THE WALL STREET JOURNAL.

FRIDAY, JANUARY 27, 2012

China's Cyber Thievery Is National Policy—And Must Be Challenged

By Mike McConnell, Michael Chertoff and William Lynn

Only three months ago, we would have violated U.S. secrecy laws by sharing what we write here—even though, as a former director of national intelligence, secretary of homeland security, and deputy secretary of defense, we have long known it to be true. The Chinese government has a national policy of economic espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today.

Evidence of China's economically devastating theft of proprietary technologies and other intellectual property from U.S. companies is growing. Only in October 2011 were details declassified in a report to Congress by the Office of the National Counterintelligence Executive. Each of us has been speaking publicly for years about the ability of cyber terrorists to cripple our critical infrastructure, including financial networks and the power grid. Now this report finally reveals what we couldn't say before: The threat of economic cyber espionage looms even more ominously.

The report is a summation of the catastrophic impact cyber espionage could have on the U.S. economy and global competitiveness over the next decade. Evidence indicates that China intends to help build its economy by intellectual-property theft rather than by innovation and investment in research and development (two strong suits of the U.S. economy). The nature of the Chinese economy offers a powerful motive to do so.

According to 2009 estimates by the United Nations, China has a population of 1.3 billion, with 468 million (about 36% of the population) living on less than $2 a day. While Chinese poverty has declined dramatically in the last 30 years, income inequality has increased, with much greater benefits going to the relatively small portion of educated people in urban areas, where about 25% of the population lives.

The bottom line is this: China has a massive, inexpensive work force ravenous for economic growth. It is much more efficient for the Chinese to steal innovations and intellectual property—the source code of advanced economies—than to incur the cost and time of creating their own. They turn those stolen ideas directly into production, creating products faster and cheaper than the U.S. and others.

Cyberspace is an ideal medium for stealing intellectual capital. Hackers can easily penetrate systems that transfer large amounts of data, while corporations and governments have a very hard time identifying specific perpetrators.

Unfortunately, it is also difficult to estimate the economic cost of these thefts to the U.S. economy. The report to Congress calls the cost "large" and notes that this includes corporate revenues, jobs, innovation and impacts to national security. Although a rigorous assessment has not been done, we think it is safe to say that "large" easily means billions of dollars and millions of jobs.

So how to protect ourselves from this economic threat? First, we must acknowledge its severity and understand that its impacts are more long-term than immediate. And we need to respond with all of the diplomatic, trade, economic and technological tools at our disposal.

The report to Congress notes that the U.S. intelligence community has improved its collaboration to better address cyber espionage in the military and national-security areas. Yet today's legislative framework severely restricts us from fully addressing domestic economic espionage. The intelligence community must gain a stronger role in collecting and analyzing this economic data and making it available to appropriate government and commercial entities.

Congress and the administration must also create the means to actively force more information-sharing. While organizations (both in government and in the private sector) claim to share information, the opposite is usually the case, and this must be actively fixed.

The U.S. also must make broader investments in education to produce many more workers with science, technology, engineering and math skills. Our country reacted to the Soviet Union's 1957 launch of Sputnik with investments in math and science education that launched the age of digital communications. Now is the time for a similar approach to build the skills our nation will need to compete in a global economy vastly different from 50 years ago.

Corporate America must do its part, too. If we are to ever understand the extent of cyber espionage, companies must be more open and aggressive about identifying, acknowledging and reporting incidents of cyber theft. Congress is considering legislation to require this, and the idea deserves support. Companies must also invest more in enhancing their employees' cyber skills; it is shocking how many cybersecurity breaches result from simple human error such as coding mistakes or lost discs and laptops.

In this election year, our economy will take center stage, as will China and its role in issues such as monetary policy. If we are to protect ourselves against irreversible long-term damage, the economic issues behind cyber espionage must share some of that spotlight.

Mr. McConnell, a retired Navy vice admiral and former director of the National Security Agency (1992-96) and director of national intelligence (2007-09), is vice chairman of Booz Allen Hamilton. Mr. Chertoff, a former secretary of homeland security (2005-09), is senior counsel at Covington & Burling. Mr. Lynn has served as deputy secretary of defense (2009-11) and undersecretary of defense (1997-2001).