**Andy Keiser**
Visiting Fellow, National Security Institute
George Mason University's Antonin Scalia Law School

**Testimony before the United States House Committee on Small Business**
**June 27, 2018 hearing titled: ZTE: A Threat to America's Small Businesses**

Thank you Chairman Chabot, Ranking Member Velazquez and distinguished members of the Committee.

As someone who spent the first part of my career roaming these halls as a House staffer, it's wonderful to be back home among friends – particularly before a Committee that is taking a sobering, bipartisan look at one of America's greatest long-term national security threats: the threat posed by Zhongxing Telecommunications Equipment Corporation (ZTE) and Huawei to our telecommunications infrastructure.

I will start with a story to which I imagine many of you will easily relate. My former boss, House Intelligence Committee Chairman Mike Rogers, first became interested in the activities of ZTE and Huawei not because he was a former U.S. Army officer or Federal Bureau of Investigation (FBI) special agent. Initially, his interest did not even stem from his position on the Intelligence Committee, but because a Michigan company approached him with a problem.

As each of you would do, he listened to that small business owner carefully. As it turned out, Chinese telecommunications companies –ZTE and Huawei – were bidding to build cellular telephone towers in the most rural parts of Michigan, far from population centers like Detroit. This small business owner was happy to compete but said the Chinese telecoms were coming in not just under his price, but under what *the materials would cost* to build the towers.

That got a former FBI agent thinking: why on earth would they be doing that? More on this later.

As I don't need to remind this room, small business is the lifeblood of the American economy. Small business employs more than half of the U.S. workforce and two out of every three new private-sector jobs created in America are created by small businesses.

Small business in America is inherently resilient, creative, and able to adapt quickly to market conditions. One thing small business cannot do effectively, however, is compete against nation-state attacks, aggressive, unrelenting international espionage, and theft of trade secrets. And those are exactly the challenges presented by ZTE and Huawei.

For thousands of years, China viewed itself as superior to all other world powers. Following a self-described "century of humiliation" resulting from imperialist incursions from the West and Japan, it now seeks a return to that perch.

Under the consolidated leadership of Xi Jinping, newly declared "President for life," China today intends to become a global economic, military and technological leader rivaling or surpassing the United States and it aims to do so in the next 10-15 years. There are troubling indicators: China's gross domestic product is currently on track to surpass that of the United States by 2029. And the Chinese military is rapidly modernizing, directly targeting areas in which the U.S. maintains dominance, including in the cyber domain, space and power projection at sea.

When I attended the Shanghai-hosted World's Fair in 2010, China was portrayed as a civilization that led the world for millennia. The storyline went that, now with failing powers like Russia and stagnating powers like the United States and Europe, China will again be called upon to lead the way into the future.

Part of China's grand vision includes dominance in fields that have dual economic and military benefit. In 2015, Chinese leaders unveiled the "Made in China 2025" strategic plan. It focuses on the country becoming the world's leader in high-tech fields, squarely within the learned and stolen expertise of ZTE and Huawei.

ZTE and Huawei are working fast to put Western vendors out of businesses to secure market dominance. In just seven years, Huawei went from an afterthought with poorly-functioning equipment and only 10 percent market share to having the top position now in the lucrative LTE radio business. Excluding the United States, Huawei enjoys roughly 38 percent of the total market share globally.

By investing heavily in research and development, ZTE and Huawei are organically improving their native capacity to innovate, but they also have copied and stolen their way to success. Huawei has admitted to stealing router product secrets from Cisco. The theft was extensive, all the way down to the spelling errors in the manuals. And apparently Huawei stole the design for Apple's iPhone literally down to the last screw.

