CHINA'S PURSUIT OF NEXT FRONTIER TECH: COMPUTING, ROBOTICS, AND BIOTECHNOLOGY

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED FIFTEENTH CONGRESS
FIRST SESSION

THURSDAY, MARCH 16, 2017

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2017

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Public Law No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Public Law No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); as amended by Public Law No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Division J of the "Consolidated Appropriations Act, 2008," Public Law Nol. 110-161 (December 26, 2007) (regarding responsibilities of the Commission, and changing the Annual Report due date from June to December); as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291 (December 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter is available at www.uscc.gov.

April 12, 2017

The Honorable Orrin Hatch
President Pro Tempore of the Senate, Washington, DC 20510
The Honorable Paul Ryan
Speaker of the House of Representatives, Washington, DC 20515

DEAR SENATOR HATCH AND SPEAKER RYAN:

We are pleased to transmit the record of our March 16, 2017 public hearing on "China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology." The Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106-398 (as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 § 1259b, Pub. L. No. 113-291) provides the basis for this hearing.

At the hearing, the Commissioners heard from the following witnesses: Addison Snell, Chief Executive Officer, Intersect360 Research; Mark Brinda, Partner, Bain and Company; John Costello, Senior Analyst for Cyber and East Asia, Flashpoint; Henrik I. Christensen, Director, Contextual Robotics Institute and Professor of Computer Science, University of California, San Diego; Jonathan Ray, Associate Deputy Director, Defense Group, Inc.; Patrick J. Sinko, Associate Vice President for Research and Distinguished Professor of Pharmaceutics and Drug Delivery, Rutgers University; Ben Shobert, Founder and Managing Director, Rubicon Strategy Group and Senior Associate for International Health, National Bureau of Asian Research; Kenneth A. Oye, Professor of Political Science and Data Systems and Society and Director, Program on Emerging Technologies, Massachusetts Institute of Technology; and Edward H. You, Supervisory Special Agent, Biological Countermeasures Unit, Weapons of Mass Destruction Directorate, Federal Bureau of Investigation. The hearing covered China's pursuit of critical capabilities in computing, robotics, and biotechnology, which will help advance its technological and military development. It specifically examined what steps the Chinese government has taken to develop its own technological leaders and reduce its dependence on foreign technology, compared U.S. and Chinese technological leadership in these sectors, and considered the broader implications of these policies for U.S. economic and national security interests.

We note that the full transcript of the hearing will be posted to the Commission's website when completed. The prepared statements and supporting documents submitted by the participants are now posted on the Commission's website at www.uscc.gov. Members and the staff of the Commission are available to provide more detailed briefings. We hope these materials will be helpful to the Congress as it continues its assessment of U.S.-China relations and their impact on U.S. security.

The Commission will examine in greater depth these issues, and the other issues enumerated in its statutory mandate, in its 2017 Annual Report that will be submitted to Congress in November 2017. Should you have any questions regarding this hearing or any other issue related to China, please do not hesitate to have your staff contact our Congressional Liaison, Leslie Tisdale, at 202-624-1496 or ltisdale@uscc.gov.

Sincerely yours,

Carolyn Bartholomew	Hon. Dennis C. Shea
Chairman	*Vice Chairman*

cc: Members of Congress and Congressional Staff

CONTENTS

THURSDAY, MARCH 16, 2017

Panel I: Computing

Panel II: Industrial and Military Robotics

Panel III: Biotechnology

CHINA'S PURSUIT OF NEXT FRONTIER TECH: COMPUTING, ROBOTICS, AND BIOTECHNOLOGY

THURSDAY, MARCH 16, 2017

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 419 of Dirksen Senate Building, Washington, D.C. at 9:30 a.m., Commissioners Katherine C. Tobin and Daniel M. Slane (Hearing Co-Chairs), presiding.

OPENING STATEMENT OF COMMISSIONER KATHERINE C. TOBIN HEARING CO-CHAIR

HEARING CO-CHAIR TOBIN: Good morning. Good morning to those here and to those who are watching the webcast. Welcome to the third hearing of the U.S.-China Economic and Security Review Commission's 2017 Annual Report cycle. I want to thank our witnesses for joining us here today and for the time they have put into their excellent written testimony.

I would also like to thank the Senate Committee on Foreign Relations and its staff for helping to secure this hearing room.

Today's hearing will assess China's efforts to become a technological leader in three emerging sectors: computing, robotics and biotechnology. Globally, advancements in these sectors are creating millions of high-paying, high-skill jobs and spurring the creation of entire new industries, such as data analytics. Many of these technologies have dual commercial and military applications and are important drivers of U.S. economic growth and technological and military superiority.

The Chinese government is utilizing preferential support for domestic firms, localization targets and high market access barriers to build domestic capacity and eventually replace foreign technology and products with domestic technology and production, first at home, then abroad.

These policies are slowly closing market opportunities for U.S. and other foreign firms in China and creating new Chinese competitors that will be able to challenge U.S. companies in the United States and in third-country markets with potential negative impacts on U.S. employment, productivity, and innovation.

Through these policies, China is rapidly closing its technological gap. For example, access to the most advanced computing capabilities has become indispensable for researchers, companies and governments, and provides a competitive edge in technological and scientific innovation and research.

China in the last decade has rapidly expanded its high-performance computing capabilities, challenging the U.S. leadership. It now has the world's two fastest supercomputers and is tied with the United States for the number of supercomputers. In addition, China is expected to beat the United States in rolling out an exascale computer, which would be ten times faster than the world's current leading supercomputer.

China is seeking to replicate its computing success in biotechnology and robotics.

As our Congress considers new legislation and appropriations, it's critical to examine closely how the Chinese government is developing its own technological leaders and to consider what role the United States government should play in ensuring the U.S. maintains its technological edge, thereby keeping high-paying jobs and research and development centers in these sectors in the United States.

I will now turn the floor to my co-chair, Commissioner Slane, for his opening remarks.

PREPARED STATEMENT OF COMMISSIONER KATHERINE C. TOBIN HEARING CO-CHAIR

Hearing on "China's Pursuit of Next Frontier Tech: Computing, Robotics, And Biotechnology"

Opening Statement of Commissioner Katherine C. Tobin
March 16, 2017
Washington, DC

Good morning, and welcome to the third hearing of the U.S.-China Economic and Security Review Commission's 2017 Annual Report cycle. I want to thank our witnesses for being here today, and for the time they have put into their excellent written testimony. I would also like to thank the Senate Committee on Foreign Relations and its staff for helping to secure our hearing room.

Today's hearing will assess China's efforts to become a technological leader in three emerging sectors: computing, robotics, and biotechnology. Globally, advancements in these sectors are creating millions of high-paying, high-skill jobs and spurring the creation of entire new industries such as data analytics. Many of these technologies have dual commercial and military applications and are important drivers of the U.S. economic growth and technological and military superiority.

The Chinese government is utilizing preferential support for domestic firms, localization targets, and high market access barriers to build domestic capacity and eventually replace foreign technology and products with domestic technology and production first at home then abroad. These policies are slowly closing market opportunities for U.S. and other foreign firms in China, and creating new Chinese competitors that will be able to challenge U.S. companies in the United States and in third country markets, with potential negative impacts on U.S. employment, productivity, and innovation.

Through these policies, China is rapidly closing its technological gap. For example, access to the most advanced computing capabilities has become indispensable for researchers, companies, and governments, and provides a competitive edge in technological and scientific innovation and research. In the last decade, China has rapidly expanded its high-performance computing capabilities, challenging U.S. leadership. China now has the world's two fastest supercomputers and is tied with the United States for the number of supercomputers. In addition, China is expected to beat the United States in rolling out an exascale computer, which would be 10 times faster than the world's current leading supercomputer. China is seeking to replicate its computing success in biotechnology and robotics.

