Prepared Testimony
of
Michael R. Wessel
Before the
Subcommittee on National Security and Foreign Affairs
Made in the USA: Manufacturing Policy, the Defense Industrial Base, and U.S. National Security
September 22, 2010

Mr. Chairman, Ranking Member Flake and Members of the Committee. I want to thank you for providing me the opportunity to testify on this important topic. Your hearing today addresses critical questions that, unfortunately, have not been given adequate attention. I look forward to today's hearing and future efforts by your Subcommittee to help ensure the nation's security interests are being properly protected.

I am here today in my individual capacity and any views I express are my own. That being said, my views are informed by my service as a Commissioner on the US-China Economic and Security Review Commission (China Commission), my work with a variety of private sector entities, and my more than 20 years of service on the staff of former-Democratic Leader Richard Gephardt where, in addition to having served as his general counsel, I handled trade, economic and other policy matters.

While I am here as an individual, let me quickly highlight the work of the China Commission. The Commission is a bipartisan Congressionally appointed panel created in the wake of Congress' passage of Permanent Normal Trade Relations. Its purpose is to provide analysis and advice to Congress on the U.S.-China relationship and the challenges and opportunities that result. In addition to our hearings and research – both internal and prepared by outside parties – we deliver classified and unclassified annual reports to Congress on the major economic and security aspects of our relationship. I'm proud to say that in most of the past several years, we have issued unanimous reports by the six Democratic and six Republican Commissioners. As we have seen with this Committee and with this Congress, confronting our national and economic security interests can unite us.

Mr. Chairman, our national security interests have changed dramatically over the years. For four decades, our challenges were defined by the Cold War. We lived in a fairly polarized world where our energies were focused on stopping the spread of communism and deterring the former Soviet Union. With the fall of the Berlin Wall and the subsequent attacks on 9/11, the principal challenges to our national security now come from a variety of places and in a number of different ways. We must be prepared to confront existing and emerging threats that are changing rapidly.

But, as we prepare for new challenges, we must recognize that we also have to maintain our traditional capabilities. While cyberspace and the electronic spectrum are increasingly important to our national security interests, there will still be a need for a U.S. presence around the globe. The requirement for actual "boots on the ground" and "traditional" hardware will not disappear.

As new threats develop, some believe that the importance of the U.S. defense industrial base will diminish. Nothing could be further from the truth. Indeed, I believe that there is a vital need to recognize that "Made In the USA" may, in fact, be more important than it has ever been. As Rosie the Riveter was a symbol of America's ability to confront the enormous power of our enemies in World War II, we must have the capability – here at home – to confront any and all challenges in the future. We cannot rely on the tender sensibilities of others as we are ultimately responsible for the security of our citizenry and the protection of our interests here and abroad.

Unfortunately, the globalization of supply chains and the decimation of our manufacturing base have already put our interests at risk. We no longer have the domestic capacity to produce adequate stocks of ammunition to supply our troops and law enforcement. There are actually waiting lists to fill the orders of police departments here at home. At a hearing of the China Commission, we were told that there was no longer a domestic supplier for the propellant used in Hellfire missiles – the helicopter launched missiles our armed services use – and that we would have to rely on China for future supplies. We now have to rely on China for supplies of rare earth minerals. They control 90 percent of the world's supply yet they have subjected these vital products to export restrictions. These difficult-to-obtain elements are critical components in the magnets used in the guidance systems of our Joint Direct Attack Munitions (JDAMS). These are the "smart bombs" that have allowed us to precisely strike targets from vast distances, thereby keeping our troops out of harm's way.

This is not just a "China problem." Press reports identified Switzerland's refusal to provide critical parts for the JDAMS after the beginning of the Iraq war because of that country's opposition to U.S. actions. France refused to grant the U.S. "over-flight" rights for the bombing run on Libya. Turkey denied the U.S. military access to a northern invasion route in the run up to the Iraq War. While Turkey eventually relented with regard to the provision of supplies, it refused to allow transit rights to our combat forces. What would happen, on a broader and longer-term basis if other countries followed the lead of Switzerland, France or Turkey in limiting our supply of spare parts, basic componentry, or full weapons systems?

