "Knowledge Diffusion." Though Huawei's claim that over 40 percent of its employees consist of R&D staff may be exaggerated, it clearly attempted to recruit the best and the brightest in the domestic and foreign telecoms pool.

30. Sunny Li Sun, "Internationalization Strategy of MNEs from Emerging Economies: The Case of Huawei," *Multinational Business Review* 17, no. 2 (2009): 129–55.

31. Huio, Yiqian, and Degni, "A Study on Risk Perception"; and USCC, "National Security Implications."

32. Mu and Lee, "Knowledge Diffusion"; Pomfret, "History of Telecom Company."

33. Huio, Yiqian, and Degni, "A Study on Risk Perception." For a detailed analysis of Huawei's rapid rise to equipment dominance in Argentina's telecommunications

market, see Janie Hulse, *China's Expansion into and US Withdrawal from Argentina's Telecommunications and Space Industries and the Implications for US National Security* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2007).

34. USCC, "National Security Implications," 34–35.

35. Huio, Yiqian, and Degni, "Study on Risk Perception"; Pomfret, "History of Telecom Company." Huawei recently contracted again with IBM to aid in its drive to become a major international producer of tablet computers, smart phones, and cloud computing. It is seeking "branding" advice on future product positioning. See "IBM Hired by Huawei for Branding Advice on Expansion into Tablets, Cloud," Bloomberg, September 15, 2011.

36. Sun, "Internationalization Strategy of MNEs."

37. Pomfret, "History of Telecom Company." Pomfret notes that Ren traveled by bus while lugging a suitcase full of cash, as there were no Chinese credit cards at that time.

38. USCC, "National Security Implications"; Sun, "Internationalization Strategy of MNEs"; and Huio, Yiqian, and Degni, "A Study on Risk Perception."

39. US-China Economic and Security Review Commission, *Hearing on China's Industrial Policy and Its Impact on US Companies, Workers, and the American Economy*, 111th Cong., sess. 1, March 24, 2009, 131–32, www.uscc.gov/hearings/2009hearings/written_testimonies/09_03_24_wrts/09_03_24_suttmeier_statement.php (accessed June 13, 2011).

40. Pomfret, "History of Telecom Company."

41. Huawei, "We See beyond Telecom"; and "Long March," *Economist*.

42. Ariel Tung, "Huawei Longs for Breakthrough in US," China Daily, September 9, 2011, http://usa.chinadaily.com.cn/weekly/2011-09/09/content_13655416.htm (accessed October 25, 2011).

43. Prasso, "What Makes?"

44. USCC, "National Security Implications," 23; and Hille, Kirchgaessner, and Taylor, "Access Denied."

45. Pomfret, "History of Telecom Company." Huawei ranks first in the developing world.

46. Sun, "Internationalization Strategy of MNEs"; Hille, Kirchgaessner, and Taylor, "Access Denied"; and "Long March," *Economist*.

47. Huawei, "We See beyond Telecom"; Huio, Yiqian, and Degni, "A Study on Risk Perception"; and USCC, "National Security Implications," 14.

48. Hulse, *China's Expansion*.

49. Jamil Anderlini et al., "Industrial Espionage: Data out the Door," *Financial Times,* February 1, 2011, www.ft.com/cms/s/0/ba6c82c0-2e44-11e0-8733-00144feabdc0.html (accessed June 13, 2011). See also USCC, "National Security Implications," 17–18.

50. Jamil Anderlini, "Motorola Claims Espionage in Huawei Lawsuit," *Financial Times,* July 22, 2010, www.ft.com/intl/cms/s/0/616d2b34-953d-11df-b2e1-00144feab49a.html (accessed June 13, 2011); USCC, "National Security Implications," 17–18. Motorola did not claim that Huawei had any direct contact with the absconding Motorola official, however.

51. One academic source has claimed that Cisco first offered to make a deal whereby it would give up all of its low-end products to Huawei if Huawei would concede the high-end market to Cisco. Huawei refused the offer; see Sun, "Internationalization Strategy of MNEs."

52. For a study of the use of patents for strategic purposes, see Bronwyn Hall, "Exploring the Patent Explosion" (NBER Working Paper 10605, National Bureau of Economic Research, Cambridge, MA, July 2004).