As our Congress considers new legislation and appropriations, it is critical to closely examine how the Chinese government is developing its own technological leaders and to consider what role the U.S. government should play in ensuring the United States maintains its technological edge, thereby keeping high-paying jobs and research and development centers in these sectors in the United States.

I will now turn the floor to my co-chair, Commissioner Slane, for his opening remarks.

OPENING STATEMENT OF COMMISSIONER DANIEL M. SLANE
HEARING CO-CHAIR

HEARING CO-CHAIR SLANE: Thank you, Commissioner Tobin, and welcome to our panelists and guests today. Today's hearing comes at an opportune time. China is determined to reduce its dependence on foreign technology and create its own technological leaders through higher market access barriers for foreign firms and overseas acquisitions.

But while China is aggressively closing the technology gap, China's future dominance in these sections is not a foregone conclusion.

I wanted to express our appreciation to Katherine Koleski and our great staff for all their help in putting this hearing together and thank our panelists for coming today.

PREPARED STATEMENT OF COMMISSIONER DANIEL M. SLANE
HEARING CO-CHAIR

Hearing on "China's Pursuit of Next Frontier Tech: Computing, Robotics, And Biotechnology"

Opening Statement of Commissioner Daniel M. Slane
March 16, 2017
Washington, DC

Thank you, Commissioner Tobin, and welcome to our panelists and guests. Today's hearing comes at an opportune time. China is determined to reduce its dependence on foreign technology and create its own technological leaders through higher market access barriers for foreign firms and overseas acquisitions.

But while China is aggressively closing the technological gap, China's future dominance in these sectors is not a foregone conclusion.

Our new administration is in the process of formulating its policies toward China, creating opportunities for a fresh approach to resolving long-standing issues over China's industrial policies and U.S. market access in China. In addition, the United States remains home to the world's leading experts, research, and technological breakthroughs in these sectors and if provided the right support, the U.S. can remain at the forefront.

Before we proceed, I would like to remind you that testimonies and transcript from today's hearing will be posted on our website, www.uscc.gov. You'll find a number of other resources there, including our Annual Reports, staff papers, and links to important news stories about China and U.S.-China relations. And please mark your calendars for the Commission's next hearing, "Hotspots along China's Maritime Periphery," which will take place on April 13th.

PANEL I INTRODUCTION BY COMMISSIONER KATHERINE C. TOBIN

HEARING CO-CHAIR TOBIN: Now, I would like to introduce our first panel, which is focused on computing. This panel will assess China's efforts to develop high-performance computing, cloud computing, and the next generation of computing, such as quantum computing and its related information services.

The panel will also examine how China's policies affect U.S. companies' market access in China and the broader implications of China's policies for U.S. economic and national security interests.

We will hear first from Addison Snell. Mr. Snell is the Chief Executive Officer of Intersect360 Research, where he provides market information, analysis and consulting for global high-performance computing and hyperscale industries.

He previously worked as a high-performance computing industry analyst for IDC and was a marketing leader and spokesperson for SGI's supercomputing products and strategy. In 2010, Mr. Snell was named one of the "People to Watch" by HPCwire.

Next, we have Mark Brinda. Mr. Brinda is a partner in the New York office of Bain & Company where he splits his time between Bain's Technology, Media and Telecom practice and its Private Equity practice.

Prior to Bain, Mark was an analyst with ABN Amro in San Francisco. There he worked in the Technology Investment Banking Group on a variety of key transactions. He holds an MBA from the University of Chicago's Graduate School of Business and a BA from New York University, where he earned dual degrees in economics and philosophy.

Finally, we have John Costello. Mr. Costello is a senior analyst for cyber and East Asia at the business risk intelligence firm Flashpoint.

Mr. Costello formerly served as a New American Congressional Innovation Fellow with the Republican staff of the House Oversight and Government Reform IT Subcommittee. He's also worked as an analyst at Defense Group Inc's Center for Intelligence Research and Analysis.

John recently co-authored a chapter on Chinese information warfare in the edited volume China's Evolving Military Strategy.

Gentlemen, please keep your remarks to seven minutes so we'll have sufficient time for questions and answers, and, Mr. Snell, we'll begin with you. Thank you.

OPENING STATEMENT OF ADDISON SNELL
CHIEF EXECUTIVE OFFICER, INTERSECT360 RESEARCH

MR. SNELL: Thank you, commissioners.

High-performance computing, or HPC, is a vital tool for innovation, in scientific research, in industries such as manufacturing, oil exploration, pharmaceuticals, chemical engineering and finance, and, of course, in national security, including military intelligence, homeland security and cybersecurity.

Traditionally, the United States has been the dominant world leader in HPC, and today the U.S. still leads both on the supply side with technology vendors like Intel, HPE, Dell, IBM, Cray and others, and also on the demand side with nearly half the worldwide consumption of HPC technologies by revenue.

However, at the top of the supercomputing market, there has been a new dynamic signaling a shift. For the past four years, the most powerful supercomputers in the world have been installed at national research centers in China, as ranked by the semiannual Top500 list. At present, the most powerful supercomputer is the Sunway TaihuLight system in Wuxi, with a benchmarked performance of 93 petaflops, which is 93 quadrillion, or 93 million billion, calculations per second.

The second most powerful is the Tienhe-2 system at Guangzhou, with a benchmarked performance of 34 petaflops. After that, the next three are at U.S. Department of Energy labs, the Titan system at Oak Ridge, the Sequoia system at Lawrence Livermore, and the Cori system at Lawrence Berkeley, all benchmarked between 14 and 18 petaflops.

This is the most visible of several market indicators and public declarations that China has embarked on a strategy of becoming the world leader in high-performance computing. This intention should not be dismissed. The timing of this move comes against an industry backdrop of change. We're now seeing a shift in how the next generations of HPC systems will be built, based on fundamental changes in underlying processing technologies.

These paradigmatic shifts in supercomputing architecture have occurred before. In 1996, for example, the ASCI Red system at Sandia National Labs was the first to reach a teraflop, which was a trillion calculations per second. But that was also the first major supercomputer with a clustered architecture approach, assembling supercomputers as networks of industry-standard servers.

Over the next ten years, clusters would slowly emerge as the new dominant model for HPC. These shifts are not easy. It's not as simple as building a faster supercomputer. When you change the hardware approach, you also have to change the software approach, as well as how you manage the system. It was the new software model that took years to percolate through the industry.

That's where the industry sits today as we approach exaflops, which will be quintillions of operations per second, or if you prefer, that's billion billions or million-million-millions, needing not only to build the hardware system but also revisit topics like software and system management due to changes, underlying changes in the processing technologies, and a proliferation of specialized options.

In this vein, the Chinese investments are even more interesting. The Sunway TaihuLight system was essentially built, not bought. It was an internal investment at the Chinese national supercomputing centers using almost entirely indigenous technologies to China. The architecture was co-designed with scientific researchers who have already begun some programming work on the new system.

A new paradigm gives the opportunity for new leaders to emerge. Consider as a metaphor the transition of mobile phones. A country without any kind of investment in land lines could suddenly leap ahead with a well-timed investment in towers. We expect China to be able to field an exaflop system--that's back to that quintillion number we were talking about--as early as late 2019. After that, Japan is likely to deploy an exaflop system in late 2020 or 2021.

The U.S. plan had been to deploy two exascale systems in roughly 2023--one based on Intel processing architecture and one based on IBM POWER architecture with acceleration from graphics processing units from NVIDIA--justifying the lag behind other countries by discussing exascale over exaflops, which emphasize parallel advancements in areas like application programming and system management. A newly ratified addendum to the Exascale Computing Project in the United States seeks an additional earlier machine based on a so-called "novel architecture" in 2021, still behind China and perhaps Japan.

The two areas of greatest concern in the path to exascale are software and skills. In addition to the ongoing commitment to the Exascale Computing Project under DOE, we have the following recommendations, as reflected in our provided statement:

One, we recommend national initiatives in low-level software tools and programming models together with stakeholders in industry and academia.

Two, we recommend government-funded partnerships between industry and academia.

