Statement before the

Senate Committee on the Judiciary

"5G: The Impact on National Security, Intellectual Property, and Competition"

A Testimony by:

James Andrew Lewis

Senior Vice President and Director, Technology Policy Program

Center for Strategic and International Studies (CSIS)

May 14, 2019

226 Dirksen Senate Office Building

I would like to thank the Committee for the opportunity to testify on a topic of critical importance to the United States. This goes well beyond 5G, although 5G is the focal point. 5G networks will shape the digital economy - this is why there is such intense competition. The United States can manage 5G risk with two sets of policies. The first is to ensure that American companies can continue to innovate and produce advanced technologies and face fair competition overseas. The second is to work with like-minded nations to develop common approaches to 5G security.

Telecom is a strategic industry and a reliance on Chinese companies creates risk for the United States and its allies. A secure supply chain for 5G closes off dangerous areas of risk for national security in terms of espionage and the potential disruption of critical services. China's coercive behavior and aggressive global campaign of cyber espionage makes it certain that it will exploit the opportunities it gains as a 5G supplier.

How did we get here? America and other Western countries assumed China would be a friend and would evolve to become a market economy, and perhaps even somewhat democratic. For a time, this seemed to be the direction China was taking. In that period, American and Western companies were eager to do business in a fast-growing market with low labor costs. Money and technology poured into China, and what technology China was not given or could buy, it would steal. Companies knew that there were risks, but they thought these risks were manageable. China was for the first few decades of its growth, still a poor country, still developing and this encouraged an underestimation of risk.

How should we portray the struggle with China? It is easy for the U.S. to look backwards and dredge up Cold War terms and concepts that are inappropriate for a new kind of conflict in a new century – we do not need another Solarium Commission, this is not an arms race, nor in fact, is it a Cold War. What we discuss in Washington is too often like ancestor worship rather than strategy. The chief similarity between the Cold War and the conflict with China is that it is a battle for global influence where both China and the U.S. have advantages and disadvantages. China's greatest advantage is that it is willing to spend money while the U.S. is not. China's political system is not particularly attractive and Han nationalism limits China's influence, but many countries will, in the near term, want to work with China.

China was allowed into the World Trade Organization (WTO), opening global markets to its industries, but the preparatory agreement between the U.S. and China did not require any Chinese commitment on protection of intellectual property (IP). This was an immense mistake. China did not extend reciprocal treatment to Western companies. China used non-tariff barriers and subsidies contrary to its WTO commitments, and it was not held accountable, perhaps the greatest failing of the WTO and one reason why it is in such disrepute today. Now that it is the second largest economy in the world, the policies the U.S. and others followed in regard to China until a few years ago have come back to haunt us.

5G is a problem because neither the U.S. nor other Western nations objected in the WTO to China's mercantilist behavior in telecommunications. Huawei founder and chairman Ren Zhengfei even said, "If there had been no government policy to protect [nationally owned telecom companies], Huawei would no longer exist." Huawei uses predatory pricing enabled by

Chinese government subsidies to drive its competitors out of business, it benefits from China's economic espionage (Chinese IP theft was a significant contributor to the demise of Nortel, the Canadian telecommunications company). It has a long record of industrial espionage and IP theft on its own account that began with the company's founding and continues to this day, as evidenced by the many court cases for IP theft it has faced. Huawei's reliance on industrial espionage, its murky ownership, and its long-standing and close ties to the Chinese security services raise serious questions for any country thinking about 5G.

There has been a significant change in attitudes over the last few years on the issue of China. Until recently, Western companies and trade associations would usually often demur from any criticism of China or any effort to get it to change its behavior. This is no longer the case. There is a growing consensus in the U.S. and other advanced economies on the risks of doing business with China. The Chinese are puzzled, by the global reaction to government's aggressive mercantilism and disregard for global business norms, to the extent they can read about it in their heavily censored media.

5G and Risk

Why is 5G important? First, 5G is more than phones, it is a new kind of network technology that will connect millions of devices and provide unparalleled mobility and capacity. This means that self-driving cars, smart cities, telemedicine and smart factories - a whole range of new activities and devices - can use 5G to provide expanded services at lower costs. 4G, the smart phone revolution, created the "app economy" which in five years has grown from nothing to more than $100 billion, or about five percent of U.S. GDP. 5G will more than duplicate this success and generate hundreds of billions in revenues.

