Statement before the Senate Committee on Commerce, Science and Transportation

"5G Supply Chain Security: Threats and Solutions"

A Testimony by:

James A. Lewis

Senior Vice President and Director, Technology Policy Program, CSIS

March 4, 2020

253 Russell Senate Office Building

Mr. Chairman, Ranking Member Cantwell, distinguished members of the Committee, thank you for the opportunity to testify. The fifth generation of telecommunications network technology is an important development and I hope my testimony can dispel some of the myths and offer a path forward for American prosperity and security.

We often hear that 5G is a race the U.S. cannot lose. It sounds dramatic, but I am not sure what it means. I am sure, however, that if there is a race, we are not losing. The U.S. is well positioned to take advantage of 5G technology, just as it did with 4G. The difference this time is we have real competition, a competitor who is well resourced, with a strong technology workforce, and a long record of unscrupulous behavior. We face a dynamic competitor in China, and there are things the U.S. can do to strengthen both its security and its technological leadership. Congress can play an important role in this.

The 5G issue has become politicized and this shapes reporting in unhelpful ways. Let's dispel some of the myths. First, the U.S. has not been rebuffed in Europe. In speaking to colleagues in the UK and Europe, there is broad agreement with the U.S. on the risks of using Huawei. The UK action is best seen as a partial ban on Huawei. The UK has blocked Huawei from two thirds of their network and from being used in sensitive areas around government and military installations. They and other European countries are committed to maintaining supplier diversity and avoiding Huawei dominance. The U.S. needs to find ways to benefit from these shared concerns to develop secure telecommunications networks.

Where there is disagreement is in how to manage risk. The U.S., Japan and Australia have banned Huawei technology in their networks. This is the only way to eliminate risk entirely. Those who advocate a partial ban argue that if properly implemented, it makes the risk of using Huawei manageable. Some European countries will copy the UK's decision. This provides the U.S. an opportunity to work with our allies to ensure that a partial ban reduces risk and there could be real advantages for the security of telecom networks and cybersecurity. The recently issued European Union 5G Toolbox provides a framework to guide policy in a way that, if implemented fully, would reduce China's use of telecom infrastructure for espionage and influence.

A full ban is the best outcome for security. It is not, in the judgment of some of our allies, the best outcome for their economies. Germany, for example, faces a dilemma. If it bans Huawei, the Chinese have explicitly threatened to retaliate again German auto exports, and China is Germany's largest market - China is playing hardball. German car companies have reportedly asked Chancellor Merkel not to ban Huawei. However, if Germany uses Huawei, China's intent is to use espionage to hollow out the German industry, and in particular the auto industry. If countries ultimately choose a partial ban, we will need to work with them to ensure that it is well implemented.

There is a larger debate over whether banning Huawei from the "core" of telecom networks and confining them to the "edge," such as the Radio Access Network (such as the cell tower that connects your phone to the network) will actually work. U.S. and Australian agencies say no, the UK and others (including some American tech companies) say yes. Frankly, the issue is moot. The UK has chosen a partial ban, others will follow them. It would be best for security if

countries adopted a full ban, but if they do not, the U.S. needs to help make the partial ban as effective as possible. There is concern about how Germany may implement a partial ban, but the way to persuade it and others to cooperate with the U.S. is not by using heavy-handed threats to cut intelligence sharing. All Europeans say this doesn't help our case and if we use a more deft diplomacy that focuses on winning European cooperation in the battle against Chinese espionage, we are more likely to be effective - the Europeans are already aware of the problems of doing business with China, having declared that China is a "Systemic Rival."

The root of the 5G problem is Chinese espionage and Chinese predatory economic practices. Our European and Asian partners have realized the extent of the Chinese espionage campaign against them. Countries near China are eager to cooperate, but there is an ambivalence in Europe. China is not a military threat to them and there is a reluctance to admit that the China market that Europe depends on comes with real economic risk. Europeans say they want "technological sovereignty," to be free of both China and the U.S., and they cite Snowden in an effort to show moral equivalence between the U.S. and China. Spying, illicit subsidies, and predatory pricing helped Huawei to drive western telecom manufactures from the market and other sectors of the European economy, such as aerospace and automobiles, are now at risk. Our task is to persuade European allies that it is better if the democracies stand together.

Spectrum for 5G is not an issue. The FCC and NTIA have done a god job at supporting 5G deployment. In talking to major telecommunications suppliers, they say it would be nice if the spectrum allocation process was faster and less expensive, but most say that it is working well to meet their needs for 5G. Spectrum decisions have not put the U.S. at a competitive disadvantage. The U.S. has one of the most flexible regulatory frameworks that permits operators to migrate to another technology in a wide range of bands. The United States is one of the first deploying in high bands but we are also seeing deployment in other bands. 5G will be deployed in the low, medium and high bands in the United States. U.S. spectrum allocations have created demand for tech companies to develop solutions that will allowed for 5G rapid deployment.