53. Olsen, "Huawei's Open Letter." Care should be taken in evaluating these numbers: they do not speak to patent quality. Patent experts have noted that in China patent standards are lower than in Western countries. Still, the fact that Huawei has continually increased international filings means that it aims to achieve recognition beyond China's border. For more on the general topic, see "Patents, Yes: Ideas, Maybe," *Economist,* October 14, 2010.

54. "And the Winners Were . . ." *Economist*, December 10, 2010. The *Econonist* has recently called Huawei "China's brightest technology star." See "Long March," *Economist*.

55. In recent days, another very late comer to telecoms competition—Google—has adopted an identical defensive IP strategy. In order to protect itself from patent litigation, Google bid almost $1 billion for the patent assets of Nortel, the Canadian telecom company that is in bankruptcy. See Claire Cain Miller, "Google Bids $900 Million for Nortel Patent Assets," *New York Times,* April 5, 2011.

56. Kathrin Hille and Paul Taylor, "Huawei Declares Truce with Motorola," FT.com, April 13, 2011, www.ft.com/intl/cms/s/0/b6813068-65f6-11e0-9d40-

00144feab49a.html#axzz1bprb7c3O (accessed October 25, 2011); Kathrin Hille and Paul Taylor, "Relief for Huawei as It Settles with Motorola," FT.com, April 13, 2011, available at www.ft.com/intl/cms/s/0/9b767044-65f6-11e0-9d40-00144feab49a.html (accessed June 13, 2011); and USCC, "National Security Implications," 17–18. IP clashes have also erupted between Ericsson and ZTE, the SOE that is another emerging telecoms power. Ericsson filed an IP suit against ZTE in Europe in 2010. On April 11, 2011, ZTE filed a countersuit in the PRC with the goal of prohibiting sale of the named products in that market. See Owen Fletcher, "ZTE Sues Ericsson in China, Escalating Clash," *Wall Street Journal,* April 12, 2011. Of even greater interest, increasingly bitter IP disputes have broken out between Huawei and ZTE. Huawei has sued ZTE over alleged patent and trademark violations in three European countries. In turn, ZTE has charged Huawei with patent violations in the PRC. See Kathrin Hille, "Huawei Sues Rival ZTE over Patents," *Financial Times,* April 28, 2011; and Lee Chyen Yee, "ZTE Sues Huawei in China for Patent Infringement," Reuters, April 29, 2011.

57. For details of the burgeoning patent wars, see Richard Waters, "Tech Patent Arms War Reaches New Level of Intensity," *Financial Times,* March 21, 2011; Steve Lohr, "A Bull Market for Tech Patents," *New York Times,* August 17, 2011; and Brian Womack and Zachary Treuer, "Google to Acquire Motorola Mobility for $12.5 Billion," Bloomberg, August 15, 2011.

58. For a sample of the critics, see Steve Lohr, "A Bull Market for Tech Patents," *New York Times,* August 17, 2011; and Steven Pearlstein, "High Tech's Patented Battle Maneuvers," *Washington Post,* August 21, 2011.

59. Olsen, "Huawei's Open Letter." In its attempts to defend the use of Chinese government credit lines, Huawei has revised the baseline numbers over the course of 2011. In the February letter, Huawei identified a pool of $30 billion from two memoranda of understanding (MOUs) with the China Development Bank (CDB). The letter also stated that "US$10 billion has been loaned to our customers from the China Development Bank." In an August 9, 2011, letter to the US Secretaries of Defense and Energy, however, Huawei upped the total available credit to $40 billion (the second CDB MOU apparently was an add-on, not a supplement to the first MOU). But then Huawei stated that only $2 billion had actually been drawn down by its customers since 2005. It thus shortened the dates for the calculation, omitting earlier credits from the years when the company was clawing its way into the international competitive arena. See William B. Plummer, vice president, external affairs, Huawei, to Secretary of Defense Leon E. Panetta, August 16, 2011. These issues are further analyzed in the text.