Countries hope to duplicate the success of U.S. companies in creating 4G and hope to "capture" 5G so as to reap the economic benefits for themselves. China is not alone in this as European and Asian countries seek to be the first to deploy 5G networks and gain the boost to innovation it will provide. This is a competition over who owns the revenue streams that 5G innovations will produce. Building and deploying 5G networks will create the next wave of global innovation, which is one primary reason for not letting China unfairly dominate this market.

There would be no grounds for objection if China competed fairly, but it does not, since it stifles foreign competition in China, fails to provide Western companies with reciprocal treatment, and uses subsidies, espionage, and other illicit techniques to win foreign markets. China has innovative companies, particularly in the internet sector, and while these companies make excellent products, they suffer from a trust issue, snice the social media and messaging services they provide are completely monitored by the Chinese government. A more important problem for China is that these innovative companies were private, not state-owned, and grew up during a period of relative political openness. As the Chinese government adopts more intrusive policies to control company operations and investments, and as the Chinese political space closes, there is a risk that China's ability to innovate will be damaged. One thing to watch if this occurs, is that China will expand its already massive technological espionage campaign to compensate.

The illicit acquisition of technology remains central to Chinese espionage. When President Xi Jinping came to power, he reorganized Chinese intelligence tasking and collection priorities. Xi reportedly ordered an accounting of Chinese cyber espionage. Before Xi, a significant proportion of Chinese espionage was "private," used for private gain by PLA units. Under Xi, cyber espionage has been reorganized as part of a larger military modernization effort. Chinese intelligence collection is more focused on strategic priorities, and, some would say, better in performing clandestine missions. This comes at a time when, according to the U.S. Intelligence Community, Chinese spying has reached unprecedent levels. This still focuses on acquiring advanced technologies, since China still relies on Western sources for this.

Much of the 5G discussion has focused on supply chain issues and the risk of using Chinese telecom equipment.[1] There are three parts to this discussion. First, many technologies use the internet to connect to their manufacturer even after sale for maintenance, updates, and status reports. We are all familiar with how our phones or computers are updated, often without our knowledge. An increasing number of products will remain connected to the manufacturer after sale, allowing both improved services, but also creating new opportunities for malicious actions, particularly when the manufacturer comes from a hostile foreign power.

Major telecom “backbone” equipment connects to the manufacturer over a dedicated channel, reporting on equipment status and receiving software updates as needed, usually without the operator’s knowledge. Equipment could be sold and installed in perfectly secure condition, and a month later, the manufacture could send a software update to create vulnerabilities or disrupt service. The operator and its customers would have no knowledge of this change.

Huawei, for example, with both its 4G network equipment (which is widely used in Europe and Africa) and its new 5G technologies, retains access and control to this equipment. It would be possible for Huawei to send a command to network equipment installed in another country instructing it to disrupt service. The UK, which established a monitoring center to review patches and updates from China to the UK for Huawei equipment, concluded that it could not guarantee that it would detect this kind of command. The risk is increased by China's 2017 national Intelligence Law, which makes it compulsory for all Chinese companies to comply with requests for assistance from the Ministry of State Security - there is no appeal. The 2017 law only codified existing practices and it raises concerns about the use of any Chinese technology which remains connected over the internet to its manufacturer in China.

The products of a Chinese company could be completely trustworthy, but a decision by the Chinese government could change overnight. In the context of China's increasingly aggressive global espionage campaign, which relies heavily on both human and cyber espionage, there are reasonable grounds for the distrust of Chinese products. The issue is not whether one trusts the Chinese company, but whether one trust the Chinese government.

No major telecommunications service provider wants to find itself dependent on Huawei. Even Chinese telecom companies will say privately that they do not wish to see Huawei dominate the market. Interviews with executives from these companies emphasize the need to preserve

[1] CSIS recently released a report on 5G supply chain issues: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf

supplier diversity. One European executive compared this to the market for commercial aircraft, where Boeing and Airbus must compete against each other. A Huawei-dominated market would mean higher prices and less innovation (since competition drives innovation).

Similarly, providing telecommunications equipment can provide advantages in the collection of communications intelligence. The poster child for this risk is the headquarters building of the African Union, which was built by China using Chinese technology. When the building was still new, its systems administrators noticed something strange. Every night at about 2:00 in the morning, there was a huge outflow of data from computers on the headquarters networks, even though the building was empty. On inspection, it was discovered that this data was going to Shanghai, where Chinese cyber espionage groups are located. The AU example is a warning. The increased risk of coercive disruption or espionage are the primary objections to relying on Chinese 5G technology.

