Gambling with Source Code

By: Nir Kshetri

Kshetri, Nir (2016). "Gambling with Source Code ", IEEE *Computer*, 49(2), 74-77.

Made available courtesy of IEEE: http://dx.doi.org/10.1109/MC.2016.45

Abstract:

Tech companies required to comply with controversial regulations in foreign countries as a cost of doing business there must trade off the potential economic benefits with the risk of long-term harm.

Keywords: China | IBM | ICT | source code

Article:

In October 2015, IBM agreed to let officials from China's Ministry of Industry and Information Technology (MIIT) examine the source code of some of the company's products, which are widely used by Chinese firms in the financial, Internet, and energy sectors—supposedly to ensure that it had no "security flaws." IBM justified its controversial decision to comply with the demand, which took the industry as well as the Obama administration by surprise, on the need to expand market share in China and cited earlier agreements by Microsoft to allow the Chinese as well as Russian and UK governments to access Windows source code.(1,2)

However, critics argue that IBM is putting its intellectual property (IP) at risk, and that its action could encourage other US tech companies seeking a competitive advantage overseas to likewise reveal their "secret sauce" to foreign governments.(3) While providing short-term economic benefits, this could ultimately damage companies' long-term prospects as well as compromise both their own and national cybersecurity infrastructure.

CHINA'S MOTIVATION: SUSPICION AND DISTRUST

The ostensible purpose of China's recent demand that US tech companies operating in their country submit source code to officials for review is to check for hidden backdoors enabling

"third parties" to monitor Chinese computer users.(1) Due to deep-rooted suspicions among Chinese policymakers about spying by Western governments and corporations, computer hardware and software imported from the US and its allies are subject to detailed inspection. Analysts argue that China's broader goal is to create a domestic information and communications technology (ICT) industry that will minimize reliance on foreign ICT and its associated security dangers.(3)

As far back as 2000, newspaper reports highlighted China's long-standing distrust of Western ICT and its impact on national security.(4) For example, an 8 February editorial in the People's Liberation Army Daily noted that "some countries" with highly developed ICT industries are "taking advantage of their monopolistic position" to "control information technologies, infiltrate information resources," and dump ICT products in underdeveloped countries "to attain political, economic and military objectives." In the China Economic Times of 12 June, Xu Guanhua, then Chinese vice minister of science and technology, argued that a key aspect of developed countries' military strategy was exploiting exported software for "coercing, attacking or sabotage."

Revelations in 2013 by Edward Snowden, a former CIA employee and NSA contractor, of mass US government surveillance heightened Chinese fears. Commenting on US intelligence agencies' alleged hacking of China's major mobile companies and universities, an editorial by the Xinhua News Agency noted: "These, along with previous allegations, are clearly troubling signs. They demonstrate that the United States, which has long been trying to play innocent as a victim of cyber-attacks, has turned out to be the biggest villain in our age."(5)

Following the US government's indictment of five high-ranking Chinese army officials in May 2014 for alleged cybercrimes against US companies, China announced that it would perform rigorous national security inspections of imported tech products. Nationalist bloggers described the inspections as a "hard blow to anti-China forces" and suggested that US companies such as Cisco, IBM, and Microsoft would be negatively affected.(6)

A NEW REGULATORY ENVIRONMENT IN CHINA

The first sign of trouble came in January 2015, when China required foreign companies selling ICT to its banks to turn over source code, submit to government audits at any time, and build back doors into their products that the Chinese government could access. US and other Western firms, with their governments' backing, strongly objected to the new policies and complained that they amounted to protectionism.(7)

China suspended the requirements in April 2015, but some analysts correctly predicted that China would try to achieve the same end in a different way.(3) In July 2015, China's parliament, the National People's Congress, drafted a new law calling on the Chinese government to define national and industrial cybersecurity standards that all technology vendors must comply with. Critics suspect that such standards could exclude foreign vendors or require them to provide the Chinese government or domestic firms with access to their IP.(8)

China’s real, unstated goal appears to be to remove most foreign technologies from its banks, military systems, state-owned enterprises, and key government agencies in the near future. For example, the China Banking Regulatory Commission requires banks and financial companies to have at least 75 percent of their computer systems using “safe” technology by 2019 and to spend at least 5 percent of their ICT budgets for this purpose.(9)

THE CARROT AND THE STICK

Foreign businesses operating in China deemed friendly to the government have easier access to China’s enormous but tightly regulated market. However, noncompliance with government regulations and/or harsh criticism of the regime can lead to severe restrictions and even exclusion from that market. For instance, foreign media outlets, blogs, and social media sites that try to flout China’s strict Internet censorship and surveillance laws are often blocked.(10)

China is actively striving to reduce its dependence on traditional manufacturing and diversify its economy. In 2015, President Xi Jinping laid out plans to accelerate development of a native ICT industry.(11) To nurture this industry’s growth, the government relies on a system of subtle rewards and punishments to acquire needed technologies from foreign firms.