The risks to our national security run far deeper. The first salvos in our next conflict may be lobbed in bits, bytes and bots. Our defense capabilities increasingly rely on "informationalized" capabilities. The electronic spectrum is key to everything we do– from GPS guided smart bombs, to troops on the battlefield linked to Predator drones to the logistical support for our armed services carried over the Internet. High technology and telecommunications play a significant role ensuring our capabilities. All of these technologies must be part of a secure and reliable supply chain. The growing risks that result from too many of our companies – and our military – abandoning the "Made In America" logo have increased dramatically.

Today, a growing percentage of the high technology equipment our military uses and which controls our nation's critical infrastructure is produced offshore – more and more of it in China. Many of our leading manufacturers display their company logos on the outside of the box, but little inside may be produced here (and, of course, the label may not be either).

You have read the stories of network intrusions apparently executed by Chinese entities. They have exfiltrated terabytes of data from our government and our government contractors. In their electronic reconnaissance efforts, they are attempting to map out the various ways we depend on the Internet for such essentials as power generation and emergency response. Just as any potential adversary might wish to determine how to deploy an offensive cyber strategy, in a possible conflict.

China is a strategic competitor. But, due to the lack of transparency in their system, what other intentions they may have are unknown. Admiral Mullen, in a speech at the Asia Society in June of this year said:

> *"Every nation has a right to defend itself and to spend as it sees fit for that purpose. But a gap as wide as what seems to be forming between China's stated intent and its military programs leaves me more than curious about the end result. Indeed, I have moved from being curious to being genuinely concerned."*

The role of the information spectrum in their plans was addressed in DOD's 2010 report, Military and Security Development Involving the People's Republic of China:

> *"An essential element, if not a fundamental prerequisite, of China's emerging antiaccess/area-denial regime is the ability to control and dominate the information spectrum in all dimensions of the modern battlespace. PLA authors often cite the need in modern warfare to control information, sometimes termed "information blockade" or "information dominance," and to seize the initiative and gain an information advantage in the early phases of a campaign to achieve air and sea superiority. China is improving information and operational security to protect its own information structures, and is also developing electronic and information warfare capabilities, including denial and deception, to defeat those of its adversaries. China's "information blockade" likely envisions employment of military and non-military instruments of state power across the battlespace, including in cyberspace and outer space. China's investments in advanced electronic warfare systems, counter-space weapons, and computer network operations— combined with more traditional forms of control historically associated with the PLA and CCP systems, such as propaganda and denial through opacity, reflect the emphasis and priority China's leaders place on building capability for information advantage."*

As the U.S. has outsourced and offshored its production of technology equipment we are increasing our security risks. The ability of the Chinese to alter code, to alter hardware to include electronic back doors, and to embed malicious code and other capabilities in our network are just some of the many risks. By outsourcing so much of our critical electronic componentry, we aren't just letting the fox guard the henhouse, we are inviting the fox to the dinner table.

This is not an academic issue. Some in the government are asleep at the switch.

Several years ago, I was reading the Washington Post business section and came across a small item reporting that the State Department had put in an order for about 15,000 computers and, via CDW, Lenovo, a Chinese state-invested enterprise, had won the contract. The contract was for computers to be placed on both classified and unclassified systems. As you may know, computers placed on classified

systems are configured differently and it would have been clear to the Chinese which computers would be carrying that data. The opportunity to monitor traffic, exfiltrate data or engage in "zero day" activities, for example, was clear.

Working with then-Chairman Frank Wolf, colleagues on the Commission and I raised the issue with procurement experts in the government who hadn't even thought about the matter. They were unaware of Lenovo's recent purchase of IBM's PC division, despite the fact that it had been subject to review by the Committee on Foreign Investment in the United States (CFIUS). Ultimately, the State Department agreed to change its procurement to ensure the security of its system. Flaws in procurement regulations and processes were clear and promises were made about the need for reforms. To date, I am unaware that sufficient reforms have been made. Indeed, one government entity that I am aware of, that shall go unnamed, recently had to seek a specific clause in a contract with a previously-cleared government contractor to ensure that equipment by the Chinese state-owned telecommunications firm Huawei was excluded from its system. Despite ongoing and increasing concerns about Huawei's activities – including, for example, a recent letter by eight Republican Senators questioning the provision of that company's equipment to Sprint-Nextel, the Chinese technology giant continues to supply telecommunications equipment across the country for networks that could carry U.S. government traffic.