The complaint that the U.S. has mismanaged 5G spectrum allocation has led to a variety of strange proposals, such as a Federally-operated 5G network or a Federally-anointed spectrum monopoly. All of these are silly and one way to explain this is that government monopolies were a good economic policy in the 15th century but have not worked as well since then. The best 5G policies rely on market forces. If there is an issue in spectrum allocation, it is one the Committee if very familiar with, and that is the process for deciding when the U.S. Department of Defense should retain spectrum or when it should be reallocated for economic purposes. NTIA has done a good job of balancing security and economics, but in the new international competitions, emphasis on economic benefit might better serve U.S. national interests.

Standards are a battleground, but in 5G it is a battle where the U.S. is holding its own and retains the lead. This is not an easy fight. China is politicizing the standards process, flooding meeting with its experts, and is already leading in some bodies like the International Telephony Union (ITU). This is not the case for 3GPP, the standards body responsible for 5G. Its rules block efforts by one government to seize control and frankly, Chinese technology is in many cases inferior, making people reluctant to use it as a standard. Interviews with leading American 5G

companies show that the 3GPP standards process is still led by western companies, not China.

One crucial element for maintaining this advantage is to not see expanded export controls inadvertently damage the ability of American companies to participate in standards discussions. The U.S. Department of Commerce rules have created uncertainty. It is not good for U.S. companies to be sidelined in standards discussions by our own rules while Chinese companies are not.

Huawei is not the only supplier of 5G technology, nor is it the best equipment available. In fact a review by a European intelligence agency found Huawei was the most vulnerable to intelligence exploitation because of engineering and software problems. Huawei has undeniable strengths, and of them is its public relations department. Which has had considerable success in persuading people of the necessity of buying from Huawei as it is the "only" supplier of 5G technology which they must buy if they are not to "fall behind." Nokia and Ericsson offer 5G technology that is better and more secure, and Samsung is also establishing a presence in the 5G market.

The discussion of 5G has been shaped by the precedent of the internet, a technology that has reshaped corporate fortunes and national economies. People assume that 5G's economic effect will be the same, but this should come with a precautionary note. The Internet was created in the 1970s, commercialized in the 1990s, and began to rapidly reshape markets in the first decade of this century. Change is not instantaneous and the idea of falling behind unless you immediately install Huawei completely misrepresents the economics of digital economies.

5G (and Wi-Fi) will enable connections between sensors, the data they create, and powerful internet computing resources. Innovators can take advantage of this connection to create new services and applications. These will be new enterprise and industrial applications such as smart seaports, hospitals, or factories. Self-driving cars are part of this and 5G will speed their use.

5G could be the start of another round of innovation and growth similar to what we saw with the arrival of the internet, but for this to happen, 5G must be accompanied by "complementary investments." These include the invention of new products and services that make use of 5G networks, and the development of new business models and processes that can profit from 5G. The U.S. is strong here, but so is China. The need for complementary investments and innovations put the "race" metaphor in context, because what companies and countries do with 5G is more important than how quickly they deploy or how "much" 5G they have.

The doomsday argument is that because of slowness in American 5G deployment and the allocation of the wrong spectrum frequencies, U.S. inventors will not be able to come up with innovations that will take advantage of 5G. But the U.S. is not slow in 5G deployment and the spectrum issue is not a significant obstacle.

China does not lead in 5G. China will have more 5G phones or cell towers simply because it has more people, but this is the wrong thing to measure. American and Chinese deployments are roughly equivalent, with 57 cities in China that have 5G as opposed to 50 in the U.S. The key metrics are revenue and market share from the ability to use 5G to create economic growth.

Companies will use 5G services to be more efficient and innovative, and innovators will create new services and products that 5G can enable, but what ultimately counts is how people use 5G to make money.

One way to make money from 5G is to sell the technologies that enable it. This is where much of the public attention has focused because of the security risks. There are five companies that sell telecom network technologies - Ericsson, Huawei, Nokia, ZTE, and Samsung - but they sit atop multinational supply chains that are largely American, Japanese, and Chinese companies that make hardware and software components used by the five major suppliers.