Nonetheless, Huawei has surpassed every telecommunications provider in the Asia Pacific, Europe and in Latin America. Only markets in the United States and Middle East remain competitive due to the concerns raised by vocal U.S. government security leaders in the Administration and Congress. Huawei is now dominant in fixed access, IP routing, and LTE in many markets and is growing shares of these critical businesses in others. Western vendors are still able to compete for certain products and in certain markets, but it is unclear how long that will remain true. Absent U.S. government initiative and continued attention, the only telecommunications infrastructure option available in the world in the not-too-distant future could be a Chinese one.

In my view, ZTE and Huawei do not share the motivation of most Western companies. Profit is not the motive. Deploying equipment in rural Michigan and all around the world at or below cost is not being done to make shareholders money; it is being done to harness the ability to collect vast quantities of information and to create leverage against adversaries in a potential conflict. National security thought leaders from both parties - like Senators Marco Rubio and Mark Warner – have brought attention to this threat. If Chinese telecom giants are allowed to infiltrate our telecommunications backbone, in a potential conflict they could incapacitate critical infrastructure – for instance, our electric grid — bogging us down at home, while impairing our capacity to respond overseas.

Chinese companies generally cannot be decoupled from the Chinese state. Resident Scholar Derek Scissors with the American Enterprise Institute has said, "ZTE is a tool of the Chinese state, which is controlled by the party." Indeed, under Chinese law, all Chinese companies, including Huawei and ZTE, are required to fully cooperate with Chinese law enforcement and intelligence services.

If there was any question about Chinese government support to ZTE and Huawei, consider that ZTE is currently working to secure an $11 billion financing package from the Bank of China and the China Development Bank. This was done after losing nearly half of its' value following the issuance of the U.S.

Commerce Department's denial order forbidding their acquisition of U.S. components. It is fair to say that no Western supplier would be able to secure that level of state-sponsored cash infusion under such circumstances.

ZTE and Huawei have developed dubious reputations around the world. In the past 12 years alone, ZTE and/or Huawei entities have been investigated or found guilty of corruption in Kyrgyzstan, Uganda, Cameroon, Ethiopia, Gabon, Zimbabwe, Nigeria, the Philippines, Gambia, Ghana, Algeria, Malaysia, Norway, Zambia, Singapore, South Sudan, South Africa, Papua New Guinea, Mongolia, the Solomon Islands and even in China itself.

The Arab spring led despots and dictators around the world to look to prevent a similar fate to that of Muammar Gaddafi being dragged through the streets. Andrew Rizzardi from Freedom House says the Chinese – i.e. ZTE and Huawei – own the "authoritarian telecommunications hardware store." ZTE and Huawei technologies are being used to suppress dissent in nearly all African countries. In recent years, advanced monitoring technology has been sold to Zambia, Ethiopia, Iran, Pakistan, and Venezuela by ZTE or Huawei. Authoritarianism is now officially a key Chinese export.

The most comprehensive review to date of the threat generated by ZTE and Huawei was conducted right here by the United States Congress in a bipartisan way – specifically, in 2012 by the House Permanent Select Committee on Intelligence (HPSCI). I was Chief of Staff to Committee Chairman Mike Rogers at the time and the report was fully supported by Ranking Member Dutch Ruppersberger. Many of its findings still hold true today.

The 2012 HPSCI report stated that: "the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national security interests."

Most relevant to today's hearing, the report also found that: "private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services."

As background, ZTE has its origins in the Chinese Ministry of Aerospace and the government-run 691 factory, which is a now part of a state-owned research institution. According to the HPSCI report, the Zhongxinxin group, owned in part by two state-owned enterprises, has a controlling interest in ZTE.

Internal Chinese Communist Party committees are also embedded within Huawei and ZTE. As of 2012, ZTE had Communist Party Committee members on its Board of Directors and serving as key shareholders.

During the HPSCI investigation, ZTE repeatedly argued that it could not provide internal documentation or fully answer the Committee's questions for fear that it would be in violation of China's state secrets law and could be subject to criminal prosecution in China. In my view, this lack of response proves the point of concern.

