

**Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing on China's Non-Traditional Espionage Against the United States:
The Threat and Potential Policy Responses
Wednesday, December 12, 2018**

We've heard a constant drumbeat over the past two years about the national security threats posed by Russia. Attempts to sow discord and inflame partisan differences through social media, and attempts to interfere with our elections through cyber intrusions are real threats. They should not be underestimated. I've held seven hearings on election meddling.

But the media hysteria over all things Russia has distracted attention from arguably a greater, more existential threat: China's efforts to overtake the United States as the world's preeminent superpower in all phases of society. China has made no bones about doing this through any and all means. Whether it be President Xi's stated goal of becoming "the world's biggest superpower" by 2050, or the "Made in China 2025" initiative that called for a ten year overhaul of China's manufacturing and high-tech industries, the PRC's plans for superiority includes economic dominance.

The United States remains the most creative, innovative society on earth. Although China has made significant strides in various sectors – including technology, telecom, advanced robotics, artificial intelligence, and scientific research – one tool of economic advancement continues to be pervasive. That's economic and other forms of espionage.

In simple terms, it's called cheating. And it's only getting worse.

In the past nine months alone, DOJ has investigated, charged, or convicted at least 16 individuals and four corporate entities in eight separate cases involving theft of trade secrets. Over the past five years, six more individuals have been either investigated, charged or convicted by DOJ for stealing research from American universities. One case involves a Chinese intelligence officer who is a deputy division director from China's main spy agency. He's the first Chinese intelligence official to be brought to the United States and tried in open court. A slew of other Chinese intelligence officers and hackers were charged in a multi-year plan to steal sensitive commercial aviation data. Then there is the massive plot by a Chinese government-owned company to steal U.S. semi-conductor technology. These cases, in particular, highlight the threat of Chinese state-controlled economic espionage.

Just last week, we saw the arrest of the Chief Financial Officer of Huawei, the largest telecommunications company in China. And a financial firm owned by China's Ministry of Finance reportedly used various shell companies to conceal efforts to get sensitive satellite technology from Boeing. That technology has potential military applications.

Although those two cases did not strictly involve espionage, they point to a broader issue: cold disinterest to American sanctions enforcement and a callous indifference for broader adherence to the rule of law.

When it comes to espionage, FBI Director Wray has said “there’s no country that’s even close” to the People’s Republic of China. General Keith Alexander called China’s estimated gains from economic espionage of up to \$600 billion, “the greatest transfer of wealth in history.” China is believed to be responsible for 50 to 80 percent of cross-border intellectual property theft worldwide, and over 90 percent of cyber-enabled economic espionage in the United States. Reports issued this year by the White House Office on Trade and Manufacturing, the U.S. Trade Representative, and ODNI all report detailed findings on China’s role as a prime cyber-attacker and thief of American intellectual property and technology.

The National Institutes of Health announced in August of this year that it has discovered NIH grants are going to researchers who are not disclosing their contributions from foreign governments. Chinese “Talent programs” seek to recruit American researchers, in order to bring technological advancements back to China. Confucius Institutes, found at many of our nation’s top universities, and directly funded by the Chinese government, stifle intellectual freedom and quiet all those who would criticize China with revisionist histories.

In response to the growing number of cases, DOJ recently announced a new initiative to combat Chinese economic espionage. I look forward to hearing more about the initiative and any legislative proposals needed to address these problems.

We often get distracted by the shiny objects in front of us. I fear that China is all too happy to have our attention deflected away from the threat they pose to our economy, our innovation, our businesses, and our very standing in the world.

Nobody is in favor of billions in American IP being stolen. Nobody supports researchers violating the terms of their government grants in favor of a foreign government. We all should condemn cyberattacks on government and private sector information and systems. The question is: how can we counter these activities? I hope we can come to an answer together.