And three, we recommend ongoing pursuit of next-generation technologies.

Regardless of these recommendations, the HPC market will continue, powering new innovations and ideas around the world. Supercomputers today are close to a million times more powerful than they were 20 years ago. In another 20 years, they could be a million times more powerful still. The leaders in supercomputing will be the ones that do not rest on their achievements but rather continue to chase the next challenge over each new horizon.

Thank you.

PREPARED STATEMENT OF ADDISON SNELL
CHIEF EXECUTIVE OFFICER, INTERSECT360 RESEARCH

"China's Pursuit of Next Frontier Tech: Computing, Robotics, And Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

EXECUTIVE SUMMARY

For its hearing on "China's Pursuit of Next Frontier Tech," the U.S.-China Economic & Security Review Commission (USCC) is seeking testimony on the current and potential future state of supercomputing innovation worldwide, with an emphasis on China's position on the global stage relative to the U.S. Addison Snell, CEO of Intersect360 Research, provides this written testimony in answer to USCC's questions for the hearing. Mr. Snell will also provide oral testimony to answer additional questions at the hearing on March 16, 2017. Information about Mr. Snell, Intersect360 Research, and the questions asked are in the Appendices of this report. A transcript of the oral testimony will be made available at the USCC's website, www.uscc.gov.

In this statement, we give an overview of the high performance computing (HPC) industry, including analysis of hardware, software, and industry trends. Where relevant, market data from Intersect360 Research is included, particularly for the analysis of significant HPC market segmentations. In the next section, we give a country-level analysis of national supercomputing strategies and programs, for the U.S., China, and other significant countries. In the closing section we give our analysis, conclusions, and recommendations.

While the U.S. still leads by far in the most straightforward market share metrics of production (vendors, supply-side) and consumption (buyers, demand-side), industry indicators show the U.S. is falling behind in the leading edge of advancement. Chinese leadership has apparently recognized the relationship between HPC and economic growth and has set forth on a program to drive the country into a leadership position. The best response to this new challenge is to continue if not increase national support for HPC at all levels.

National supercomputing efforts are essential to motivating investment at the high end. From that point, U.S. companies excel at seizing opportunities to drive markets forward. Against these strengths, the top limitations to Exascale deployments are software and skills. If we do build a system, how will we use it? A key feature of the Exascale Computing Program is its emphasis on co-design, finding end-user stakeholders to collaborate on the design of next-generation supercomputing technologies, bolstered by government funding. We recommend:

- *National initiatives in low-level software tools and programming models, together with stakeholders in industry and academia.*
- *Government-funded partnerships between industry and academia.*
- *Ongoing pursuit of next-generation technologies.*

Regardless of these recommendations, the HPC market will continue, powering new innovations and ideas around the world. Supercomputers today are close to a million times more powerful now than they were 20 years ago. In another 20 years, they could be a million times more powerful still. The leaders in supercomputing will be the ones that do not rest on their achievements, but rather continue to chase the next challenge over each new horizon.

STATE OF THE HIGH PERFORMANCE COMPUTING INDUSTRY

High performance computing (HPC) is the use of computational servers and supercomputers, together with their attendant storage, networking, and software components, for the modeling and simulation of complex phenomena. As such, HPC is a critical segment of the information technology (IT) sector, powering innovation and scientific discovery in a wide range of disciplines across industry, public-sector research, and national defense. From clusters of a few servers to the world's largest supercomputers, HPC enables the exploration of new frontiers in science and engineering, by complementing or even replacing physical testing and experimentation that otherwise may be expensive, time consuming, or even impossible.

The Importance of HPC

For centuries, scientific method has been based on the two pillars of theory and experimentation. Today there are many who call out computational modeling and simulation as a third fundamental pillar of science, as more discoveries are made possible by HPC. As such, HPC is linked inextricably to scientific research, yes, but also to industries such as manufacturing, oil exploration, pharmaceuticals, chemical engineering, and finance, as well as to national defense, homeland security, and cybersecurity.

HPC in Research

The largest supercomputers in the world are concentrated in government and academic research centers, addressing "grand challenge problems" such as predicting the path of a hurricane, modeling the spread of cancer in the body, or simulating the neural pathways of a human brain. But it is not only in these world-renowned supercomputing centers that discovery takes place. Researchers at almost any center of higher learning will leverage HPC in some dimension, be it astrophysics, biochemistry, geology, or archeology, whether on their own lab systems or by accessing resources available via public cloud computing.

HPC in Industry

Although the public perception of supercomputing is predominantly linked to public-sector research, more than half of HPC spending worldwide comes from commercial organizations. Scientific innovation begets advancements in engineering and technology, and industrial organizations seek competitive advantage from investment in computing. Some of the top industries that leverage HPC are:

- *Manufacturing:* Digital product simulation allows manufacturing companies to design, test, and modify virtual products in a computer environment without the time and expense of building and testing physical prototypes. At a large scale, this applies to car manufacturers conducting virtual crash tests of automobiles and airplane manufacturers modeling the aerodynamics and noise of wind over a wing. At a smaller scale, increasing numbers of consumer products manufacturers are deploying HPC for any number of household products—for example, designing a bottle such that it uses less plastic yet is still less likely to break if dropped from table height.
- *Energy:* Oil and gas exploration companies use HPC to model the earth's crust from seismic readings. Doing so lets them find the underground, prehistoric lakes and riverbeds they can extract oil from today. As oil and gas are extracted, the companies continue to run simulations to maximize yield. HPC has even helped oil companies return to fields they had previously abandoned, armed with new technology and new information. Oil companies tend to use some of the largest, most powerful supercomputers in the commercial sector.
- *Pharmaceuticals:* Drug discovery is an expensive R&D proposition. For every 100 targets, pharma companies hope one will prove viable to come to market. HPC helps those companies "fail faster," eliminating losing designs earlier in the process, so that more time and effort is spent on the most promising candidates. It was HPC that enabled the burgeoning field of genomics, and HPC has applications across computational chemistry, molecular modeling, pharmacokinetics and pharmacodynamics (PK/PD), bioengineering, and biostatistics.
- *Chemical engineering:* Countless new products and innovations begin with the introduction of new plastics and polymers. Chemical engineering companies use HPC in their manufacturing process, for example, by using modeling to optimize their mix tanks for improved yield. In the future, HPC may be increasingly used in the design of these chemicals as well, similar to how HPC is used in other industries.
- *Electronics design:* As semiconductor designs continue to shrink, it becomes perpetually more costly and difficult to design and test them. Semiconductor companies use HPC for electronic design automation (EDA) of their chips, reducing costs and improving yields.
- *Finance:* HPC has revolutionized how the finance industry works. Banks use large HPC clusters for econometric simulations, running new products through millions of potential worldwide economic situations before selling them to the public. In addition to risk management, financial services companies deploy HPC for high-frequency trading, pricing, and a wide range of analytics applications, such as fraud detection. In all, finance is one of the largest consumers of HPC technology in industry (just behind manufacturing, if large product manufacturing and consumer product manufacturing are combined), and also one of the fastest growing.