A UK Alternative

The Chinese State, led by a single unchallengeable party, is not hesitant about using coercion, including explicit threats to cut trade, against those who oppose it. When Australia banned Huawei from selling 5G, China retaliated by blocking Australia's major exports to China for two weeks. When Canada detained Huawei's CFO at the request of the U.S., the Chinese retaliated by going around and arresting random Canadians in China for imaginary crimes. Those who question whether Huawei has close links to the Chinese government might ask why there was such a pronounced reaction when the CFO was detained. Many countries are afraid to ban Huawei because they fear Chinese retaliation and a few, including the UK and Germany, do not want to put their economic relations with China at risk.

One explanation for the recent UK announcement that it would allow Huawei into its 5G infrastructure, under certain limitations, is that senior levels of the British government, alarmed by the possibility of major economic damage from Brexit, hoped to allay this risk by pursuing both expanded trade with China and a free trade agreement with the U.S. The week of the UK announcement, a Ministerial-level British delegation flew to China to negotiate trade deals. Perhaps this was only coincidence, but we should help the UK realize why it will become increasingly difficult to accommodate China while maintaining close security ties with the U.S., and that what its former Prime Minister David Cameron called the "Golden Era" of cooperation with China is over.

A complete ban is the only way to eliminate this risk, but a ban appears so far to be politically unacceptable for the UK. The recent UK announcement that it would allow Huawei to supply the "edge" but not the "core" of 5G networks is an effort to mitigate the risk of using Huawei without imposing a complete ban. The UK says it will use four different techniques for 5G risk reduction.

First, Huawei technologies will not be allowed in sensitive areas such as around Whitehall. Second, Huawei technologies will be kept from the core but installed in the "Radio Access Network" that connect mobile devices (such as a phone) to the larger telecommunicate system (cell towers and base stations are visible examples of the RAN). There is some doubt that this

architectural solution will actually work. Finally, the UK would develop security standards for telecommunications equipment that would emphasize trusted suppliers and demonstrably trustworthy equipment (and internal reviews by GCHQ found Huawei to be the most "buggy" telecom gear). While there are strong objections to this partial ban, it is attractive to many European countries, including Germany, as it avoids a direct confrontation with China. Other countries are considering a similar approach.

A simplified portrayal of the UK "architectural" solution would divide 5G networks into four parts that range from the edge to the core of the network and the network "cloud." At the edge there are the devices, such as mobile phones or cars. These connect over a "Radio Access Network" (RAN), cell towers with some computing capability. The RAN connects user devices to the core network. The core uses specialized routers, switches, and other packet handling technologies to aggregate and manage billions of calls. Service providers are also moving towards using "software defined networks" (SDN) where much of the core processing is in the cloud. Both RAN and core connect back to the manufacturer, who has the ability to monitor traffic and manipulate software.

The fundamental question is whether there is a meaningful distinction between core and edge that can address security concerns. The UK proposal would allow Huawei to provide RAN but not core technologies. Access to the core delivers intelligence advantages (by providing access to bulk traffic), and some argue that access to the RAN, which uses its computing power to manage traffic in bulk, also provides an intelligence advantage. To further complicate the picture, initial deployments of 5G in many countries will be layered over existing 4G network infrastructures, whose technologies have often been provided by Huawei (as is the case in the UK and Germany).

China's 5G Push

Huawei seeks not only to supply the full range of technologies - edge devices, RAN, core infrastructures - but to dominate the standards processes for 5G. Chinese IT companies, helped by government subsidies, attempt to dominate global standards bodies. Representatives from China’s State-Owned Enterprises or other companies that receive government backing (like Huawei) now seek to shape the agenda and outcomes in standards groups for 5G and the Internet of Things.

China is politicizing the international standards process. Anecdotal reports from attendees at international standards meetings tell of greatly expanded Chinese participation. In looking at the membership of 3GPP, the 5G standards umbrella organization, the U.S. and China are tied for leadership when we look at the number of member companies and associations. Chinese companies must vote the party line, which is to support Chinese proposals even if they are technologically inferior. Last summer, the Chairman of Lenovo was forced to apologize publicly and promise never to vote again for a non-Chinese standard after Lenovo representatives voted in favor of a technologically superior American proposal instead of a Chinese proposal. This is not how the standards process is supposed to work, but China will flout norms to gain dominance. China was unable to dominate the first round of 5G standards discussions, but it will be back in force for further rounds. The U.S must find ways to work with Western partners to ensure the

standard process remains politically neutral and that American companies are not underrepresented.

