Peterson Institute for International Economics

Policy Brief

NUMBER PB13-11

MAY 2013

Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers

Theodore H. Moran

Theodore H. Moran, *nonresident senior fellow, has been associated with the Peterson Institute for International Economics since 1998. He holds the Marcus Wallenberg Chair at the School of Foreign Service in Georgetown University. Since 2007 he has served as associate to the US National Intelligence Council on international business issues. Moran also currently serves as a paid member of the International Advisory Council of the Chinese electronics multinational Huawei. This* Policy Brief *draws on his forthcoming Institute book with Lindsay Oldenski,* Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China.

When Eric Xu, executive vice president of the Chinese telecommunications giant Huawei Technologies Ltd., recently declared that his company is "not interested in the US market anymore," the comment was widely construed as exasperation over repeated allegations that Huawei constitutes a national security threat to the United States. The *Economist* characterized his statement as the equivalent of "You can't fire me, I quit!" noting that the House Intelligence Committee had been warning against the use of Huawei-made equipment in US telecommunications and information networks.[1]

Huawei officials quickly affirmed that the company would continue to do business in the United States but indicated that the experience of repeatedly being singled out as a threat to US national security due to its Chinese origins would lead the firm to devote its largest commercial efforts elsewhere.

Weaknesses and vulnerabilities in US information technology (IT) systems have become an increasingly high-level US government concern in Washington. This concern is all the more pressing because, according to investigation conducted by the information security company Mandiant Corporation (2013), the large increases in cyberattacks against the United States in recent years appear to have emanated from China, likely originating in facilities controlled by the People's Liberation Army (PLA).

The question is not whether the concerns about Chinese cyber threats to US national security are legitimate but whether singling out particular companies by nationality of their headquarters resolves the vulnerability of US IT networks. In this *Policy Brief* I argue that targeting one or two companies on the basis of their national origins does nothing for US security in a world of global supply chains for all IT providers. Indeed such a strategy could lull legitimate watchdogs into a false sense of complacency. Meanwhile, the current approach locks the United States into a policy of discrimination and distortion that discourages valuable inward investment from overseas, while providing a precedent for highly damaging copycat practices in other countries. Indeed, we should not be surprised if China now emulates this approach in a "digital tit for tat" sequence of policy moves.

To counter cybersecurity threats, a multilateral nondiscriminatory procedure is needed for vetting IT goods and services—and patches and upgrades—from supply chains that originate anywhere in the world. I outline what such a multilateral system to validate the integrity of IT inputs might look like.

BACKGROUND OF ALLEGATIONS AGAINST HUAWEI

Huawei has grown rapidly in recent years to become the second largest supplier of IT equipment by revenue in the world, behind Ericsson, which is based in Sweden. The Shenzhen-based company has been particularly successful in Europe,

1. "You Can't Fire Me, I Quit," *Economist*, April 24, 2013, www.economist.com/blogs/schumpeter/2013/04/telecoms (accessed on May 1, 2013).

India, Japan, and emerging markets generally. Huawei's early growth was largely outside China, as Chinese authorities discriminated against the private employee–owned firm in favor of state-owned IT companies. Now Huawei's position in Chinese markets is expanding rapidly as well.

Targeting one or two companies on the basis of their national origins does nothing for US security in a world of global supply chains for all IT providers.

In the United States (and Australia), Huawei's growth has been hampered by repeated allegations that the company might pose a national security threat to US users, particularly if it sells products to major network providers like Verizon and AT&T. The suspicions originated in the reputation of its founder, Ren Zhengfei, who started his career as an engineer in the IT brigade of the PLA. The concern about possible ties between Huawei and the PLA—or other parts of the Chinese government—has led to formal investigations of proposed acquisitions by the Committee on Foreign Investment in the United States (CFIUS), the interagency panel established to investigate possible security dangers posed by foreign takeovers of US companies.

CFIUS procedures have grown increasingly careful, professional, and painstakingly empirical over the years, but they are limited to investigating foreign takeovers of US companies, not procurement of goods and services from foreign companies. Accordingly, many US actions toward Huawei have occurred outside the guidance of formal procedures or laws, motivated by suspicions but without rigorous judicial or government investigative mechanisms. These actions have taken the form of ad hoc interventions by senior US government officials with potential buyers of the Chinese company's equipment. In 2009, for example, Huawei was a leading bidder on an AT&T plan to upgrade the US network to operate with 4G (fourth generation) technology, only to find that the head of the National Security Agency (NSA) told AT&T that Huawei must be excluded from consideration if AT&T wanted to maintain its contracts with the US government. The next year, as Huawei appeared set to win major network upgrade business from Sprint Nextel, the Secretary of Commerce called Sprint's CEO to warn that Sprint's relationship with US government agencies would be imperiled if Huawei were the chosen provider. These interventions are not covered under the legislation that governs CFIUS investigations of potential acquisitions of US companies by foreigners.