60. The degree to which Huawei will be vulnerable to attack under WTO subsidy rules is not entirely clear. WTO subsidy provisions do hold export credits in violation if they are used "to secure a material advantage." Annex 1 to the WTO Agreement on Subsidies and Countervailing Measure, however, does carve out an exception for a 1979 Organisation for Economic Co-operation and Development (OECD) export-credit agreement setting mutual terms and limitations on export credits (and for nations that abide by that agreement even though not among the original twelve signers); World Trade Organization, "Annex 1 to the Agreements on Subsidies and Countervailing Measures," art. 3, item (k), Switzerland, 1995. Subsequently, the WTO Appellate Body in the case of Brazil-Aircraft hinted that beyond the OECD exception there might be instances where an export subsidy was not used to provide a material advantage. This has confused legal scholars, many of whom have expressed skepticism about the practical application of this potential reprieve. In any case, the PRC is not a party to the OECD arrangement, nor does it abide by the terms of the arrangement. The author is grateful to Simon Lester, a noted WTO legal scholar, for explaining the background to this debate in an e-mail, Simon Lester to Claude Barfield, July 18, 2011. The Brazil-Aircraft case cited in the e-mail also dealt with alleged unfair subsidies, in this case by the Brazilian government.

61. Over the past two years, the favorable terms of the credit line have been crucial to Huawei's landing large contracts with Argentina's largest landline company and with Latin America's largest mobile phone carrier. For details, including usually secret specifics about the terms of the loans, see: "Huawei's $30 Billion China Credit Opens Doors in Brazil, Mexico," Bloomberg, April 25, 2011. The article also notes that China is not alone in providing favorable credit lines; the Swedish Export Credit Corporation issued a similar $1 billion credit line for an Ericsson contract in Russia.

62. Export-Import Bank of the United States, *Annual Report* (Washington, DC: Government Printing Office, 2010).

63. The major EU wireless manufacturers (Ericsson and Nokia-Siemens) did not request EU action: both have extensive holdings in mainland China and did not want to risk retaliation by the PRC. For details, see Matthew Dalton, "Europe Raises Cry over China's Tech Exports," *Wall Street Journal*, October 6, 2010; John Martens and Jonathan Stearns, "Option Gets $48 Million From China's Huawei, Drops Anti-Dumping Complaint," Bloomberg, October 27, 2010; and Jonathan Stearns and Maryam Nemazee, "China May Face More Subsidy Complaints in Europe, De Gucht Says," Bloomberg, October 4, 2010.

64. Matthew Dalton, "EU's De Gucht: May Push WTO Complaint on China Export Credits," Dow Jones Newswires, April 28, 2011.

65. Quoted in Joshua Chaffin, "Stakes Raised in EU Bid to Curb China Exports," *Financial Times*, May 16, 2011.

66. *Inside US-China Trade,* May 11, 2011; and "China and the US," The Lex Column, *Financial Times,* May 9, 2011.

67. Paul Rasmussen, "China: EU Subsidises Infrastructure Vendors," *Fierce Wireless Europe,* February 23, 2011, www.fiercewireless.com/europe/story/china-eu-subsidises-infrastructure-vendors/2011-02-23 (accessed June 13, 2011).

68. Chaffin, "Stakes Raised"; and Hosuk Lee-Makiyuma, "Chasing Paper Tigers: Need for Caution and Priorities in EU Countervailing Duties (CVDs)," ECIPE Policy Brief no. 01/2011, ECIPE, Brussels, Belgium.

69. Bill Gertz, "Inside the Ring: Huawei Bid Challenged," *Washington Times,* August 18, 2010; David Barboza, "China Telecom Giant, Thwarted by US Deals, Seeks Inquiry to Clear Name," *New York Times*, February 26, 2011; and Hille, Kirchgaessner, and Taylor, "Access Denied." Also see specific letters: Sens. Jon Kyl, Saxby Chambliss, James Inhofe, Richard Burr, Tom Coburn, and Rep. Darrell Issa to President Barack Obama, April 4, 2011; Sens. Jon Kyl and Sherrod Brown to Secretaries Gary Locke and Tom Vilsack, and FCC Chairman Julius Genachowski, June 28, 2011. The administration promised action but hedged on the timing and exact details: see Howard A. Schmidt, special assistant to the president and cyber-security coordinator to Sen. Kyl, May 27, 2011.