If China wins the standards battle, it would also help ensure Huawei's dominance. Huawei also uses predatory pricing to drive competitors from the market. A European telecommunications executive said in an interview that Huawei offered a ninety percent discount over the market price in a recent competition and was "desperate" to get in the telecommunications "core" of his countries networks. Large discounts have been offered to Indian telecommunications firms (sometimes in the form of no-cost or low-cost loans) and an unpublished study by a European government found that Huawei routinely offered discounts of twenty to thirty percent over competitors' prices. Huawei can afford these discounts because of financial support from the Chinese government and this support is prompted by both mercantilist and intelligence motives. The effect has been to drive Western telecommunications firms from the business.

For telecommunications systems, there remain only five major producers. In order of market share, they are Ericsson, Huawei, Nokia, ZTE and Samsung. There are no American producers as the last, Lucent, went out of business more than a decade ago. However, U.S. component manufacturers dominate the 5G market, particularly for semiconductors. None of the five major suppliers could make 5G network equipment without Intel, Qualcomm, Xilinx and Cisco equipment. American technology remains essential for 5G mobile telecommunications. A Huawei executive, for example, has stated that only 30% of Huawei equipment uses Chinese technology. American companies have been strong performers in developing 5G technologies, but the United States and its allies face a fundamental challenge from China. The focus of competition is over 5G’s intellectual property, standards, and patents.

China is of course racing to end its dependence on the U.S. and will invest more than $100 billion over the next five years to build its own semiconductor industry, but for now and for the foreseeable future, it relies on U.S. technology. It is crucial that the U.S. develop supportive policies for research, education, and intellectual property protection to support its semiconductor industry, and push back against foreign efforts to use anti-trust or patent laws to hobble U.S. competition.

It's worth noting that while the U.S. is the unique supplier of the most advanced technologies necessary for 5G, many subcomponents come from Chinese firms. The positive expectations for China as an economic partner mean that there is a deeply intertwined global supply chain, with American, European and Japanese companies manufacturing in China, Chinese companies relying on US. technology, and U.S and European technology that may itself incorporate Japanese or Chinese components. Nor does every Chinese company create risk. This depends on what they make and whether their product connects back to China. It would be very difficult - and perhaps impossible - to bifurcate the global supply chain into "Chinese" and "Western." This complex, interconnected supply chain is a source of risk - the Chinese worry about it as well - and we need to develop policies and techniques other than a radical split to manage this risk.

Another set of objections to using Chinese technology for 5G relates to competitiveness and innovation. By reducing the market share of Western companies, unfair Chinese 5G competition also reduces the ability of these firms to fund research and development (R&D) by reducing their

revenue shares. Success in deploying 5G depends not just on supply chain security, but on the ability to innovate, to build the new "apps" that will take advantage of 5Gs potential. This is part of a broader technological competition. Technology and the capacity to create new technologies are the basis of information age power. 5G is the most salient example of a new kind of competition for global influence, along with other technologies like artificial intelligence or quantum computing, that will help determine a nation's economic competitiveness and military capability.

Next Steps for the U.S.

The United States is well-positioned to lead in 5G, but success and security require action by the Federal government. The United States does not need to copy China's government-centric model, but it does need to reorient its regulations, laws, and policies to compete in the 21st century. This requires a comprehensive strategy for managing risk with the next generation of network technologies. The elements of a strategy should include:

1. Closer intelligence, technology, and security partnerships with the countries that share the assessment of the risk of using Chinese network technologies and agree on the need to address it. The foundation for this partnership is the Five Eyes and the Nordic countries, Japan, and other nations in Europe and Asia that share our concerns.

2. Robust security standards for telecommunications equipment and supply chains (noting that some European customers of Huawei may try to dilute standards to ensure that Huawei has continued access to their markets). The Prague Principles and the draft principles releases by Germany's Federal Network Agency offer good starting points for this.

3. Foreign assistance funding to encourage developing countries not to buy Chinese 5G technology. We will not match Chinese subsidies, but we can reduce the financial burden of excluding Huawei.

4. Support for Western telecom infrastructure companies for research and development. This could involve the use of Cooperative Research and Development Agreements (CRADA) to subsidize R&D. This is a politically sensitive suggestion and support for foreign R&D should be accompanied by support for US research into the secure use of 5G and on the next generation of telecommunications equipment. The goal should be to preserve diversity in telecommunications technology suppliers so that we do not find ourselves dependent solely on suppliers in a hostile country.

