Securing U.S. Surface Transportation from Cyber Attacks
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
Testimony of James A. Lewis, Center for Strategic and International Studies
Tuesday, February 26, 2019

I would like to thank the Committee for the opportunity to testify. My testimony will discuss the risks to homeland security from the use of Chinese technology and equipment.

Chinese companies face a serious branding problem in many countries. There is a level of distrust that has been created in good measure by Chinese government policies. The most prominent of these policies are China's aggressive mercantilism, its disregard for international law, its massive espionage campaign and, for the U.S., its announced intention to displace America and become the most powerful country in the world, reshaping international rules and practices to better fit the interest of China's rulers.

Espionage has been a part of the of the Sino-American relationship since China's opening to the West in 1979. It is worth remembering that at this time, the U.S. and China shared a common enemy – the Soviet Union. This created incentives for cooperation that have long vanished. Chinese espionage initially focused on repairing the disastrous effects of Maoists policies on China's economic and political development. This meant the illicit or coercive acquisition of western technology. As China's cyber capabilities improved, beginning in the late 1990s, some PLA units turned to hacking as a way to supplement their incomes, moonlighting by stealing western intellectual property and then selling it to Chinese companies.

The illicit acquisition of technology is still a hallmark of Chinese espionage activity, but there have been significant changes since President Xi Jinping came to power in 2013. One of the first things Xi did, reportedly, is order an inventory of Chinese cyber espionage activities. He found that many of these had not been ordered by Beijing, that Beijing did not have full control over tasking and assets, and some operations were for private interest and did not meet China's strategic requirements.

Xi changed this. The Chinese military has been reorganized as part of a larger effort to modernize the PLA. Xi's anti-corruption campaign greatly reduced the ability of PLA units to "moonlight." Chinese intelligence collection is better organized, more focused on strategic priorities, and, some would say, better in performing its missions. This comes at a time when, according to the U.S. intelligence community, Chinese espionage has reached unprecedent levels. Today, these efforts focus on the acquisition of advanced military and commercial technologies, since China still lags the U.S. in technology, as well as military and government targets.

The U.S. and China reached an agreement in 2015 to end commercial cyber espionage, but it is generally believed that this agreement has broken down in the last year. At the risk of sounding overly dramatic, some would describe this situation as an undeclared espionage war between China and the U.S. In fact, this is not a war, but a very intense contest where the U.S. is largely

on the defensive. Our allies also face a similar problem with Chinese efforts in Australia, Japan, Germany, the UK, Canada, and other advanced economies.

These activities create distrust, and a more specific ground for distrust is China's 2017 National Intelligence Law. For some years, the U.S. had advised China to move away from an informal, ad hoc system of rules and put in place a formal legal structure based on laws. The Chinese took our advice and one result is that long-standing Chinese policies and practices have been codified into the 2017 Intelligence Law. The most important part of that law for today's hearing is that it creates a legal obligation for Chinese companies to cooperate fully with intelligence agencies upon request. There are no grounds for appeal or an ability to refuse such requests.

This means that a Chinese company could be completely innocent of any wrongdoing, its products harmless, but a decision by the Chinese government could change that in an instant. In the context of an increasingly aggressive global espionage campaign, often conducted using cyber techniques, there are reasonable grounds for the distrust of Chinese products. The first question to ask is not whether you trust a Chinese company, but whether you trust the Chinese government.

Concerns over the Intelligence Law have become so significant, in part because of the implications of using Huawei telecommunications equipment, that China's official news agency felt obliged last week to put out a press release calling for a comprehensive and accurate translation. China's Foreign Ministry pointed out that while Article 7 of the law stipulates the obligation for Chinese companies and individuals to "support, assist and cooperate" with the country's intelligence service, Article 8 stipulates that China's intelligence service should carry out its work according to law, protect human rights, and safeguard the legal rights and interests of individuals and organizations. Unfortunately, this promise is undercut by China's recent behavior in regard to human rights and in the protection (better expressed as the absence of protections) for the intellectual property of foreign companies.