In March 2013, Sprint and Softbank at their own initiative traveled to Capitol Hill to make public assurances to Representative Mike Rogers (R-MI), chairman of the House Intelligence Committee, that no Huawei equipment would be used in a merged Sprint-Softbank IT system.[2] During the previous two years, Rogers had repeatedly warned against potential national security threats in US telecommunications networks. In a joint statement, Rogers and Representative Charles A. (Dutch) Ruppersberger of Maryland, ranking Democrat on the intelligence panel, said: "The threat posed to US national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority, given the country's reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers."[3] To address these vulnerabilities, the House Intelligence Committee began an investigation of Huawei and another Chinese IT supplier, ZTE Corporation, in 2011.

COMMITTEE'S INTELLIGENCE REPORT ON HUAWEI AND ZTE

In the spring of 2012, committee staff met with and interviewed senior corporate executives of Huawei at corporate headquarters in Shenzhen, China. In May, Ruppersberger and Representatives Devin Nunes (R-CA), Michele Bachmann (R-MN), and Adam Schiff (D-CA) met with senior executives, including Ren, the Huawei founder, in Hong Kong. On September 13, the committee held an open hearing, which included Charles Ding, corporate senior vice president and Huawei's representative to the United States.

Despite these meetings and concurrent exchanges of documents and written materials, "neither company," the report stated, "was willing to provide sufficient evidence to ameliorate the Committee's concerns." As a result, the report recommended that "US government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts." Further, it said: "Similarly, government

2. "Chairman Rogers Statement on Proposed SoftBank/Sprint Deal: SoftBank/Sprint Plans Will Not Integrate Huawei Equipment," press release, March 28, 2013, http://intelligence.house.gov/press-release/chairman-rogers-statement-proposed-softbanksprint-deal (accessed on May 1, 2013).

3. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, report by Chairman Mike Rogers and Ranking Member C. A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, October 8, 2012, US House of Representatives, 112th Congress, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf (accessed on May 1, 2013).

contractors—particularly those working on contracts for sensitive US programs—should exclude ZTE or Huawei equipment in their systems." Finally, it concluded, "US network providers and systems developers are strongly encouraged to seek other vendors for their projects."[4]

Huawei responded by asserting that the company had indeed provided voluminous information to the committee and that the committee had held Huawei "guilty until proven innocent" without supplying any evidence of cybersecurity threatening behavior. (The committee's report had referred to a confidential annex but did not indicate what kind of proof might be found there.) Huawei's claim that the evidence was lacking was supported by the *Economist*, which said the report "appears to have been written for vegetarians. At least, there is not much meat in it."[5] Much of the material backing the report has not been made public. In *Heat Without Light*, Claude Barfield of the American Enterprise Institute, declared in November 2012 that the House Intelligence Committee and the Obama administration "owe it to the American people" to make public the results of their investigations (Barfield 2012).

Apart from the questions about the thoroughness, fairness, appropriateness, or even legality of the House report recommendations, does discriminating against specific IT suppliers on the basis of suspicions related to their nationality and the personal history of one of their officers constitute an effective approach for dealing with cybersecurity problems?

TOWARD A MULTILATERAL NONDISCRIMINATORY APPROACH TO CYBERSECURITY THREATS

The serious attention being paid by the Obama administration to the very real dangers of cybersecurity is welcome at a time when the threats seem greater than ever before. The role of the Chinese government and military in hacking into US systems has been pinpointed by many authorities, particularly the Mandiant investigation. Mandiant's wording was careful, however. It said that the latest threats were "likely government-sponsored" and that PLA was a logical suspect because its "mission, capabilities, and resources" were "similar" to the threat it had identified (Mandiant Corporation 2013). (In response, the Chinese Defense Ministry said in February 2013: "It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence.")[6] What might be a genuinely effective approach to combating such dangers?

What one sees driving through Shenzhen on the way to Huawei headquarters is instructive. Along the highway are facilities and research campuses of Ericsson, Lucent-Alcatel, Samsung, Cisco, Siemens-Nokia, Motorola, Infosys, and NTT Docomo—in short, facilities operated by all the major IT rivals and competitors of Huawei. Most of these companies outsource the manufacture of components, in turn, to India, Israel, and Russia, as well as Taiwan, Malaysia, Thailand, and Mexico. In an era of global IT supply chains, the potential for inserting trapdoors, backdoors, and surveillance mechanisms in hardware or software is ubiquitous.

How might it be possible to deal realistically with ensuring supply chain integrity?

Huawei itself provides a possible answer. Its own security assurance program offers to place all source code in escrow to a trusted third party that can verify that goods and services are "clean" to buyers or governments. The most advanced instance of such vetting is Huawei's Cyber Security Evaluation Center at Banbury in the United Kingdom, which is staffed by Huawei employees who are UK nationals with UK government security clearances. The center makes a forensic audit of Huawei hardware and software according to UK government specifications and provides it to UK intelligence and other agencies, which are expected to share information with counterparts in the United States and elsewhere. Hardware and software—including patches and upgrades—must pass inspection and receive an embedded time/date stamp that a subsequent user can verify to ensure that no changes have been made to the code after leaving Banbury.