HPC in Defense

With how intrinsic HPC is to the advancement of scientific research and industry, it is no surprise that HPC is also critical to national security. For starters, advancements in industry and research can have direct translation to military efforts, for example, in the manufacture of a new helicopter or the availability of an ultra-local weather forecast supporting an operation. Many supercomputing endeavors may be classified when it comes to military and defense issues, but there nevertheless several categories of applications we can be sure of:

- *Combat simulations:* One of the most straightforward ways in which supercomputing is deployed for national defense is in combat simulations, ranging from “person-in-the-loop” models like flight and tank simulators to large-scale wargames. (The 1983 movie *WarGames* was based on exactly this concept.)
- *Nuclear stockpile stewardship:* HPC allows the maintenance of a nuclear stockpile without the need for nuclear testing. Nuclear explosions can be simulated using supercomputing technologies.
- *Defense and response simulations:* In addition to simulating combat, HPC can be used to simulate defensive responses to possible attacks, modeling for example, how to respond to an attack on the electrical grid or the release of a chemical agent in a metropolitan area. (Theoretically, these simulations could also be used offensively, not just defensively.)
- *Intelligence and security:* HPC is used in the gathering and analysis of data streams that can provide evidence of planned attacks or point toward an enemy’s weaknesses. Information analysis can also be used to make borders safer, including linking the analytics with emerging advancements such as facial recognition.
- *Cybersecurity and cyberattack:* Cybersecurity is an issue that affects companies and private citizens, but at the government level, it is a matter of national security. HPC is now being used in some cases to model defensive responses to cyberattacks. That said, this is an instance in which HPC is used offensively more frequently than defensively, and at larger scale. Supercomputing can be used to break passwords, to hack into systems, and to analyze any information that is acquired.

What Is an HPC System?: Eras of Innovation

Like in the industries fueled by HPC, there is a rapid pace of change in HPC itself. The very nature of HPC is that there is always a harder problem to solve. Simulations take on grander scale and more realism. Models get built with higher fidelity and more degrees of freedom. Until one day we reach the end of science and declare there is nothing left to be discovered or invented, there will be a need for a more powerful computer to enable insight and innovation.

When we examine the HPC industry, we consider what constitutes HPC at the low end of the market. At a minimum, we consider scientific and engineering tasks that can be run in parallel over at least two “nodes”: otherwise independent elements that are being used in concert to address the task. Technical computing extends down to applications that can be run on individual PCs or workstations, but we consider this to be below the threshold of the HPC market.

As the HPC market has grown and spread, the systems themselves have gone through transformations in architecture. The ongoing evolution in how an HPC system is built has continually changed the dynamics of the industry in terms of who has access to HPC systems, how difficult they are to use, and how much they cost.

While innovation in HPC is continuous, a long-view history of the industry can segment development into distinct eras:

- *Specialized design (technologically contained / architecturally distinct):* Originally, supercomputers were relatively self-contained devices. A single technology vendor would design all the pertinent hardware and software components to build a scalable system, including processing units, networks, and operating systems. These designs were inherently custom to each specific vendor, and there were only a few companies that made them, such as CDC, Cray, IBM, and NEC. Over time, enterprise computing engendered an evolution in which server technology—using RISC processors and variations of the UNIX operating system, from companies such as IBM, HP, Sun Microsystems, Silicon Graphics, and Digital Equipment Corp.—could be scaled up for HPC. These components and operating environments were more familiar to more users, but the systems were still unique to their specific vendors.
- *Commodity clusters (technologically disaggregated / architecturally identical):* In the 1990s, some HPC users—including major supercomputing centers—began constructing HPC systems as "clusters" of lower-cost, industry-standard servers, connected over an Ethernet network. This allowed users to build systems to any size while getting components from any vendor using x86-architecture processors from Intel or AMD, running versions of the open-source Linux operating system. (Linux is still the dominant operating system for HPC.) However, because the clusters were in fact comprised of distinct components, existing software modules had to be rewritten for the new architecture. Many people argued that the cluster model was less efficient and harder to program for, but after 10 years, clusters had become the dominant paradigm for building HPC systems. Over time, many enhancements became available (such as 64-bit processors, blade form factors, or faster networks), but the cluster architecture and its accompanying software model remained.
- *Specialized elements (technologically disaggregated / architecturally distinct):* Today we are seeing the HPC industry in the early stages of another architecture transition[1], the seeds of which were sown about 10 years ago, in a pair of parallel developments. For one, microprocessor speeds (measured in GigaHertz, GHz) plateaued, and microprocessor companies like Intel and AMD focused instead on putting multiple processing "cores" onto a single chip. For systems that serve multiple applications, each of which only requires a fraction of a core (as in a typical PC environment), this makes little difference, but for an HPC application that already must span multiple processors, the change required a new level of optimization in software. Simultaneously, other processing options began to come to the fore, including increasing interest in various types of "accelerators," additional processing elements that can be added to a system in order to boost the performance of certain functions. The biggest push in acceleration came from NVIDIA, a gaming company that found a market for its graphics processing unit (GPU) products in accelerating HPC applications.

---

[1] For further reading on this topic, see: Snell, Addison, "Beyond Beowulf: Clusters, Cores, and a New Era of TOP500," published on TOP500.org, November 11, 2014, https://www.top500.org/news/beyond-beowulf-clusters-cores-and-a-new-era-of-top500/.

With these and multiple other developments, there are now myriad options for building HPC systems out of specialized processing elements. And while this sounds promising in terms of providing options, it also presents a tremendous challenge in determining (a) which architectural components will best suit a given problem and (b) how to rewrite software in order to run most efficiently. Furthermore, applications have varying requirements. As a result, 88% of HPC users now say they expect to support multiple architectures over the next few years, attempting to align application workloads to the elements that best suit them.[2]

This is important in that we are now at another crossroads in the HPC industry, at which HPC-using organizations must revisit how software components must be built to take advantage of new technology developments, against a backdrop of uncertainty as to which technologies will win out in the market. As we move into the new generation of supercomputing, there could be significant change in where leadership in the industry comes from.

Measuring Supercomputing

The most common metric of supercomputing performance is "flops," short for floating-point operations per second.[3] (In computer parlance, a floating-point operation is one with an arbitrary number of decimal places, such as "2.4 x 1.624 = 3.8976"; this is in contrast to integer-only operations.) As with other computer terms like "bytes," flops are usually expressed with a numerical prefix: "100 Megaflops" means 100 million calculations per second.

Of course, the HPC industry is well beyond Megaflops. At the uppermost echelon of supercomputing, we have also transcended Gigaflops (billions of calculations per second) and Teraflops (trillions), into the range of Petaflops (quadrillions, or millions of billions). Currently, the top supercomputer in the world, measured by theoretical peak performance, is the Sunway TaihuLight[4] at the National Supercomputing Center in Wuxi, China, with a peak of 125 Petaflops—a mere factor of eight short of the next prefix marker, Exaflops (quintillions, which can be thought of as billion-billions or million-million-millions).

In the previous paragraph, "theoretical peak" is worthy of emphasis, because actual delivered performance will fall somewhere short of this mark, depending on the software application and its programming. For this reason, it is common to look at benchmarked supercomputing performance for specific applications.

The TOP500 List [5]

The semi-annual TOP500 list is a ranking of the top 500 supercomputers in the world according to the LINPACK benchmark[6], a straightforward exercise of solving a dense matrix of equations. On this benchmark, the Sunway TaihuLight is still top, with a delivered performance of 93 Petaflops, or about

---

2 Intersect360 Research special study, "Processor Architectures in HPC," 2016.

3 Because the *ps* at the end of the word *flops* stands for "per second," some people also use "flops" as a singular noun—one flops, one Petaflops. Colloquially the singular is often shortened to "flop," and we used this construct in this statement.

4 Intersect360 Research, *This Week in HPC* podcast, June 21, 2016, https://soundcloud.com/this-week-in-hpc/new-1-supercomputer-crushes-competition-and-china-takes-top500-by-storm.

5 To view the current (and past) TOP500 rankings, along with analysis of the systems on the lists, see http://www.top500.org.

6 Specifically, the High Performance LINPACK (HPL) benchmark; for more information, see: https://www.top500.org/project/linpack/.

74% of its theoretical peak. The second-ranked system is also in China, the Tienhe-2 (or “Milky Way 2”) system at the National Supercomputer Center in Guangzhou, with a delivered LINPACK benchmark performance of 34 Petaflops, against a theoretical peak of 55 Petaflops (62% efficient).

The next three systems on the current list (published November 2016) are all in the U.S., at labs run by the Department of Energy: “Titan” at Oak Ridge National Laboratory, 18 Petaflops LINPACK, 27 Petaflops theoretical peak (65% efficient); “Sequoia” at Lawrence Livermore National Laboratory, 17 Petaflops LINPACK, 20 Petaflops theoretical peak (85% efficient); and “Cori” at Lawrence Berkeley National Laboratory, 14 Petaflops LINPACK, 28 Petaflops peak (50% efficient).