Another way to make money is to sell 5G services - this is what telecom companies will do. The most "disruptive" way to make money, and the way that probably offers the best outcomes for economic growth, is to create applications (apps) that take advantage of 5G. Your smartphone is in effect a tiny computer. The change in how people use the internet, from desktops to smartphones and apps, helped American companies define the mobile internet and create the "app economy" that rapidly grew to be worth billions of dollars. 5G industrializes the app economy and expands it beyond games and other consumer programs, and this is where the opportunities for economic growth will appear. 5G will move the app economy from consumer applications (like Angry Birds) to industrial and enterprise applications.

It is true that Europe and China announced they intend to dominate 5G the way the U.S. dominates 4G, and American companies face new competition, but success depends on making products and offering services that appeal to the market. The most important market segment for 5G will be enterprise applications that allow companies to operate more efficiently and productively. Examples of these enterprise apps would include supply chain management systems, customer relationship management systems, and knowledge management systems. So far, the "killer app" for 5G has not been created, but U.S. companies are strong in these markets. It is not credible to expect the nimble, well-resourced, and entrepreneurial U.S. tech sector being squeezed out of a profitable market.

The policies that promote success in each of these areas are different. For technology producers, the focus on competition is over 5G's intellectual property, standards, and patents. Policy should encourage and support R&D, protect intellectual property, and ensure a level playing field in international standards and trade.

Each competitor has different plans for 5G. Germany intends to use 5G for industrial applications, part of its "Industry 4.0" plan, and its strong manufacturing sector may give it an advantage. 5G will play a central role in the development of smart and self-driving cars, and all countries with an automotive industry will compete in this. China already has valuable consumer apps (like WeChat), a strong developer base, and will also pursue industrial and enterprise applications. China had an advantage in developing apps for the internet of things since its companies are the source of many of these products. But Chinese companies also face trust issues, since any Chinese-made device that connects to the internet could be exploited by Chinese intelligence agencies.

Telecom technology used to be somewhat static, changing slowly. It relied on specialized

hardware, each generation providing incremental improvements over the prior in speed and reliability. New technologies like cloud computing were layered on top of established protocols and equipment. This is now changing. Telecommunications technology is now going through a transition similar to the effect of the commercial internet on computing three decades ago. This has major implications for security and business.

The move to an open, modular approach to telecom will change supply chain dynamics in ways that favor the U.S. (and Japan). The supply chain for telecom will depend on semiconductors, chipsets, and specialized software (including "open source" software), all areas where the U.S. has a substantial lead over China - in some cases there are no Chinese competitors. Estimates of how long this telecom transformation will take range from three years to a decade. The shift puts Huawei at a disadvantage. China will of course invest to catch up (accompanied by increased espionage), but money alone won't remedy China's lag in software and semiconductors.

The most visible aspect of this change is Open Radio Access Network Alliance, an industry group developing architectures and software that will enable virtualized networks (e.g. those based on software rather than hardware), commodity computers, and standardized interface.

The companies that make the modular components for new telecom technologies included both familiar names and new startups. Qualcomm, Intel and Samsung make chips. Microsoft (which has a huge 5G lab) writes operating system software. Cisco, Sienna, Xilinx, Nokia, Fujitsu, and NEC make other essential components, as do a number of new companies, such as Altiostar. These are all American, Japanese or Korean companies. In contrast, Huawei's strength in the new technologies is in RAN cell towers.

It is much easier to tell a story of gloom and peril, but it's not a good guide for law or policy. There are, however, steps we need as part of a comprehensive approach to 5G. The three most difficult challenges are rebuilding the sources of American technology leadership, effectively partnering with allies, and resisting China's efforts to use espionage and predatory trade practices to attain dominance. These are not unique to 5G and it is important to see 5G as only a part of a larger technological competition.

Some recommendations are things the Committee has heard many times, such as rebuilding the American tech workforce through investments in college education and spending more on R&D for the "hard sciences." It's worth noting that these steps would help with competing with China in the standards battle by expanding the tech and engineering workforce needed for the standards process.

An implementable suggestion is to restore the STEM scholarship programs established by the Eisenhower administration in reaction to our last technological security threat in the 1950s. This means paying students to study engineering, math, sciences, coding, and languages. The Chinese are not reluctant to spend money to build their tech workforce and is this is one of their greatest advantages over us.

The U.S. can safeguard the standard process not only by increasing the number of American participants, but by working with European and Japanese partners to ensure that standards bodies

remain open and equitable, and with governance structure that remains able to resist efforts to politicize or capture them.

A crucial element of maintaining a U.S. presence in standard bodies is to make clear that export control regulations do not prevent U.S. companies from participating in international standards discussions. The Commerce Department needs to immediately clarify that standards participation remains exempt from export regulations. This is a self-inflicted wound that the U.S. must avoid.