Complementing this audit of hardware and software is the option that indigenous trusted third-party installers—such as Bechtel, CDTI, or TESSCO—can take delivery of goods and services that have been verified as secure and deliver, install, maintain, and manage upgrades/updates for purchasers. If the buyer wishes, therefore, no Huawei individual or entity will touch Huawei goods or services between security audit and installation (or upgrade) with the final user.

Perhaps the vetting process can be improved, and the vetting standards devised by technical professionals should be reviewed by a panel of experts rather than lay persons like myself. But, the logical extension of this method for ensuring supply chain integrity is clear. We may need an array of independent cybersecurity assessment cells around the globe that vet the hardware and software of all major IT providers without discrimination, providing results to private clients and govern-

4. Ibid.

5. "Put on Hold: Two big Chinese telecoms firms come under fire in America," *Economist*, October 13, 2012, www.economist.com/node/21564585 (accessed on May 1, 2013).

6. Statement published on the Chinese Defense Ministry's website, http://eng.mod.gov.cn, February 20, 2013.

ments alike. It is in the interest of IT buyers and suppliers everywhere to devise a system of safeguards and inspections that prevents compromise of globalized supply chains without disrupting the vital flow of technology.

IMPLICATIONS FOR BROADER ECONOMIC CONCERNS IN THE UNITED STATES AND ABROAD

The CFIUS investigations of national security implications of potential acquisitions are founded in law and are careful, limited, and evidence-based (even if evidence that might reveal intelligence sources and methods cannot be shared with either the acquiring company or the target of the acquisition). These methods often frustrate suppliers and investors, but they are effective in protecting national security. US multinationals can live in a mirror-image world where other governments behave in similar fashion when it comes to foreign acquisitions in their economies.

By contrast, US treatment of Huawei has been arbitrary, lacking in governing rules and standards, in a way that sends a bad signal to international investors about how they might be treated around the world. Imagine a world in which random politicians in Europe, Japan, South Korea, Russia, or elsewhere started dictating which international vendors were allowed—or forbidden!—to sell goods and services to government ministries, government contractors, and private parties within their economies. Similarly, it should not be acceptable for ministers of commerce or directors of intelligence around the world to block business transactions on the basis of unexplained suspicions and undocumented allegations.

Owing to such US behavior, Chinese companies are reluctant to even consider venturing into the United States. Daniel H. Rosen and Thilo Hanemann report that Chinese investors now fear the frustrations and difficulties of being singled out if they take steps to invest in the United States and consequently hold back.[7] Lindsay Oldenski and I estimate—using an innovative new gravity model for benchmarking expected foreign direct investment (FDI) levels—that Chinese investment in the United States is far lower (approximately 50 percent lower) than what other economic parameters would predict (Moran and Oldenski 2013).

Oldenski and I find that inward investment—including by Chinese companies (such as it is)—provides better-than-average jobs for Americans, while building more productive plants and engaging in more research and development (R&D) locally, than typical US companies. Foreign investors in the United States produce many positive side-effects, including competitive pressures and technology spillovers, that make local American firms more competitive. Indeed, about 12 percent of total productivity growth among firms in the United States from 1987 to 2007 can be attributed to productivity spillovers from inward FDI.

Nowhere is this more needed than in the US IT sector. A 3G (third generation) wireless network contract in the United States costs approximately $155 per month; in Europe, an identical contract costs $51 to $59 per month. To download a gigabyte of data over a 4G LTE (fourth generation, long-term evolution) wireless network for mobile phones and terminals in Europe costs about $2.50 per gig; in the United States, the same service costs $7.50 per gig. These IT price differentials drag down the competitiveness of US businesses, not to mention place a burden on US consumers. The IT sector in the United States badly needs more competition—including more competition from foreign firms—not less.

CONCLUSION

Singling out foreign producers of IT goods and services on the basis of their nationality, rather than hard evidence, and forbidding them from doing business or acquiring companies in the domestic market is ineffective, discriminatory, and unfair. The dangers and risks of compromise of national security are real. But in a world where supply chains of IT companies of every nationality are thoroughly globalized, a multilateral nondiscriminatory system is needed to ensure the integrity of equipment, software, patches, and upgrades from all sources. Much remains to be done to establish an appropriate regime to protect national security and also the rights of investors and companies doing business with foreign firms. But efforts to set up such a regime must begin now.

REFERENCES

Barfield, Claude. 2012. *Heat Without Light* (November 27). Washington: American Enterprise Institute.

Mandiant Corporation. 2013. *APT1: Exposing One of China's Cyber Espionage Units* (February 19). Mandiant Intelligence Center. Alexandria, VA. Available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed on May 1, 2013).

Moran, Theodore H., and Lindsay Oldenski. 2013 (forthcoming). *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China*. Policy Analyses in International Economics 100. Washington: Peterson Institute for International Economics.

7. Personal communication, April 26, 2013.