The next five systems in the current ranking include two in Japan, one in Switzerland, and two more in the U.S. The rest of the top 25 also include systems in the U.K., Italy, Germany, Saudi Arabia, and France. Among the rest of the top 100, there are systems in South Korea, Poland, Russia, the Czech Republic, Switzerland, Sweden, Finland, Australia, and the Netherlands.

The TOP500 list is frequently used as a proxy for the state of the HPC market, but this has several drawbacks. First, a system need not be represented on the TOP500 list. Because running the LINPACK benchmark itself requires the dedication of time, expertise, and resources, inclusion on the list is usually driven by a desire to be recognized. Many commercial organizations decline to participate in TOP500 ranking. (The top-ranked commercial system on the current list is at #16, a 5 Petaflops (LINPACK) system owned by Total Exploration Production, an oil exploration company in France.) Even in the public sector, there are several systems not listed; perhaps most notable among these is the Blue Waters supercomputer at the National Center for Supercomputing Applications at the University of Illinois, which may in fact be the most powerful supercomputer at an academic site in the U.S.

Participation in TOP500 is also often driven by a campaign of inclusion, particularly by system vendors who wish to claim a strong position for marketing benefits. Not only may vendors encourage their customers to participate, but the submission rules also allow systems to be included by proxy: If the LINPACK benchmark is run and verified on one system, then it can be assumed to run at least as well on any system of the same configuration with at least as many processing elements. Some of these submissions’ locations are identified only generally by industry, such as “Government” or “Automotive.” This is more common in the lower tiers of the list, where the systems are not as distinctive.

In 2016, the proportion of systems on the TOP500 list based in China suddenly expanded. This does not mean that China suddenly discovered supercomputing, but rather, that (in a sense) China suddenly discovered the TOP500 list, and that there was a somewhat nationalistic desire for its systems to be counted.

The TOP500 list is also often criticized because the LINPACK benchmark used for the ranking is not representative of general mixed supercomputing workloads. In fact, it is a relatively straightforward benchmark. To use an athletic metaphor, it measures sprints, not decathlons, and it certainly does not extend to also include crossword puzzles and a talent contest. As such, the benchmark taxes the computing elements of a system far more than others, such as the memory, the network, the data storage, or (quite pointedly) the programmability.

One might own a supercomputer that in its time excels at LINPACK and little else. These are often derided as “stunt” machines, good for PR value but not for science. However, it is important to acknowledge that we have heard this debate before. When clustered architectures became the new supercomputing paradigm, there was little software available to run on them, and programmability was viewed as a major hurdle. The first machine to achieve a Teraflop on LINPACK was the ASCI Red cluster, first installed in 1996 at Sandia National Laboratories, as part of the Accelerated Strategic Computing Initiative (ASCI) under the DOE’s National Nuclear Security Administration (NNSA). Although ASCI Red did run its intended applications in nuclear stockpile stewardship quite well, it became a touchstone of debate in the supercomputing community, in that it was not at the time viewed to be a “general purpose” system for scientific discovery. In the years that followed, clusters came to dominate on LINPACK and the TOP500 list, but it took years of effort to get many scientific applications to use clusters efficiently. For some applications, non-clustered (single system) supercomputers are still preferred today.

A final criticism of the TOP500 list is that it is not representative of the HPC market as a whole, which is far broader than 500 (mostly public-sector) systems at the top end of the market. A thorough industry analysis looks quite different than an analysis of the TOP500 list, in many segmentations.

Nevertheless, the TOP500 list is a useful tool, and the best one available for ranking individual supercomputing systems at the top of the market. It provides a starting point with interesting data, and it helps to prod investment. But careful, thoughtful, thorough analysis of the supercomputing market must go beyond the TOP500 list and the LINPACK benchmark.

Current HPC Market Dynamics

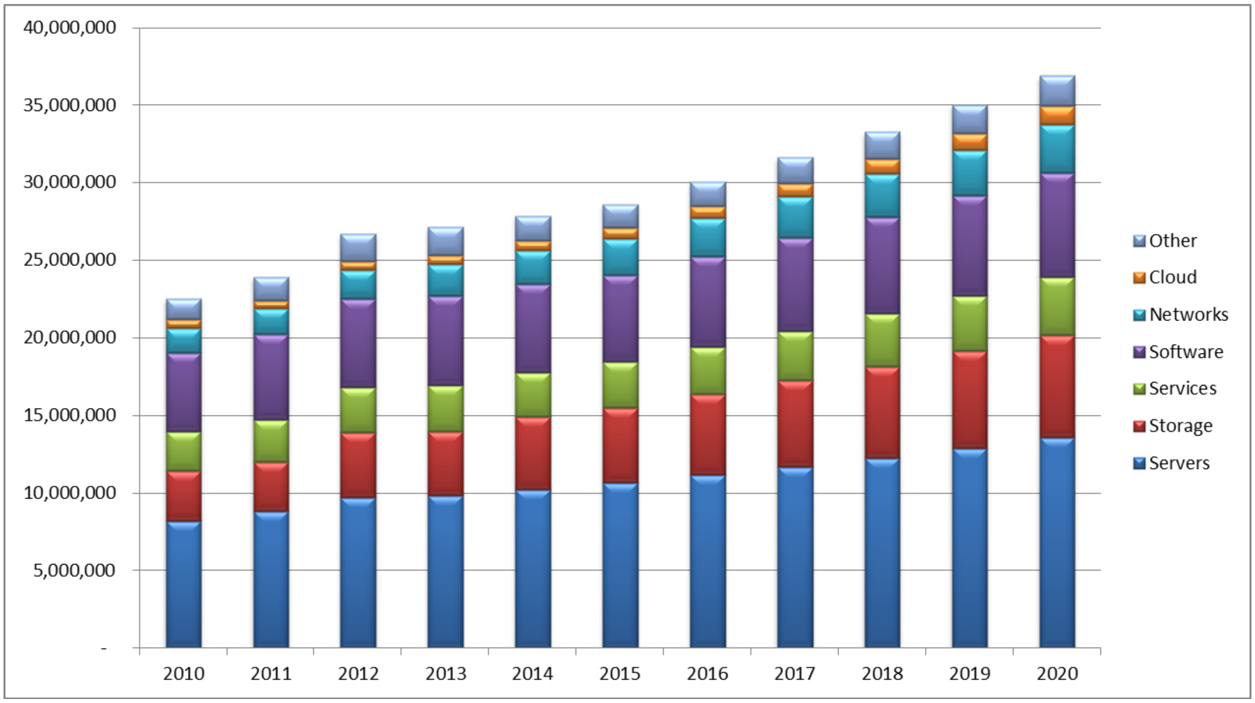
In 2016, the total worldwide HPC industry was a $30.1 billion market[7], including all product and services categories, such as servers, storage, software, networking, services, and even HPC conducted over public cloud resources. This figure does not include internally budgeted items, such as power consumption or personnel costs, which can also be considered as part of a total HPC budget for an organization.

Of this $30.1 billion, the largest component is servers, which include all types of HPC systems. At $11.1 billion in revenue, servers comprise 37% of the HPC market. The next largest components are software ($5.8 billion, 19.4%) and storage ($5.2 billion, 17.3%). Although networking appears as a relatively small component ($2.5 billion, 8.2%), it is important to realize that system networking is most often included with an HPC cluster, and therefore is absorbed into the cost of servers.

---

[7] For this and other market revenue figures, we use a 2016 forecast based on 2015 actuals. Intersect360 Research will complete its analysis of 2016 actual revenue in roughly May 2016.