The risks from the globalization of supply chains in the technology area are clear. An increasingly informationalized military and our critical infrastructure – including our nation's financial sector, which is completely dependent on computers and the Internet, are vulnerable. These risks are growing and little is being done about it. Only recently, a Washington Post headline summed up the problem: "U.S. cyber-security strategy yet to solidify".

These are just a few examples of the risks to our security interests that result from the hollowing out of our manufacturing base. And, quite frankly, it appears that the Department of Defense does not have a good handle on actually what's happening to our supply chains. In research done for the US-China Commission, we identified significant problems in identifying lapses in knowledge throughout military supply chains, especially beyond the first and second tiers. Finding information below Tier II suppliers is extremely difficult to obtain to actually assess what risks might exist. It may be because the information is too hard to obtain with the multitude of weapons systems, suppliers and component parts. But, it could also be a function of simply not wanting to know.

The problems associated with the hollowing out of our manufacturing base run deeper. As manufacturing capabilities move offshore, the basic skills of our workers are put at risk. Highly complex industrial machinery – five axis machine tools, for example – take substantial training to run. Nuclear-qualified welders, to assist in the production of Navy ships, for example, require years and years of training. The skills of such workers are too often taken for granted. Industrial processes have changed dramatically over the years; when you go into today's plants, you're just as likely to see a worker seated at a computer terminal as someone driving a forklift.

And, the decimation of our manufacturing base has an enormous impact on the strength of our economy. Today's economic problems, in part, are the result of an over reliance on financial services, and the blatant neglect of our "productive sector." The strength of our country is not simply measured in terms of the number of missiles we have, the planes we can launch, but is also a function of our economic success. American "power" is multifaceted but Made In America is a critical component of our ability to succeed.

Mr. Chairman. The above is just a quick summary of some of the risks to our national security interests resulting from the decline in our manufacturing and defense industrial base and Made In America. The question is, what do we do about it?

There is no proverbial "silver bullet." Indeed, the decline of our manufacturing base, the outsourcing and offshoring of production, the globalization of the economy have taken place over many, many years and will be difficult to remedy. In addition, the pace of change has accelerated and the problems have been severely aggravated by the economic meltdown our nation faced and is still grappling with.

But, that does not mean that there aren't a number of steps that can, and must, be taken to help revitalize our manufacturing and defense industrial base – broadly defined. Restoring Made In America as a fundamental tenet of our policies, within the scope of our international commitments, is vital.

Trade: For far too long trade policy has been seen as a separate "in-box" on the President's desk--one that has often been pushed to the side. Our nation's trade officials, until only recently, looked at enforcement as protectionism rather than as self-defense. We need to update and reform our nation's trade policies to make them results-oriented. Too many other nations break the rules, on a consistent basis, but we do little about it. We cannot afford to look the other way when our rights, and the commitments that our trading partners have made, are violated.

The failure to deal with China's manipulation of its currency is a perfect example of this. Most major economists have pointed out that China's currency manipulation amounts to as much as a 40% subsidy for their products coming to the U.S. and a 40% tax on our goods going there. How can an American manufacturer compete against those margins? And, the impact of China's currency manipulation is on top of its subsidies and other predatory practices. More than 50% of China's exports to the U.S. come from foreign-invested enterprises: Companies that have moved to China for a variety of reasons, including the subsidy that results from the manipulation of the Chinese currency.

And, as I noted earlier in my testimony, this shift in production poses risks to our national security. But, it is important to also recognize that, by failing to address China's currency manipulation, we are also helping to fund China's buildup in advanced weaponry. With $2.5 trillion in foreign currency reserves – the vast bulk of which are in dollar-denominated assets – the communist leadership has the additional resources to buy high tech weaponry from other countries, to fund the expansion and development of its own defense industrial base, and to help fund the sale of weapons to other nations,

many of which engage in activities adverse to our interests. And, this shift in production supports China's lock on power that allows the government to trample on human rights, freedom and democracy.

Procurement: The U.S. Government has substantial leverage in terms of its procurement dollars to support the revitalization of our manufacturing sector and defense industrial base. There are a number of steps that must be taken to ensure that U.S. taxpayer dollars are used to promote, and not undermine, their security interests.