We should note that China's government expresses similar concerns over their reliance on western technology, in part because they assume the relationship between western companies and government is the same as the relationship between Chinese companies and the government. This official distrust of western products is one reason why Beijing is spending billions of dollars to develop national sources of supply for many technologies. These subsidies also provide commercial benefit, in building national champions in Chinese industry and in eroding western companies' market position.

China also leads the world in building a national system of pervasive domestic surveillance. Communications and social media are monitored, and an array of sensors monitor and record activities in urban areas. This sensor data is correlated with information held by the government on Chinese residents' behavior and communications. This pervasive surveillance is not popular among many Chinese, but it is increasingly difficult to escape. One concern is that China will to some degree extend this pervasive surveillance to countries and persons of interest outside of China, or extend its extensive cyber espionage campaign to include coercive actions, like disrupting critical services. This is not something China would do lightly, but the risk cannot be dismissed

The combination of increased espionage, new legal obligations, pervasive surveillance, and heightened military tensions make for an uncomfortable and potentially dangerous situation, with implications for U.S. security. The U.S. and China share a deeply integrated industrial base, constructed during the time when we assumed that China was moving in the direction of becoming a market economy and a security partner. Disentangling this deeply integrated supply chain would be costly and damaging to both countries, but some in America now talk about a "divorce" while China is spending heavily to reduce its reliance on the U.S.

Beyond the espionage risk, there is potential risk for critical infrastructure that is growing. As more devices become connected to the internet and reliant on software, the opportunities for disruption will grow. This is not specifically a China problem, but a change in the technological environment as millions of devices connect to the internet in ways that China (or other malicious actors) could exploit for coercive purposes.

As the Committee has heard for many years, the state of cybersecurity remains poor and almost any network or device can be hacked with enough persistence. Cybercrime continues to grow, and cyber tools have become an essential part of state conflict. If it is any consolation, China's cybersecurity is worse than ours, if only because of their frequent use of pirated software. Improving cybersecurity should be a potential area for cooperation between the two countries, but the current state of relations does not permit that.

An environment of connected devices, often called the internet of things, is formed by devices that connect to the global internet, usually without human intervention. We all have heard of smart cars but many large systems in infrastructure and transportation also rely on computers and connectivity. This environment will provide real economic opportunities and benefit, but it also comes with an increase in risk. Our task should be to estimate this risk and then develop strategies to mitigate it. Different technologies and different companies create different levels of risk, and there are several ways to assess this.

One way to scope risk is to ask how a device connects to the internet, what onboard sensors it has, what information it collects and transmits, and how much transparency, insight, and control an operator has over this data and connection. Many large capital goods – such as power technologies, pipelines, telecommunications and ships, are continuously connected over the internet to their manufacturer, to allow for status reports, maintenance scheduling, and for the updating of software. This continuous connection provides an opportunity to collect information and to disrupt services. Instead of an update, a command could be sent to turn off, or to reduce speed.

We have seen several example of Chinese devices that report home, from drones to surveillance cameras, with the concern that under the new intelligence law, the Chinese government could compel the provision of the data collected by these technologies. This kind of monitoring and collection has been a standard practice for intelligence agencies that will certainly extend to the internet of things, and the risks of connected devices is compounded when their home is in a hostile foreign power.

We could scope risk by measuring the cybersecurity status of connected devices. The National Institute of Standards and Technology (NIST) is developing, in partnership with industry, standards for the security of IOT devices. But this is still at a relatively early stage. In general, the internet of things will be no more secure than the existing internet and may be more vulnerable, since many IoT devices will use simple computers with limited functionality.

We can also assess risk by using three metrics – the value of the data accessible through or collected by the IOT device, the criticality of a function the connected device provides, and scalability of failure. Devices that create or collect valuable data, perform crucial functions, or that can produce mass effect, need to be held to higher standards and face greater scrutiny.

For critical infrastructure, we need to ask the same questions about using Chinese products that we would ask for any critical infrastructure protection policy: how sensitive are the operations and the data associated with or accessible through the infrastructure, what would happen if the infrastructure was disrupted by an opponent, how would we continue to operate and then recover in the event of a malicious incident, and for foreign products, and to what degree is control or access shared with the foreign manufacturer.