The founder of Huawei, Ren Zhengfei, was a director of the People's Liberation Army (PLA) Information Engineering Academy, which is associated with 3PLA, China's signals intelligence division and the country's version of the National Security Agency. Ren also retains veto power over the company's decisions.

According to the HPSCI report: “Huawei operates in what Beijing explicitly refers to as one of seven “strategic sectors.” Those are considered as core to the national and security interests of the state. In these sectors, the Chinese Communist Party ensures that “national champions” dominate through a combination of market protectionism, cheap loans, tax and subsidy programs and diplomatic support in the case of offshore markets.”

A separate, major U.S. investigation into ZTE began in 2012 after Reuters reported on the firm’s business dealings with Iran. The Department of Justice found that ZTE conspired to evade Iran sanctions to secure contracts worth hundreds of millions of dollars by installing telecom equipment that required U.S. components, which was in direct violation of U.S. export controls.

ZTE admitted committing 380 violations and engaged in an elaborate scheme to prevent disclosure to the U.S. government, including forming a group to destroy, remove and sanitize all evidence relating to its dealings with Iran.

After failing to comply with the terms of the settlement, the U.S. Department of Commerce issued an April 15, 2018 denial order stating that ZTE demonstrated “a pattern of deception, false statements, and repeated violations.”

The denial order forbidding ZTE from acquiring U.S. components went on to state that: “ZTE agreed to a record-high combined civil and criminal penalty of $1.9 billion, after engaging in a multi-year conspiracy to violate the U.S. trade embargo against Iran to obtain contracts to supply, build, operate and maintain telecommunications networks in Iran using U.S.-origin equipment, and also illegally shipping telecommunications equipment to North Korea.”

Also, in April, Federal Communications Commission (FCC) Chairman Ajit Pai circulated a proposal to ban Huawei and ZTE from receiving government funds that subsidize low-income Americans’ access to phone and internet service.

In a statement, Chairman Pai wrote that: “Hidden ‘back doors’ to our networks in routers, switches—and virtually any other type of telecommunications equipment—can provide an avenue for hostile governments to inject viruses, launch denial-of-service attacks, steal data, and more.”

In a 92-page submission responding to the FCC, Huawei attempted to equate PLA-founded Chinese telecommunications companies with U.S. companies who have a manufacturing presence in China. This is a ludicrous comparison as the U.S. companies are there due to requirements of doing business in China, not out of any allegiance to the Chinese government. The response, carefully written by American lawyers at two leading Washington, DC law firms, parses language from the Directors of the FBI and the National Security Agency in an effort to minimize the threat. It also attributes numerous Constitutional rights afforded to Huawei’s U.S. subsidiary. I doubt that the founding fathers of the United States intended to protect the rights of companies controlled by our adversaries seeking to compromise core national security interests.

In response to the ongoing and known security threats by these two companies, last month the Department of Defense ordered all ZTE and Huawei equipment to be removed from military installations.

ZTE and Huawei have the capability, clout, motive and growth strategy to pose a continuing national security threat to the United States – one that directly harms American small business. Surely in part due to your steady work in this committee raising the profile of the issue, Congress has become convinced of this in a bipartisan way.

The legislative House and Senate activity occurring around the 2019 National Defense Authorization Act could provide a long-term solution to the threat posed to the U.S. by reinstating the Commerce Department's denial order forbidding ZTE from using U.S. components, perhaps except for providing common-sense security patching and upgrades. This would be a severe blow to ZTE and would be a critical win for the United States of America's national security posture as we confront a rising China threatening our interests around the globe.

Chairman Rogers and Congressman Ruppersberger again teamed up to pen an Op-ed earlier this year in the *Wall Street Journal* which called the threat from ZTE "a clear and present danger to U.S. national security." I agree completely and encourage this body to respond accordingly.

Chairman Chabot and Ranking Member Velasquez, thank you so much for convening this hearing and raising these important issues. I look forward to your questions.