The first step is for a more aggressive assessment of where our defense dollars are actually going and how the globalization of supply chains may threaten our interests. Clearly, in this time of rising federal budget deficits, we need to ensure that our defense dollars are deployed in the most cost-effective manner. But, at some point, there is a tradeoff between cost and security. After the fall of the Berlin Wall, there was an aggressive move to a procurement strategy based on Commercial Off The Shelf (COTS) contracting. This shift from "mil-spec" procurement to buying items on the open market allowed for cost savings and an ability to buy 1st generation technology, rather than long-lead time items that often were outdated when they were finally placed in service. But, by moving to this new system, the Defense Department opened itself up to new risks, some of which are only now becoming clear.

Earlier this summer, Senators Tom Carper and Sherrod Brown wrote a letter to Defense Undersecretary Ashton Carter, about the need for stronger policies to address the problem of counterfeit parts in defense supply chains. Their important effort needs to be supplemented by an assessment of procurement policies and an examination of supply chains to determine where, in fact, the components and parts for our military, first responders, and our critical infrastructure actually come from. Do the Department of Defense, the Department of Homeland Security and other responsible agencies even know what the risks are for the proliferation of foreign-sourced components?

The telecommunications infrastructure of our nation is vital to our security. Yet, procurement policies of our government fail to adequately protect our interests in this vital area. Components from foreign suppliers whom security officials have identified as potentially harmful are making their way onto our systems. In addition to monitoring the major telecommunication systems, the Government Services Administration needs to assess its contracting rules to ensure that prime contractors are not using questionable components or services on their networks.

This concern is evidenced by the letter that Representatives Shea Porter, Forbes, Wolf and others sent to the Director of National Intelligence recently asking him to assess the risks and vulnerabilities to our defense and intelligence interests and critical infrastructure from the increasing globalization of supply chains and provision of services. This is an important request that needs to be carefully reviewed by this Committee and the Congress.

And, as noted earlier, Americans want to know that their tax dollars are being used to put their fellow citizens to work, whenever possible. Buy America policies are consistent with our international commitments but, all-too-often, policymakers seek to avoid the requirements. These policies should be

aggressively pursued as part of our procurement efforts not only to help revitalize our manufacturing and defense industrial base but to advance our security interests.

Research and Development Policies: We need to do a better job of focusing our tax and economic policies on revitalizing our nation's manufacturing and defense industrial base. Often, our policies are developed based on broad theoretical approaches rather than what common sense might dictate. Take for example, the recent push to reauthorize the research and development tax credit. Clearly, there are a variety of reasons to extend the credit and provide more confidence to our companies that the R&D credit will exist in the future, allowing them to make long-term plans for the investments. But, simply focusing our policies on preserving the research here, without regard to where the ultimate manufacturing is to be done, might actually undermine our security in the long run. We should extend the R&D credit to first stage deployment in domestic facilities. Testing the R&D on the shop floor would more likely result in the products produced with taxpayer-subsidized research actually being made here at home. At any time, but certainly at this time in our economic history, we need to stimulate the expansion of new production in America.

As well, we need to examine what the migration overseas of American R&D and production by some of our companies is doing to undermine our manufacturing and defense industrial base here. We need to consider that this may actually be advancing the capabilities of potential adversaries. More and more of our firms are moving production facilities and R&D facilities to China and elsewhere around the globe. We need to better understand the implications.

For example, it's clear that the operations of international commercial aerospace firms have helped advance the ability of the Chinese to produce both commercial and military equipment. China is moving quickly to produce a regional commercial jet (ARJ-21) and a wider body airframe (C919). The operations of international aerospace firms have assisted the Chinese in developing their civilian sector, through platform integration, for example. But, this help has also resulted in the "leakage" of other technologies that has assisted the Chinese in the development of an increasingly sophisticated military industrial base. The resulting risks need to be more seriously assessed.

Mr. Chairman. Members of the Committee. The above are just a few recommendations that could be considered by the Committee. Despite the length of my testimony, I have only begun to touch on these issues. I would welcome the opportunity to work with you and your staffs as you continue your important work.

Thank you.

###