The type of data collected and transmitted is a crucial element of a risk assessment. Intelligence analysis data is driven by access to large amounts of data and the ability to correlate it with other data. Data analytics provides new intelligence insights. A well-known example is the hack attributed to China of the Office of Personnel Management and the theft of personal information. It is likely that OPM was one of a series of related hacks, of insurance companies, airlines and travel agencies, that provided additional data that could be used to gain insight into America personnel and practices. This means that even seemingly insignificant data, if correlated with other information, may provide influence value. The more "granular" the data, and whether it refers to specific individuals, the greater its value. Less granular data, such as how many people are sitting on a train or at which stop they exit, may not pose much risk.

Managing our new competition with China will be difficult given the close interconnection between the U.S. and Chinese economies. This is a 30-year commercial and technological partnership not easily dismantled by either side. Given the deep interconnections that have grown between the Chinese economy and the rest of the world, a bifurcation similar to that seen during the Cold War is not possible, and it is not now in our interest. A greater degree of separation between the two economies is necessary, but must be carefully developed for specific technologies and based on a judgment on the risk that their use could provide China with an intelligence, military or unfair commercial advantage.

These risks are manageable, and we have to contrast them to the risk to the America economy from a violent disruption of trade with China. Generally speaking, a complete divorce is not in our interest; and it is certainly not in China's interest. There are specific technologies and circumstances that require greater scrutiny and countermeasures, but this does not apply across the board (at least at this time). Working with our allies, we can modify China's behavior to make this relationship more stable and less risky. We have done so in the past, but this will be a process that will take years to complete, and in the interim, there are steps we must take to reduce the risk of Chinese interference and espionage.

The most obvious is continued work to improve network and device security. This will require some measure of regulatory action and close partnership with the affected industries and operators. One size does not fit all when it comes to regulation, so the potential risk of IOT and Chinese technology must be managed using the sector-specific model developed in the previous administration, and partnerships between companies, agencies with oversight, and DHS's new Cybersecurity and Infrastructure Security Agency (CISA) should be the core of this effort.

The development of security standards is a necessary complement to any regulation or voluntary action. The NIST Cybersecurity Framework is a good starting point for this, but must be extended and modified for different kinds of transportation systems. CISA's Transportation Systems Sector Cybersecurity Framework Implementation Guide, published in June 2015, provides guidance to owners and operators on how to assess and implement cybersecurity standards.

All of these measures -voluntary action, regulation and standards - must be predicated on the knowledge that we cannot keep opponents out of our networks and devices – we can make it harder for them but not impossible. This means that measures to increase resiliency, to allow for some level of continued operation in degraded conditions is essential. This adds expense to critical infrastructure, of course, and one part of any plan is to ask how this additional burden will be funded and whether the increase in risk is outweighed by the potential savings – we should not automatically assume that the mere existence of risk cancels out financial benefits.

All of these steps require oversight to assess risk and improvement. This is clearly a task for Congress and this Committee, but also for the responsible agencies, industry bodies, and in particular for CISA. The key question for assessment is whether the use of the Chinese technology increases the risk of disruption or espionage, and the answer to this will depend in good measure on how the Chinese products connect to the internet.

Finally, a purely defensive approach will be inadequate. The U.S needs to develop and articulate credible counterthreats to dissuade and deter foreign attackers. This may require more than sanctions and indictments. Although they are useful and have effect over the long term, they may need to be reinforced other punitive measures, part of a larger strategy on how to impose consequences and change opponent thinking. Given the level of vulnerability and the potential increase in risk from both the acquisition of foreign technology and the digitizing of critical services, we must persuade opponents that any interference will come with unacceptable risk or retaliation by the U.S.

There are trade issues that I have not touched upon, such as the Chinese practice of building national champions through government subsidies and, in some cases, industrial espionage. China also uses non-tariff barriers and other protectionist mechanism to hobble or block competition from foreign firms in China. These Chinese practices harm our national interests and should be opposed as part of a larger effort to change China's behavior and move it in the direction of reciprocity.

I thank the Committees for the opportunity to testify and look forward to any questions.