In March 2015, IBM chairman, president, and CEO Virginia M. Rometty noted that foreign companies operating in China, especially in the ICT sector, needed to cooperate with government officials in order to partner with Chinese firms and develop products for both local markets and the international market.(3) Analysts observed that IBM’s agreement to let MIIT regulators review their source code coincided with the company’s announcement of a deal with Chinese datacenter service provider 21Vianet Group to launch the Bluemix cloud computing platform in China.(12) IBM has invested $1 billion in Bluemix, which supports more than 120 tools and services.(13)

THE RISKS OF COMPLIANCE

What risks is IBM taking by revealing its products’ source code to Chinese officials? Is it possible for them to copy or steal it and pass it on to Chinese companies developing competing products? If so, how much will this impact IBM?

IBM’s source code demos reportedly will last only a few hours and be performed in a room without an Internet connection.(14) These restrictions make it extremely difficult for government officials involved in the demo to steal the code.

It’s also important to point out that software development is highly skill intensive and requires more tacit than explicit knowledge, generally making it more difficult to imitate and reproduce software than hardware. In addition, unlike hardware, software is evolutionary in nature, requiring continual updates and modifications. Even if you could acquire a product line’s source code, the code is likely to change so quickly as to become obsolete by the time you’re in a position to launch a clone product. This characteristic is akin to the high velocity of big data—most data has a short shelf-life, with its value declining exponentially over time.

Moreover, a key strength of tech giants like IBM is the ability to provide integrated solutions for customers.(15) IBM isn't a specialized manufacturer, so even if Chinese companies are able to develop some products or services using stolen code they're unlikely to significantly threaten IBM's overall business operations.

The risks of compliance, then, are real but can be overstated.

IBM'S DILEMMA

US government officials and companies are equally distrustful of their Chinese counterparts. In a 2011 Wall Street Journal editorial, former White House national security official Richard Clark asserted that "Beijing is successfully stealing research and development, software source code, manufacturing know-how and government plans."(16) Critics claim that the Chinese government routinely sponsors or sanctions cyberattacks on Western government agencies and companies and shares the knowledge obtained from these attacks with Chinese enterprises.(17)

Beyond general national security concerns, US tech companies worry that complying with China's regulations could open the door to theft of their IP and weaken their cybersecurity infrastructure. They also worry about their public image: because of China's strict censorship laws and its reputation for punishing outspoken dissidents, businesses that cave to Chinese government demands—particularly those that impact the Internet and social media— are often criticized for putting profit before democratic principles.

The other so-called BRIC countries—Brazil, Russia, and India—might follow China's lead and demand that IBM and other US tech companies reveal their products' source code to continue doing business there. Their motive might simply be to ensure that the products are indeed secure given the number of highly publicized cyberattacks on US assets. But given China's stated desire to create a home-grown IT industry and the long history of mutual suspicion between the US and China, including tit-for-tat cyberwarfare allegations, US companies might want to think twice about handing over source code to Chinese regulators—or at least proceed very cautiously.

To understand why IBM would risk doing so, even under highly controlled conditions, it's important to appreciate the dilemma the company faces. In June 2015, IBM reported that overall revenue from its products had declined consecutively for 13 quarters; the falloff was particularly acute in China, where revenue had declined by 40 percent during the previous nine months.(18) The Asia-Pacific region, excluding Japan, accounted for 14 percent of the company's 2013 revenue of $99.8 billion, and China accounts for a significant part of this revenue.(19)

IBM is thus actively pursuing expansion opportunities in the Chinese market. While announcing the source code demos, IBM senior vice president Steve Mills acknowledged that the company needs the Chinese government's support to grow its business in the country.(14) By revealing its products' source code, IBM might be hoping to convince officials that it has nothing to hide. The unanswered question is: what will China do with the information?

As US tech companies increasingly rely on revenue from overseas markets—particularly newly advanced economies like the BRIC countries—they could be required to comply with

objectionable government regulations as a cost of doing business. In IBM's case, gambling with its source code might be worth it; time will tell. However, each company faces a unique situation and must perform its own cost−benefit calculus, trading off the potential economic benefits with the risk of long-term harm—to itself, the entire industry, and even the nation.