R&D funding for the development of industrial apps and the internet of things is important. While market forces will drive some of this, we can accelerate 5G deployment and the benefits to the U.S. economy by supporting additional research. DARPA has a program on 5G security. NSF and NIST have small programs in these areas, but they are dwarfed by what China spends. We cannot expect to maintain technological leadership when we are routinely outspent. An easy suggestion would be to double the funding now allocated to 5G and cybersecurity.

There has been some discussion of whether to help Nokia and Ericsson, the two European 5G equipment manufacturers, ranging from support for R&D to outright purchases of the companies. An initial and relatively uncontroversial step would be to find mechanisms to support R&D by these companies. No option is off the table and there is perennial talk that one of the companies will be bought or merged. In the next decade, Nokia and Ericsson face the challenge of adjusting their business models to accommodate changes in telecommunications, since the proprietary "stack" that they and Huawei make will be overtaken by technological change. In the near term, it is in our interest to ensure that they continue to operate profitably and can compete on equitable terms with Huawei. One approach would be to instruct DOD to develop Cooperative Research and Development Agreements (CRADA) with both companies, to fund their R&D.

Some recommendations may seem at first glance unrelated to 5G. 5G depends on semiconductors, and the U.S. is the leading source of supply. The Chinese government does not like this and intends to develop its own semiconductor industry to replace American firms both in China and in the global market. But to make chips, China needs to buy semiconductor manufacturing equipment (SME) which it cannot produce itself. The major sources of this SME are the U.S. and Japan, along with one or two European companies. One way to limit China's role in 5G is to limit exports of SME. Some of our allies have proposed augmenting existing controls to do this. We should develop a new SME export control regime with our Japanese and European partners, and Congress can help the Administration focus on this by mandating it, with timelines.

I hesitate to make recommendations on spectrum, since the process is working well enough and since any effort at reform raises powerful antibodies to block change. Congressional interest in seeing the allocation process further streamlined and in reducing the ability of a single agency to block reallocation would be helpful for the mobile network world we have entered.

We face a difficult challenge of managing the transition from the older model of telecommunications technology to the new, internet-based approach. Some say this transition will be here in three years, others say a decade, but the goal for now is to keep the two European

suppliers viable and technologically sound. To some extent this can be left to the market, the customers of these companies will encourage them to evolve, but the U.S. can assist by emphasizing this in decisions with the governments of Sweden and Finland.

Whether or not other nations follow the UK precedent of a partial ban, we and our security problem will continue to confront the challenge of how to communicate securely over networks with untrustworthy components. Finding a way to do this, and to help those countries that choose a partial ban make it as effective as possible, is a central strategic goal for the U.S. The Prague Principles for secure telecommunications networks produced last year are a starting point for this, and the U.S. can strengthen these principles at the upcoming second meeting, by aligning them with measure criteria for security. It is not enough to say that we should avoid a telecom "monoculture." There must be an explicit commitment to buy from multiple venders and to give preference to suppliers from democracies even if the price is higher.

Huawei is a symptom of a larger problem and 5G is a symptom of larger fears. We face, for the first time in decades, a powerful, unscrupulous, well-resourced opponent who has publicly declared their intent to displace us. We are not ready for this fight and do not have a strategy to respond to this challenge. It is likely that for some time we will be unable to develop such a strategy. This is not a reflection on American politics, messy as it can be. It reflects that we are in a different kind of competition. Increasing the defense budget will not help the U.S. win. This is a competition over markets and technology, things with which the foreign policy and defense establishment are still unfamiliar. Strategies that traverse the intersection of economics and security will not at first be easy for the U.S. to construct.

China has strengths - a determined Leninist leadership willing to spend on strategic goals (and even though the U.S. is twice as rich as China, we are being outspent), an immense domestic market, and a plan to shield this market from competition while using it as a base to dominate a range of industries, assisted by predatory trade practices and a massive economic espionage campaign. China has weaknesses as well - the heavy economic costs of a repressive regime, the inefficiencies of state capitalism, clumsy diplomacy and, above all, a fear by the Party leaders of their own people. China is not our technological peer but they are making immense efforts to change this.

The U.S. needs to act in response. We have seen some efforts in the last few years, but more needs to be done, including a revitalized science and technology base and a coordinated approach with our allies on how to respond to China's espionage, unfair trade practices, and efforts to reshape global rules to better accommodate authoritarianism.

To summarize; the problems often attributed to 5G in the U.S. are often overstated or wrong; there are things we can do to speed up deployment and reduce risk, but the larger issue is to how to deal with an increasingly hostile China in a new kind of non-military competition. Thank you for the opportunity to testify and I look forward to your questions.