70. Brian Grow and Mark Hosenball, "Special Report: In Cyberspy vs. Cyberspy, China Has the Edge," Reuters, April 14, 2011; and John Tkacik Jr., "Trojan Dragon: China's Cyber Threat," *Backgrounder*, no. 2106 (Washington, DC: Heritage Foundation, February 8, 2008), www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat (accessed October 25, 2011).

71. Carl D. Leonnig and Karen Tumulty, "Perry Welcomed Chinese Telecom Firm Despite Security Concern," *Washington Post,* August 15, 2011. A follow-up story in the *Financial Times* (FT) included a favorable quote from Perry regarding Huawei: "This is a company with a really strong worldwide reputation." Huawei, he added, was "all about high standards." The FT reporter speculated that Perry would be vulnerable to criticism from other Republican presidential candidates—particularly Mitt Romney—who had been "highly critical of China's trade policies." See Stephanie Kirchgaessner, "Huawei Finds Rare Ally in White House Hopeful," *Financial Times*, November 2, 2011.

72. There were other failed investment and contract deals: these three incidents have been chosen as illustrative. For more details on other unconsummated Huawei deals, see USCC, "National Security Implications," 19–20; and Rosen and Hanemann, *An American Open Door?*, 64.

73. James K. Jackson, "The Committee on Foreign Investment in the United States," CRS Report RL33388 (Washington, DC: Congressional Research Service, July 29, 2010), www.fas.org/sgp/crs/natsec/RL33388.pdf (accessed June 13, 2011).

74. For more detail on this episode, see Hille, Kirchgaessner, and Taylor, "Access Denied"; USCC, "National Security Implications"; and Bill Gertz, "Inside the Ring: Huawei Bid Challenged," *Washington Times,* August 18, 2010. See the brief, but incisive analysis by Theodore H. Moran in his study, "Three Threats: An Analytic Framework for the CFIUS Process," *Policy Analysis* 89, Peterson Institute for International Economics, August 2009, 25–28. This paper has benefitted greatly from the CFIUS analytic framework Moran established.

75. "Fascinating History behind Huawei's China Threat to 3Com," Twilight in the Valley of the Nerds, April 7, 2010, http://nerdtwilight.wordpress.com/2010/04/07 (accessed October 26, 2011).

76. Grant Gross, "Deal to Buy 3Com Falls Apart," PC World About.Com, March 20, 2008, http://pcworld

.about.net/od/networkin1/Deal-to-buy-3Com-falls-apart.htm (accessed October 27, 2011).

77. Aaron Ricadeia, "HP's 3Com Acqusition Will Challenge Cisco," Bloomberg, November 11, 2010; Hewlett Packard, "HP to Acquire 3Com for $2.7 Billion," news release, November 11, 2009; and Rex Crum, "H-P to Buy 3Com for $2.7 Billion," MarketWatch, November 11, 2009, www.marketwatch.com/story/h-p-to-acquire-3com-for-27-billion-2009-11-11 (accessed October 27, 2011).

78. Jim Duffy, "HP's 3Com Acquisition: An Inside Look," Network World, November 13, 2009, www.networkworld.com/news/2009/111309-hp-3com-haas.html?nwwpkg=hp&ap1=rcb (accessed October 27, 2011); W. David Gardner, "HP Completes $2.7 Billion 3Com Acquisition," *Information Week,* April 12, 2010.

79. Charles A. Hunnicutt, "$2 Million Deal = Big CFIUS Mistake," Troutman Sanders Advisory, March 7, 2011; Bill Newman, "A Lawyer Looks at the Divestment of 3Leaf by Huawei," USA Inbound Acquisitions and Investments Blog, March 3, 2011; Sullivan and Worcester, "3 Lessons from 3Leaf: What to Learn from the Ongoing Match-Up between Huawei and CFIUS," USA Inbound Acquisitions and Investments Blog, February 28, 2011, www.usainbounddeals.com/2011/02/articles/news-commentary/3-lessons-from-3leaf-what-to-learn-from-the-ongoing-matchup-between-huawei-and-cfius (accessed October 26, 2011); Hille, Kirchgaessner, and Taylor, "Access Denied"; and David Barboza, "China Telecom Giant, Thwarted by US Deals, Seeks Inquiry to Clear Name," *New York Times*, February 26, 2011.

80. Bill Newman, "A Lawyer Looks at the Divestment of 3Leaf by Huawei," USA Inbound Acquisitions & Investments, March 3, 2011; Sullivan and Worcester.