Figure 1: Total Worldwide HPC Market, 2010-2020, ($000)[8]
2010-2015 actuals, 2016-2020 Forecast



HPC in the Cloud

Cloud computing ($774 million in 2016, 2.6%) is a small portion of the HPC market. Here we refer to money spent by HPC end users to run their applications on a public cloud resource (such as Amazon Web Services, Google Cloud, Microsoft Azure, or SoftLayer). We are not counting the entire infrastructure owned by cloud service providers as part of HPC; for a discussion of that market, see "The Hyperscale Market," below.

The utility computing model—renting infrastructure and paying for it on an as-used basis—has been part of the HPC market for decades, but always as a very small component. Cloud computing has made this easier, and many organizations are choosing to outsource large portions of their enterprise infrastructures to cloud providers. Indeed, beginning in 2014, we began to see an uptick in the usage of cloud for HPC, and we project a high growth rate throughout our forecast period.

However, cloud will continue to be a small part of the total HPC market. Cloud computing makes the most economic sense for those who need to fully utilize a resource for a short amount of time, much like

8 Intersect360 Research, "Worldwide High Performance Computing (HPC) 2015 Total Market Model and 2016–2020 Forecast," September 2016.

renting a car or taking a taxi. Those who need to use the resource all the time often find it more economical to buy it than to rent it.

Within HPC, public cloud resources are most often used by academic researchers, who may be able to utilize cloud in burst for their projects or dissertations. In industry, the most significant usage currently comes from pharmaceutical companies, some of whom are reducing their internal HPC footprints and using cloud resources for occasional peak workloads.

Public cloud resources do make HPC more accessible to a wider community. However, the vast majority of serious HPC users will continue to own on-premise systems.

Sunway TaihuLight and Other "In-House" Systems

As noted above, the Sunway TaihuLight system is currently the most powerful supercomputer in the world, according all available public metrics. Despite this fact, it is difficult to include in HPC industry models by revenue, because the system was *built, not bought*.

The Sunway TaihuLight supercomputer at Wuxi is the product of a Chinese national initiative to build a supercomputer from emerging domestic technologies. Little information is publicly available, but a total budget of $300 million was announced. If we took that figure as a portion of the 2016 HPC market, it would represent 1% of total spending. However, this would be misleading. Most of this money was spent on manpower to design technologies. The personnel costs of system vendors aren't considered to be market spending, and this is also the case for this system at Wuxi. Only a minority of the $300 million was spent on components from established technology vendors. (For example, some silicon parts were purchased from networking company Mellanox, but the National Supercomputer Center says it designed its own system network based on these parts.) The true retail value of this system is therefore unknown and is not part of the revenue reporting.

At a smaller scale, any organization might build an "in-house" system. To the extent that components (such as servers or networking gear) are bought from established vendors, this revenue is accounted for in the market model. But if an HPC system is truly invented or assembled from materials lying about, there is no revenue to be tracked.

HPC Market Segmentations

As described above, HPC systems range from small clusters of only a few nodes to the world's largest supercomputers, with use cases spanning industry, academia, and government worldwide. Here are most of the most pertinent top-level market segmentations.

Figure 2: Vertical Market Distribution of HPC Revenue[9]

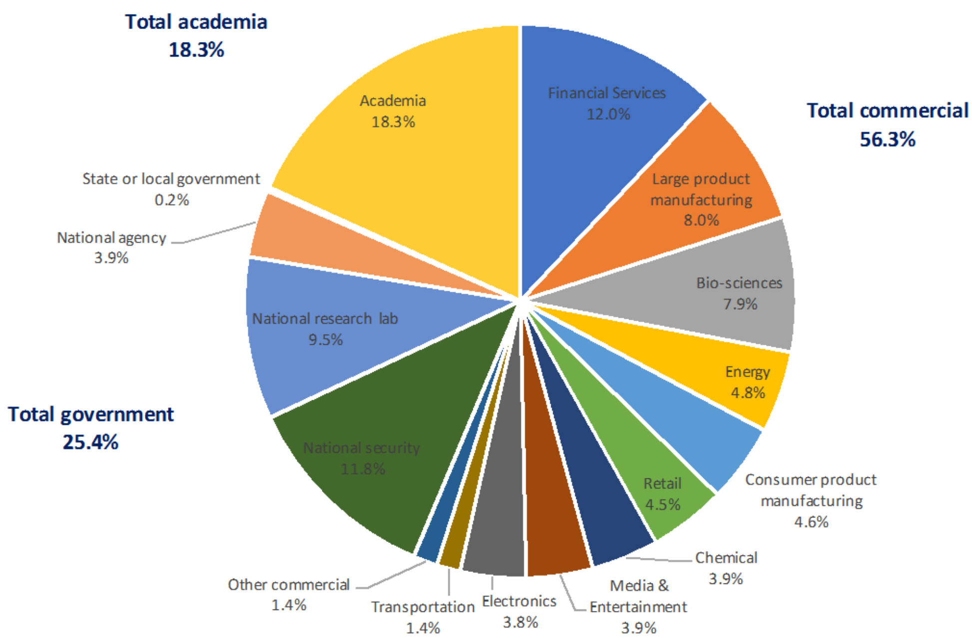
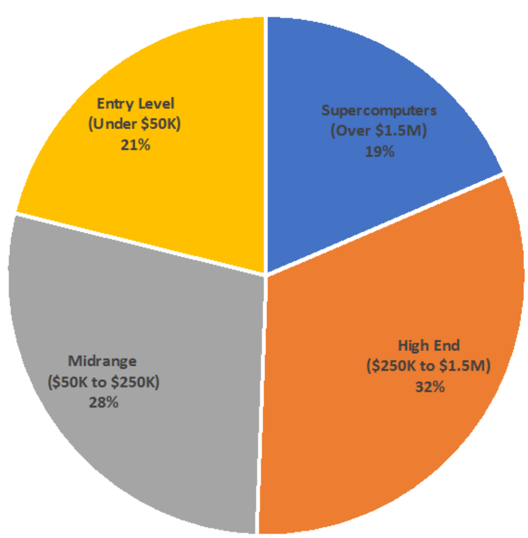


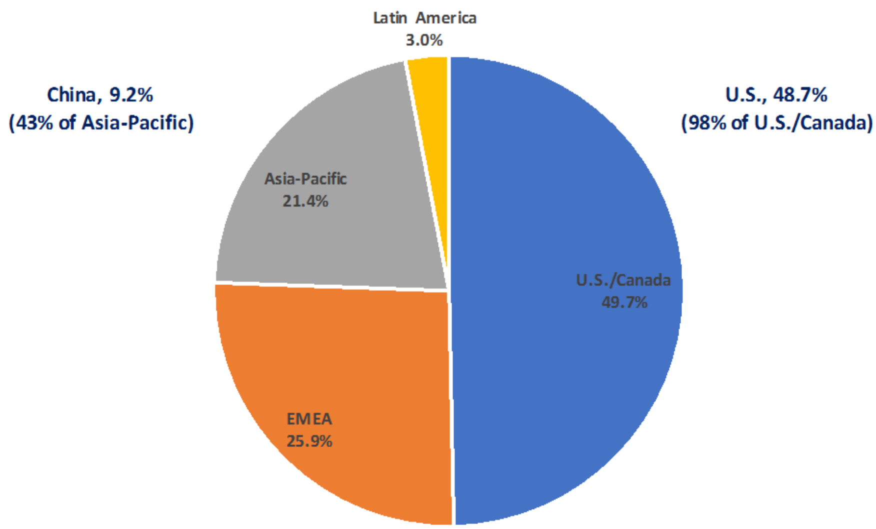
Figure 3: HPC Server Revenue, by Product Class[10]



9 Intersect360 Research forecast data, 2016.

10 Intersect360 Research forecast data, 2016.

Figure 4: Worldwide HPC Revenue, Geographical Distribution[11]



Although the world's two most powerful supercomputers are in China, and China also has more systems on the TOP500 list than any other country, there is in fact five times more HPC usage (by revenue) in the U.S. Even if we added $1 billion (all in one year) to the Chinese HPC market to represent an arbitrary high value for Sunway TaihuLight, the overall picture would not be much different.

