Statement of U.S. Senator Sherrod Brown, Chairman of the Congressional-Executive Commission on China (CECC)

CECC Hearing on "Chinese Hacking: Impact on Human Rights and Commercial Rule of Law"

June 25, 2013, Washington, DC

I thank Cochairman Chris Smith, the other Commissioners, and our esteemed panel for attending this important hearing.

I also thank the staff for their tireless efforts in supporting the work of this bipartisan Commission and its important task of monitoring human rights and rule of law developments in China.

Cyber attacks from China pose a serious threat to U.S.-China relations.
So much so that President Obama raised the issue during his recent summit with President Xi Jinping. It will be a key topic at the U.S.-China Strategic and Economic Dialogue to be held in Washington in a few weeks.

Today's hearing will focus on the aspects of cyber that fall within the Commission's mandate, namely the impact on the rule of law and human rights in China.

While recent headlines have revived the debate over the appropriate balance between security and freedom, we must not overlook the enormous impact cyber attacks from China have had and continue to have on American jobs and companies. Indeed, they seriously call into question China's commitment to the rule of law.

We are talking about the massive theft of valuable technology and commercial secrets from American companies—what General Keith Alexander, director of the National Security Agency and head of U.S. Cyber Command, calls the "greatest transfer of wealth in history."

The scale and scope is staggering. The Commission on the Theft of American Intellectual Property, which is represented here today by our former colleague Senator Slade Gorton, released a comprehensive, report identifying China as the world's biggest violator of intellectual property rights.

It estimates that China accounts for some 50 to 80 percent of IP theft in the United States and around the globe. It found that international IP theft, including from China,

costs the U.S. economy hundreds of billions of dollars per year and millions of jobs, dragging down our GDP and undermining our ability to innovate and prosper.

The IP Commission noted that a 2011 study by the U.S. International Trade Commission estimated that if China's IP protection improved to a level comparable to ours, it would add 2.1 million jobs to our economy. Yet, the IP Commission acknowledged this figure underestimated the real cost to American jobs.

The victims of IP theft include companies in my state of Ohio and across the nation. Those affected are hard-working Americans trying to make an honest living and trying to spur innovation, only to see their products, services, and technology stolen and handed over to state-owned enterprises and businesses in China.

And with the growing prevalence of computer networks and America's heavily-wired economy, cyber attacks represent an increasingly growing threat alongside more traditional forms of IP theft.

China simply doesn't play by the same rules as we do. The Chinese government has denied these attacks, even though there is mounting evidence of Chinese state involvement. This evidence includes a February 2013 report by the cyber security firm Mandiant that linked attacks on 141 companies, including 115 based in the United States, to a unit of the People's Liberation Army working from a building in Shanghai. The increase in attacks has coincided with the Chinese government's push for indigenous innovation and development of key industries, creating an environment where it's perfectly acceptable to cheat and steal your way to the top.

And as we've seen in the last few years, it's not only American companies that are the target of cyber attacks. It's also media and human rights organizations. Journalists writing about corruption in China find their computer systems hacked and passwords stolen. For human rights organizations and activists, dealing with hacking attacks from China is almost a daily fact of life.

We can't sit idly by while the Chinese government, either through active measures or by turning a blind eye, continues to perpetuate theft on a grand scale and to threaten the advance of human rights for the Chinese people, Tibetans, Uyghurs, democracy advocates, religious followers, and Falun Gong practitioners.

That's why I support a comprehensive, common sense, bipartisan approach that utilizes every tool in our arsenal to hold China accountable and to level the playing field. I urge Congress and this Administration to do everything it can – from leveraging access to our markets, trade negotiations, and WTO cases – to combat China's unfair trading practices. That includes taking up the bipartisan Currency Exchange Rate Oversight Reform Act of 2013 which I introduced earlier this month.

And I commend Senator Levin for his recent proposed legislation to hold China accountable for cyber theft. I look forward to hearing from our witnesses on what more we can do to address this most pressing issue.