81. Pomfret, "History of Telecom Company"; and USCC, "National Security Implications," 20–21. It should be noted that the *Washington Post* reported this incident. No government official denied the story, though US intelligence officials rarely confirm or deny such reports.

82. David Barboza, "China Telecom Giant, Thwarted by US Deals, Seeks Inquiry to Clear Name," *New York Times*, February 26, 2011; Hille, Kirchgaessner, and Taylor, "Access Denied"; and Kevin Brown, "Huawei's Path to Gaining a Foothold in the US," *Financial Times,* April 20, 2011. In an unusual—and generally unkwown—twist to this episode, Huawei's rival, ZTE, also competed strongly for the contract and was certain that it would have won the contest, even over Huawei. Secretary Locke's warning, however, included all Chinese companies, not just Huawei. Confidential source to author.

83. Serena Saitto and Jeffrey McCracken, "Huawei Said to Lose Out on US Assets Despite Higher Offers," Bloomberg, August 3, 2010; USCC, "National Security Implications," 19; and Stephanie Kirchgaessner, "Security Concerns Hold Back Huawei," *Financial Times,* July 8, 2010.

84. Michael Kan, "Huawei Told by US Commerce Department They Are a 'Security Concern,'" ComputerWorldUK, October 14, 2011, www.computerworlduk.com/news/public-sector/3310940/huawei (accessed November 8, 2011); and Michael Kan, "Huawei Complains of Prejudice after Exclusion from US National Wireless Project," ComputerWorldUK, October 14, 2011, www.computerworlduk.com/news/public-sector/3310388/huawei-co (accessed November 8, 2011). Note that the dismissive comment by the Commerce Department official is especially egregious, given that his or her knowledge of the national security implications at issue is likely dim at best. Whether a Chinese or other foreign multinational investor in the United States, a more professional and forthcoming response should be a standing rule.

85. Huawei, "We See beyond Telecom."

86. For profiles, see Pomfret, "History of Telecom Company."

87. Hille, Kirchgaessner, and Taylor, "Access Denied"; Ariel Tung, "Huawei Longs for Breakthrough in US," China Daily, September 9, 2011, http://usa.chinadaily.com.cn/weekly/2011-09/09/content_13655416.htm (accessed October 25, 2011). A second research facility in Bridgewater, NJ, will become the hub for wireless technologies.

88. USCC, "National Security Implications," 20.

89. Admiral Owens's link to Huawei produced substantial criticism in some defense circles. It certainly did not help that he had written an op-ed in the *Financial Times* that had been interpreted as calling for the abandonment of Taiwan to the PRC. In addition, critics charged that Owens was heavily influenced by business interests developed after his retirement from the Navy. As one stated: "it is hard to avoid drawing a linkage between the business interests of his company AEA, investors, and his enthusi-

asm for engaging the PLA." See: Bill Owens, "America Must Start Treating China as a Friend," *Financial Times*, November 17, 2009; and Wendell Minnick, "US Lawmakers Wary of Chinese Telecom Firm," *Defense News*, September 6, 2010.

90. Pomfret, "History of Telecom Company"; Hille, Kirchgaessner, and Taylor, "Access Denied."

91. Mark Palmer and Paul Taylor, "Huawei Hires Former Head of UK IT Projects," *Financial Times*, August 1, 2011.

92. "Security Fact Sheet," Huawei Technologies Co. Ltd.; "Is Huawei Really More of a Security Risk to the UK Critical National Infrastructure Than Other Foreign Telecommunications Equipment Companies Like Cisco or Ericsson?" Spy Blog, March 29, 2009, www.spyBlog.org.UK (accessed October 26, 2011); and Hille, Kirchgaessner, and Taylor, "Access Denied." British Telecom's (BT) linkup with Huawei, as well as plans for a joint security evaluation center, were not without controversy. The British press reported that British intelligence officers—including the head of the Joint Intelligence Council—were not persuaded that allowing BT to purchase Huawei equipment was a wise course of action. See Michael Smith, "Spy Chiefs Fear Secret Cyber Attack," *Sunday Times,* March 29, 2009.