5. Research on how to securely communicate over international networks that contain Huawei equipment, since many European, African and Middle Eastern companies already use Huawei and will adopt its 5G technologies.

6. A Federal strategy on telecom supply chain security that lays out U.S. policy, accompanied by significant investment in research and formal bans (either complete or partial) on the purchase and use of Huawei technology.

7. A reorientation of domestic policies to emphasize technological competitiveness. The U.S. no longer has the luxury of being unchallenged and the laissez-faire approach of the first two decades after the Cold War are no longer sustainable. This means not only expanding Federal support for research but looking at intellectual property law, anti-trust, taxation, and infrastructure investment to build technological and economic strength.

8. A long-term engagement strategy with China to bring its behavior into conformity with international norms for trade and security. China is not going away. It will always be powerful and the United States, working with its partners, must encourage and require change.

The United States cannot meet the 5G challenge on its own. When the United States successfully challenged Chinese policy in the past, it has been done in concert with nations who share our concerns. We may need to rethink partnerships in this new conflict. For example, Hungary, while a NATO member, sees Huawei as a strategic partner and is expanding its cooperation with China and Huawei. In contrast, Sweden, not a NATO member nor a treaty ally, is a strong partner in information age conflict. Many countries will find Huawei's highly subsidized prices attractive and dismiss U.S. concerns. Perhaps this could be one new measure of security partnership: a country that does not understand or ignores the risk of using Chinese 5G equipment should not be a close security partner.

The contours of the new global security landscape are still emerging but there are perhaps twenty countries in Europe and Asia who share the U.S. concerns. Many more do not. The battle for influence will be shaped not only by ideas, but by a country's investment decisions. China's overly centralized system should be a disadvantage, but in the near term, the U.S. failure to invest in public goods like basic research and infrastructure, or to spend efficiently in public goods like health care or defense, creates a disadvantage.

The U.S. is doing better than many public accounts suggest, but this will be a hard and close-run fight. The recent Prague Summit laid a good foundation for cooperative effort. Among our partners, there is no disagreement on the risk of using Chinese technology. Where there is disagreement is over how to manage this risk and how to implement agreed principles. Domestically, U.S. spectrum management policy has been effective in freeing up spectrum for 5G deployments. We do not need a nationalized 5G network. The U.S., however, faces a problem that China does not have in its plethora of state and local regulatory agencies. Beijing does not have to worry about "NIMBY."

We are at the start of a singular moment when computing power, mobile connectivity, and abundant data are restructuring economies. 5G technologies play a major role in this restructuring. The next internet will be a complex, dynamic environment where technological opportunities reshape commerce and markets in unexpected ways. 5G will be a central part of a nexus of new information technologies that will shape the future of the global economy. While the internet was created by the U.S. and has been led by American companies, if 5G leadership goes to China, it creates the opportunity for it to shape the future internet to its own advantage.

We are at the start of a long contest with China over whose rules and values will shape the world. This contest is made more complicated by the close economic ties between China and the West. China is a formidable competitor and its leaders are clear in their intentions to displace the U.S., which they see as in decline, and rebuild global rules and institutions to serve China's interests. The Belt-and-Road Initiative is part of this effort.

Respect for the rule of law is not, and this is a fundamental difference between the U.S. and China. Most countries would prefer a world ordered along the lines of Western principles, but the institutions created after 1945 are outdated, and polling data shows there is a growing public discontent with democratic governance as it is now structured (evidenced by the increase of populism and nationalist sentiment in many countries). China also has weaknesses, and is more fragile than its propaganda makes appear, but if China is unwilling to compromise and follow international norms, this will be a lengthy and difficult fight.

China has developed a competing model for innovation and investment that is well-funded and centrally directed. U.S. technological leadership is no longer undisputed. This is a much more competitive global environment where the U.S. needs to accelerate its efforts in policy and investment choices if it is to preserve its technological strengths and advantages. This is not a race the U.S can afford to ignore. Adopting the right policies and partnerships will play a crucial role. Policies that strengthen our own technology base, build strong cooperation with partners and allies, and maintain supplier diversity in telecommunications will ensure that the U.S. can manage the risk and reap the opportunities new technology will provide.

I thank the Committee for the opportunity to testify and look forward to your questions.