ACKNOWLEDGMENT

I thank Jeff Voas for numerous edits and suggestions on previous versions of this article.

REFERENCES

1. E. Dou, "IBM Allows Chinese Government to Review Source Code," *The Wall Street J.*, 16 Oct. 2015; www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

2. J. Menn, "Why IBM Lets Certain Countries, Including China, Review Its Source Code," *VentureBeat*, 18 Oct. 2015; http://venturebeat.com/2015/10/18/why-ibm-lets-certain-countries-including-china-review-its-source-code.

3. P. Mozur, "IBM Venture with China Stirs Concerns," *The New York Times*, 19 Apr. 2015; www.nytimes.com/2015/04/20/business/ibm-project-in-china-raises-us-concerns.html.

4. N. Kshetri, "Cybersecurity and International Relations: The U.S. Engagement with China and Russia," *Proc. FLACO-ISA Joint Conf.* (FLACSO-ISA 14), 2014; http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf.

5. M. Jinwei, "Commentary: Washington Owes World Explanations over Troubling Spying Accusations," *Xinhua*, 23 June 2013; 2013. http://news.xinhuanet.com/english/indepth/2013-06/23/c_132478464.htm.

6. O. Lam, "China to Perform Security Inspections for Tech Products," *Global Voices Advocacy*, 28 May 2014; http://advocacy.globalvoicesonline.org/2014/05/28/china-to-perform-security-inspections-for-tech-products.

7. P Mozur, "New Rules in China Upset Western Tech Companies," *The New York Times*, 28 Jan. 2015; http://mobile.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.

8. G. Wong, "China to Get Tough on Cybersecurity," *The Wall Street J.*, 9 July 2015; www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416.

9. S. Yang, "China Said to Plan Sweeping Shift from Foreign Technology to Own," *Livemint*, 18 Dec. 2014; www.livemint.com/Industry/HET9rKbJ7U3Ui4RzqXkfkO/China-said-to-plan-sweeping-shift-from-foreign-technology-to.html.

10. S. Cook, “How Chinese Censorship Is Reaching Overseas,” blog, 28 Oct. 2013; http://globalpublicsquare.blogs.cnn.com/2013/10/28/how-chinese-censorship-is-reaching-overseas/comment-page-2.

11. J. Cao, “IBM Gives the Chinese Government Access to Software Code,” *Bloomberg Business*, 16 Oct. 2015; http://www.bloomberg.com/news/articles/2015-10-16/ibm-gives-limited-access-of-software-code-to-chinese-government.

12. S. Fadilpašić, “IBM Lets China Review Its Source-Code,” *ITProPortal*, 19 Oct. 2015; www.itproportal.com/2015/10/19/ibm-lets-china-review-its-source-code.

13. “IBM Advances Hybrid Capabilities to China, Unveils Bluemix Local,” *The FINANCIAL*, 2 Dec. 2015; http://finchannel.com/index.php/technology/item/52442-ibm-advances-hybrid-capabilities-to-china-unveils-bluemix-local.

14. N. Arce, “IBM Raises Eyebrows, Opens Source Code Access to China: Here’s Why,” *Tech Times*, 18 Oct. 2015; www.techtimes.com/articles/96776/20151018/ibm-raises-eyebrows-opens-source-code-access-to-china-here-s-why.htm.

15. S. Denning, “Why Did IBM Survive?,” *Forbes*, 10 July 2011; www.forbes.com/sites/stevedenning/2011/07/10/why-did-ibm-survive.

16. R. Clarke, “China’s Cyberassault on America,” *The Wall Street J*., 15 June 2011; www.wsj.com/articles/SB10001424052702304259304576373391101828876.

17. A. Tonelson, “Chinese Hacking Is Made in the U.S.A.,” *Bloomberg View*, 28 Mar. 2013; www.bloombergview.com/articles/2013-03-28/chinese-hacking-is-made-in-the-u-s-a-.

18. A. Barinka, “IBM Drops after Revenue Declines for 13th Straight Quarter,” *Bloomberg Business*, 20 July 2015; www.bloomberg.com/news/articles/2015-07-20/ibm-profit-tops-analysts-estimates-as-it-pares-operating-costs.

19. “China Said to Study IBM Servers for Bank Security Risks,” *Bloomberg Business*, 7 May 2014; www.bloomberg.com/news/articles/2014-05-27/china-said-to-push-banks-to-remove-ibm-servers-in-spy-dispute.

NIR KSHETRI is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.