93. Andrew Parker, "Huawei Targets Corporate Sector," FT.com, March 9, 2011, available at www.ft.com/intl/cms/s/2/f78aea42-49b1-11e0-acf0-00144feab49a.html (accessed June 13, 2011).

94. Rosen and Hanemann, *An American Open Door?*

95. Ibid., 61, 69. While it is too early to tell whether it represents a major change, there is recent evidence that CFIUS officials are tightening the process. At a recent industry conference hosted by Reuters, an industry spokesperson claimed that in 2009 and 2010, some 38 percent of CFIUS cases went through a more prolonged, second-stage scrutiny. This was the equivalent of the total number of such second-stage investigations in the previous twenty years. See Tim Helper and Soyoung Kim, "US Scrutinizes Foreign Defense M&A," Reuters, September 9, 2011.

96. Rosen and Hanemann, *An American Open Door?,* 62.

97. Both of these contracts are described in a very recent account of Huawei's struggles in the US market. See Prasso, "What Makes?" Prasso found most companies reluctant to comment on their contracts with Huawei, but CEO Robert Parsloe, of the small network provider Northeast Wireless Networks, openly "raved" about the company's technology to service remote sections of Maine and Oregon. Parsloe claimed that he spent several months in Washington trying to ascertain the validity of security concerns but was unconvinced finally of any serious security threat from the equipment.

98. Stephanie Kirchgasser and Helen Thomas, "US Divided on How to Tackle Huawei," FT.com, July 29, 2010, available at www.ft.com/cms/s/0/0c8a5abe-9b42-11df-baaf-00144feab49a.html#axzz1Q1ulBy7Z (accessed June 22, 2011).

99. These excerpts are taken from a transcript from a conference at the Heritage Foundation: "The China Challenge: Mixing Economics and Security," Heritage Foundation, June 29, 2011. AEI research assistant Robert Foster transcribed the oral remarks.

100. Derek Scissors, "Upgrading Trade Transparency," The Foundry: Conservative Political News, November 8, 2010, http://blog.heritage.org/2010/11/08/time-to-upgrade-transparency-on-trade (accessed June 22, 2011).

101. See, for instance, Jeffrey Carr, "Why Didn't the NSA Stop T-Mobile's Deal with Huawei?" Forbes Blog, The Firewall, October 18, 2010, available at http://blogs.forbes.com/firewall/2010/10/18/why-didnt-the-nsa-stop-t-mobiles-deal-with-huawei (accessed June 22, 2011).

102. Sheridan Prasso, "What Makes?"

103. Hayden's point was reinforced by Greg Garcia, who headed cyber-security efforts under President George H. W. Bush. Both are quoted in Dean Cheng and Derek Scissors, "China and Cybersecurity: Trojan Chips and US–Chinese Relations," Heritage Foundation WebMemo, May 5, 2011, 2, www.heritage.org/research/reports/2011/05/china-and-cyber-security-trojan-chips-and-us-chinese-relations (accessed October 26, 2011).

104. Ibid., 3.

105. Derek Scissors, "Chinese Outward Investment: More Opportunity Than Danger," *Backgrounder*, no. 2579 (Washington, DC: Heritage Foundation, July 13, 2011). Heritage has also suggested that Congress be given a more firm role in the CFIUS process to avoid the random interventions that have increased over the past several years. In assessing this proposal, much will depend on the details of such a role. Formalizing a chance during the process for congressmen (and even other interested parties) to make

their views known might provide a safety valve and further airing of the issues. It would, however, be a mistake to allow Congress a role in the actual decision-making process, as this would inevitably expose CFIUS to much greater interest group pressure.

106. For more details, see *Inside US-China Trade,* June 22, 2011; September 7, 2011; Mayer Brown, JSM: "Legal Update: New Rules Issued Regarding China's Security Review Process for Foreign Investors," Washington, DC, March 31, 2011.