The reason for this is twofold. First, China has done a remarkable job at a national level of painting a picture of a stronger market, versus no such organized effort in the U.S. to make the market seem larger. Second, and more importantly, the U.S. has a much more robust breadth of HPC usage across multiple industries. Compared to the U.S., China is still a relatively poor country, and there is less penetration of HPC through multiple markets.

That said, it does leave the opportunity for ongoing strong growth in HPC in China. Furthermore, China's investments in new supercomputing architectures, using domestic technologies, should not be discounted, particularly in light of the architectural shift now in play in the HPC industry.

Key Technology Component Vendors

As discussed above, HPC environments tend to be technologically disaggregated. That is, the key components of an environment often come from multiple different sources. The following are some of the key vendors from across the HPC landscape.

[11] Intersect360 Research forecast data, 2016.

- *Servers:* Worldwide, the overall market share leader in HPC server revenue is Hewlett Packard Enterprise (HPE). HPE recently acquired SGI, a onetime big name in HPC that still retained a small but loyal following and some unique technology. Dell EMC is not far behind HPE in market share. IBM used to be the biggest vendor, until it sold off its Intel-based server lines to Lenovo. IBM still retains some share with its systems based on IBM POWER processors. Cray (which specializes in the high-end supercomputer segment) and Penguin Computing are also noteworthy U.S.-based vendors. While Lenovo is based in China, it is a worldwide brand and now a tier-one vendor for HPC servers. Although it sells predominantly in China, Inspur also has significant share. Huawei has recently emerged as an up-and-coming brand. Supermicro sells some systems under its own brand, and many more through OEM partnerships. Atos/Bull is also a serious supercomputing provider based in France, as is Fujitsu in Japan.
- *Processing elements:* Intel is the giant among the processor vendors. Over 90% of the HPC market is built on Intel-based servers. IBM retains some share with its POWER processors, and AMD is still a competitor as well. However, other elements besides the main microprocessor are now at play, with various types of accelerators and co-processors. The most significant of these are graphics processing units (GPUs) from NVIDIA. Another category of co-processors is field programmable gate arrays (FPGAs). Here Intel is also a player, thanks to its acquisition of Altera. Xilinx is the most notable competitor.

  Another alternative that has become a touchpoint of research is ARM processors, the comparatively lightweight, lower-power processing components common to mobile devices such as iPhones and iPads. Companies such as Cavium, Qualcomm, and AppliedMicro have come out with commercial, 64-bit ARM varieties, and several supercomputing initiatives have been based on the concept. ARM offers open licensing, allowing multiple vendors and research centers to design around the processors. Fujitsu has announced its intentions to use ARM processors in its "Post-K" Exascale systems[12], and China has its own efforts to design 64-bit ARM processors domestically. ARM Holdings, a U.K.-based company, was acquired by the Japanese conglomerate SoftBank in 2016.

  Many other companies provide unique solutions. To reduce the reliance on outside technology, the Chinese government has invested in the development of its own domestic processing technologies.
- *Networking:* Over the past ten years, the dominant high-end system interconnect option has been a technology called InfiniBand, which is now offered almost exclusively by Mellanox, a high-performance networking specialist with dual headquarters in the U.S. and Israel. Intel has the ability to sell InfiniBand (based on its previous technology acquisition from QLogic), but Intel primarily is pushing its own high-end interconnect, OmniPath, which is relatively new to the market. Though it has no intentional HPC strategy, Cisco sells enough Ethernet solutions to be counted among the market leaders. Some of the supercomputing vendors, such as Cray, Bull, and Fujitsu, also have their own custom networking elements to support their large systems.

---

[12] Intersect360 Research, *This Week in HPC* podcast, June 28, 2016, https://soundcloud.com/this-week-in-hpc/knights-landing-and-pascal-gpu-face-off-at-isc-and-fujitsu-surprises-with-arm

- *Storage:* Storage in HPC has no dominant vendor. Dell EMC has the greatest share, followed by NetApp. Other significant players include Seagate, Hitachi Data Systems, HPE, and IBM, along with HPC niche specialists DDN and Panasas. It is worth mentioning that while this testimony focuses primarily on computational elements, for many applications and workloads, the configuration of high-performance storage for scalable data management can be the more significant investment.

The Hyperscale Market

Not included in these HPC market models are the "hyperscale" infrastructures at large internet application and cloud providers. This includes companies such as Google, Facebook, Amazon, Microsoft, AT&T, Apple, eBay, Baidu, Tencent, and Alibaba. These companies do operate at scale, and they do consume a certain amount of high-performance technologies.[13]

Beginning in 2007, Intersect360 Research maintained "ultrascale internet" as a segment of the HPC market. But by 2014, it was evident that what became better known as "hyperscale" had grown and evolved into its own segment, with distinct dynamics from the HPC market. We define hyperscale as *arbitrarily scalable, web-facing application infrastructures that are distinct from general enterprise IT*. In the top tier of the market, there are eight companies that spend over $1 billion per year on hyperscale infrastructure. There are dozens that spend at least $100 million per year, and hundreds more that spend over $1 million. In all, the hyperscale market represented $35 billion of the enterprise IT market in 2016, concentrated into the high-end providers. This is separate from the $30 billion HPC market.

The hyperscale market is significant to this discussion for several reasons. First, it provides a second, high-growth IT segment for the consumption of high-performance components. This is a powerful attractant for technology providers. Selling to just one of these top-tier hyperscale companies can mean tremendous success. Second, techniques and technologies from the hyperscale market can migrate into HPC, whether they are innovations in hardware, in software, or in the facilities management challenges of operating large systems at scale. And third, the hyperscale market has been the epicenter of development for the rapidly developing field of artificial intelligence (AI), fueled by new capabilities in the domain of "machine learning." (See section on Artificial Intelligence in "Looking Forward," below.)

Despite all these similarities, there are key criteria that make hyperscale different from HPC. The most important has to do with function. In serving up internet applications (whether in search, social media, content streaming, retail, or any other hyperscale domain), hyperscale infrastructures are designed to handle large numbers of small jobs. By contrast, HPC infrastructures are designed to handle comparatively small numbers of larger jobs. As such, most hyperscale infrastructures would be poor fits for HPC workloads. The difference is subtly implied in the names: In hyperscale, the greater emphasis is on scale; in High Performance Computing, the greater emphasis is on performance.

---

[13] Intersect360 Research, "The Hyperscale Market: Definitions, Scope, and Market Dynamics," April 2016.

Big Data and Analytics

Another key proximity area to HPC has been the field of big data and analytics. Big data created a new category of enterprise IT applications that has some of the same characteristics of HPC applications. Analytics seeks out answers in data, with metrics like *time to insight* that measure the effectiveness of big data programs. As such, metrics of performance become important criteria in evaluating technologies for big data. Surveys in 2012 and 2013 confirmed that “I/O performance,” the ability to move data into and out of a system, was the greatest “satisfaction gap” in technologies for big data—the area with the greatest unmet need relative to satisfaction with existing solutions.[14]

However, big data has not proved to be a major boon for the HPC market. Although many organizations launched big data initiatives, for most organizations, their spending patterns did not change much. Companies began with the data, the storage, the servers, the networks, and the personnel they already had, and they did the best they could. (They may have invested in new software, but this was often inexpensive or even free. Services spending did get a small boost.)

The most significant technology that did emerge from IT’s big data awakening was flash storage, or solid state disks (SSDs). These devices offer faster I/O performance than traditional spinning hard drives, albeit at usually a higher cost per byte of storage. Many organizations inside and outside HPC now incorporate SSDs as part of their total storage hierarchy.

Analytics is a category of application that can be run on any system, whether or not it is HPC. “Analytics” is also a very broad term that can be stretched to cover many types of computing. Some HPC systems run big data workloads, but not all big data workloads are HPC.