107. Gorman, "U.S. Works."

108. Kevin Brown, "Huawei's Path to Gaining a Foothold in the US," *Financial Times,* April 20, 2011; and "Long March," *Economist*. Criticism of Huawei's lack of transparency and Ren family nepotism has also surfaced in the Chinese press, according to an unclassified CIA report. This brief analysis, published by the CIA Open Source Center on October 5, 2011, also produced a misleading article in the *Washington Times*. The article stated incorrectly that the report "for the first time" linked Huawei to a Chinese intelligence agency and that it received several hundred millions dollars from the Chinese government. The link was in the person of Huawei board member, Sun Yafang, who had at one time worked for the Chinese Ministry of State Security. However, according to the Open Source Center report, Ms. Sun's connection to the State Security ministry occurred two decades ago, before she went to work for Huawei (either in 1989 or 1992). There is no assertion in the report that she maintains a formal connection with the ministry. The report does assert, again using Chinese press sources, that Ms. Sun used her influence with the Security Ministry to help Huawei through financial difficulties "at critical times" when it was founded in 1987. And it does note that failure to disclose her past security association "has reinforced suspicions over potential close links between Huawei and the Chinese government." This last sentence is the only uncharacteristic stretch in the otherwise circumspect report. It should be noted that it is odd at this point to focus on Ms. Sun, as it has been public knowledge since Huawei was founded that Mr. Ren had previously been an officer of the PLA. Further, Ms. Sun's security background had been reported months ago. Finally, regarding government support that allegedly "contradicts" Huawei's claim that it receives little or no government subsidies, the Open Source Center and the *Times* article both cite R&D funds that Huawei has publicly acknowledged and which this study has analyzed in the preceding text. In general, the Open Source Center report is even-handed; the *Times* rendition, however, is tendentious and selective in its use of evidence. See "Annual Report Details Directors, Supervisory Board for First Time," Open Source Center, US Central Intelligence Agency, October 5, 2011; Bill Gertz, "Chinese Telecom Firm Tied to Spy Ministry," *Washington Times*, October 11, 2011; and Kathrin Hille, "Huawei Ends Its Board Secrecy," *Financial Times,* April 18, 2011.

109. "Long March," *Economist*.

110. Prasso, "What Makes?"

111. Should the company decide to undertake a public offering in the US market, it must avoid an attempt to exploit a loophole that some Chinese companies, abetted by US law firms and stock promoters, have used with disastrous consequences for both US and Chinese investors. That is, it should eschew the still-legal process known as a reverse takeover, by which a foreign company is allowed to merge with an existing US publicly traded shell company, and thereby to raise money by selling shares to US investors. This maneuver has permitted the resulting merged entity to evade the stricter regulatory scrutiny and accounting standards required of US domestic companies. Over the past year, a huge scandal from questionable and fraudulent accounting and governance practices relating to reverse mergers has unfolded in the United States. It is estimated that in the three years from 2007 to 2010, more than one-quarter of some 600 reverse takeovers involved Chinese companies. The questionable practices have resulted in dozens of suspensions and delistings from all three major US stock exchanges. For details on reverse takeovers, Chinese companies, and the wave of recent scandals, see Jamil Anderlini, "Problem Flagged Up," *Financial Times*, July 5, 2011; and Dana Aubin and Andrea Shalal-Esa, "Where Was SEC as Trouble Festered at Chinese Companies?" Reuters, July 10, 2011. For the related negative consequences for Chinese investors, see "Chinese Protest $5 Billion Loss Tied to US Stock Market Reverse Mergers," Bloomberg, August 18, 2011.

112. Scott Kennedy, "Who Is Huawei?" The China Track, October 8, 2010, http://chinatrack.typepad.com/blog

/2010/10/who-is-huawei.html (accessed June 22, 2011).

113. "Long March," *Economist*.

114. As quoted in Prasso, "What Makes?" Just as this study was completed, the *Economist* again weighed in on the opacity of Chinese capitalism in the areas of government–private sector relations. See "Privatization in China: Capitalism Confined," *Economist*, September 2, 2011. It posited the emergence of four categories of companies: large state-controlled companies, joint ventures, private companies with some state influence, and companies backed by publicly owned investment funds. Huawei was identified as belonging to the third category (as was ZTE). They are "largely in private hands [and contain] the most successful privatized companies." While praising the record of these companies, the subtitle of the article states, "Chinese companies, like companies everywhere, do best when they are privately run. In China, however, the state is never far away." Even at this late date, there are doubts about the real independence of Huawei and other allegedly private companies. This is another reason the company would be best advised to go public and list on a US stock exchange.

115. Export-Import Bank of the United States, *2010 Competitive Report* (Washington, DC: Author, 2010), 113.

116. Ibid.; and Fred Hochberg, "How the US Can Lead the World in Exports: Retooling Our Export Finance Strategy for the 21st Century," Presentation at the Center for American Progress, Washington, DC, June 15, 2011.

117. Letter from Sen. Kyl et al., August 9, 2011; Lake, "Computer Lab's."

118. Olsen, "Huawei's Open Letter"; Plummer to Chu, August 16, 2011.

119. Quoted in "Huawei's $30 Billion China Credit Opens Doors in Brazil, Mexico," Bloomberg, April 24, 2011. The Bloomberg piece also quotes executives from both Brazilian and Mexican telecom operators stating that aggressive financing terms were decisive in decisions to buy network equipment from Huawei (and ZTE). The article also states that ZTE has access to a $15 billion credit line for its customers.

120. Even free market think tanks—such as Brussels-based ECIPE—that have been extremely critical of EU trade remedy policies, have endorsed action against companies that benefit from credit policies that are fundamental to allowing "cut-throat pricing on high value-added goods." See Hosuk Lee Makiyama, "Chasing Paper Tigers: Need for Caution and Priorities in EU Countervailing Duties (CVDs)," (Policy Brief No. 01.2011, ECIPE, Brussels, Belgium, January 2011).

121. For more details on the OECD credit rules, see Hufbauer, Fickling, and Wong, "Revitalizing the Export-Import Bank."

122. USCC, "National Security Implications," 39–61.

123. Ibid., 46–48. See also Larry Walsh, "Huawei Symantec: A Potentially Disruptive Force," Channel Nomics, February 28, 2011, available at http://channelnomics.com/2011/02/28/huawei-symantec-potentially-disruptive-force (accessed June 15, 2011).

124. For analysis of the BT-Huawei alliance, including the security fears, see Jeffrey Carr, "Huawei: Cybersecurity Threat or Cybersecurity Provider?" Forbes's The Firewall, December 6, 2009, http://blogs.forbes.com/firewall/2010/12/06/huawei-cybersecurity-threat-or-cybersecurity-provider (accessed June 15, 2011); Kim Howells, "Huawei's BT Deal Raises Cyber Spying Fears," Times of India online, March 14, 2011, http://articles.timesofindia.indiatimes.com/2011-03-14/internet/28687420_1_telecoms-security-fears-chinese-technicians (accessed June 15, 2011); Simon Parry and Robert Verkaik, "New Cyber Attack Fears over the Chinese 'Red Army Lab' Being Used for FT Broadband Tests," Daily Mail Online, March 13, 2011, www.dailymail.co.uk/news/article-1365739/New-cyber-attack-fears-Chinese-Red-Army-lab-used-BT-broadband-tests.html (accessed June 15, 2011); and Wtwu, "Is Huawei Really More of a Security Risk to the UK Critical National Infrastructure Than Other Foreign Telecommunications Equipment Companies Like Cisco or Ericsson?" Spy Blog, March 29, 2009, http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/03/29/is-huawei-really-more-of-a-security-risk-to-the-uk-critical-national-infrastructure.html (accessed June 15, 2011).

125. Parry and Verkaik, "New Cyber Attack Fears."

126. USCC, "National Security Implications," 47.

127. Ibid., 49–53. One security analyst has raised questions about the deal between Huawei and T-Mobile. Jeffrey Carr stated in a blog, "I'm surprised that neither the NSA nor anyone from Congress has stopped this deal from happening. . . . If there is sufficient cause to deem Huawei technology a high security risk if employed on US systems (and I believe that there is) and since the NSA has quashed other

pending Huawei deals with comparable US companies, how is it that Huawei succeeded with T-Mobile?" See Carr, "Why Didn't the NSA?"

128. USCC, "National Security Implications," 49–50.
129. Ibid., 53.

About the Author

Claude Barfield is a resident scholar at the American Enterprise Institute. His areas of study include international trade, science and technology policy, and intellectual property. He has taught at Yale University, the University of Munich, and Wabash College. He served in the Ford administration, on the staff of the Senate Government Affairs Committee, and was costaff director of President Carter's Commission for a National Agenda for the Eighties. He received a BA from Johns Hopkins University and a PhD from Northwestern University.