The Race to Exascale

As mentioned above, there is an insatiable need for ever more powerful HPC systems to solve increasingly complex scientific problems. The TOP500 list provides a measuring stick for achievement, as new deployments leapfrog over their predecessors in how many flops they deliver. This pursuit takes on extra significance as we approach the thousand-fold increases that usher in a new prefix era.

In 1996 ASCI Red (discussed above in the section, “The TOP500 list”), was the first supercomputer to achieve 1 Teraflop of performance, perceived as a great victory for the cluster experiment. Twelve years later in 2008, the Roadrunner system, operated by NNSA at Los Alamos National Laboratory, achieved the milestone a thousand-fold greater, becoming the first system to deliver 1 Petaflop of performance.

We are approaching the time when the first Exascale system will be deployed. *Exa-* is the next prefix on the list; 1 Exaflop = 1,000 Petaflops. An Exaflop is one quintillion calculations per second; that’s one billion-billion, or one million-million-million, or if you prefer, 10^{18} or 1,000,000,000,000,000,000. If those speeds seem absurd, rest assured that there are applications that will demand them, not only in scientific research, but in industry as well.

---

14 Intersect360 Research special study, “The Big Data Opportunity for HPC,” 2012 and 2013.

The following is an excerpt from a 2014 report by the U.S. Council on Competitiveness, generated by Intersect360 Research, on the benefits of supercomputing for U.S. industry.[15] The first key finding of this report was that "U.S. industry representatives are confident that their organizations could consume up to 1,000-fold increases in computing capability and capacity in a relatively short amount of time."

> There is tremendous optimism across industry that increases in capacity would be consumed. Looking at their most demanding HPC applications today, 68% of respondents felt they could utilize a 10x increase in performance over the next five years. Perhaps more surprisingly, 57% of respondents – more than half – say they could make use of a 100x improvement in performance over five years, and 37% – more than one-third – still agreed when the threshold was increased to 1,000x. This finding is supported by the qualitative interviews, as follows:
>
> > *There are two Holy Grails at exascale that I am just dying for. One of them is computational steering, taking the engineer, the scientist, the doctor, the accountant, putting them in the chair, give them the joystick, basically running through the application and continuously optimizing to whatever state they want to be at. The other Holy Grail is being able to do digital holography, where I can truly create virtual objects, which is the ultimate VR [virtual reality]. … To me, that unlocks human creativity, and we have another Renaissance period, a scientific Renaissance.* [Interview 12, Consulting services for industrial supercomputing adoption]
> >
> > *I don't think anybody can exactly articulate the extent to which it's going to change how we do product development, but it could be radical. It could take our development time to less than half, perhaps, if you don't halve to build prototypes and have systems in the field and do all of the testing virtually. Who knows?* [Interview 3, Large product manufacturing]
> >
> > *In a research mode, we can evaluate a [single] design, but to put it into full production and try to evaluate the [entire] product line, it's impossible at that level. We can impact things at a research level – to try to understand the benefit, can we go in this direction – but to really have a broad impact on the whole product group, it's prohibitive. We're going to need somewhere between 10x and 100x in order to achieve that.* [Interview 7, Large product manufacturing]
>
> One leader from the financial industry did provide a detailed roadmap of what his organization could do with each new level of application scalability:

---

15 U.S. Council on Competitiveness and Intersect360 Research, "Solve. The Exascale Effect: The Benefits of Supercomputing Investment for U.S. Industry," October 2014, http://www.compete.org/reports/all/2695-solve.

> *There's a whole hierarchy that happens in every product in finance. When people start trading a product, the first thing they need is a price. They need to be able to compute an arbitrage-free price based on other securities. … That involves having a model that you can calibrate to the market and price the security. That's one level of computation. If it's a complicated model, it can take significant computing power to do it.*
>
> *Now, the next level up, once you can do that, you want to say, how is the price going to change if the market changes? Now you have to perturb all the market input models, and there could be five or 10 or 20 or 30, and re-compute, so now you're talking about increasing the level of computation you need by an order of magnitude.*
>
> *And then once you can do that, there's two other directions it goes. Now I want to analyze the strategy that's involving the security, so I want to pull historical data and try running out the strategy using this model every day over the last five years. So now you have a huge amount of computation to run each of these tests, another couple orders of magnitude. And then once you're trading these successfully you have a portfolio of them that you need to analyze how the whole portfolios going to behave, so it's another several orders of magnitude.*
>
> *As the computing gets faster it makes more things possible. … Once your computing catches up and you can do it on an interactive basis, you can respond to market changes, and it opens up a whole new world. When you have to do your portfolio analytics overnight, then it's a different world than when you can do them in real time, interactively, where I can say, 'Oh, the market moved suddenly. How does that impact my entire portfolio? Can I track my VaR [value at risk] as the market moves?' That's an innovation that could have a major impact on the markets.* [Interview 2: Financial services]

Exa-scale vs. Exa-flops

While the pursuit of greater levels of performance has been undiminished, one subtle detail has changed. In the industry vernacular, it is common to discuss Exa*scale*, not just Exa*flops*. The word *Exascale* does not have a specific meaning, but its usage is born from the discussion of the usefulness of a supercomputer. What good is an Exaflop if it cannot be attained by any real scientific application? In that vein, *Exascale* can be thought of to mean "having real applications that run at an Exaflop." (In practice, however, many people do not make a distinction, and once any Exaflop supercomputer is built, it is likely that many will proclaim, "Exascale has arrived!")

If it seems inevitable that such a system will be built, and soon, there are nevertheless dramatic challenges to be overcome. Some of the most significant are:

- *Power consumption:* The Sunway TaihuLight system consumes over 15 Megawatts of power for its 93 Petaflops of LINPACK performance. That ratio of 6 Teraflops per Kilowatt is already second-best among the top ten supercomputers in the ranking. (The best in the top ten is the eighth-ranked Piz Daint system at the Swiss National Computing Center, CSCS, which delivers 9.8 Petaflops for 1.3 Megawatts, a ratio of 7.5 Teraflops per Kilowatt.) Even at 10 Teraflops per Kilowatt, an Exaflop system would require a power budget of 100 Megawatts. The U.S. Exascale Computing Project sets a goal of delivering an Exaflop system with a power budget of 20 Megawatts, a ratio of 50 Teraflops per Kilowatt.

- *Reliability:* The more components you add to a system, the greater the odds that one of them will fail. The Sunway Taihulight system contains over 10 million processor cores. If only one in a million fails on a given day, there are 10 failures per day, and that does not take into consideration failures in memory, data storage, or networking. An Exascale system may have an order of magnitude more components than that. Systems of this scale will need to handle individual component failures gracefully, without significantly degrading the system as a whole.
- *Programming:* Considering the underlying hardware changes at play, as well as the increasing diversity and specialization of technologies, this may be the greatest challenge of all. Basic algorithms and programming models need to be revisited for this level of scale, and what works best on one type of supercomputer may not work efficiently (or at all) on another.

Who Will Get There First, and When?

The Chinese have a substantial edge right now at the zenith of the supercomputing market, and a funded plan to drive to Exascale. There is a good chance that China will deploy an Exascale system (built "in-house") by the end of 2019. Japan previously had an Exascale plan on a similar timeframe, but recent delays mean Japan likely won't achieve Exascale until 2020 or 2021 (likely to be built by Fujitsu).

The U.S. had initially planned to deploy its first two Exascale systems in 2022 to 2023, about three years after the Chinese. These follow three currently installed "pre-Exascale" systems at U.S. DOE labs—one system based on Intel architecture, and two by IBM with NVIDIA GPUs—but there is no commitment that the eventual Exascale systems will come from these vendors. In November 2016, the U.S. Exascale Computing Project ratified a strategy to introduce an additional "novel architecture" sooner, by the end of 2021, a full year or more ahead of the originally planned systems.[16] [17] In that timeframe, the U.S. would deploy closer to China and Japan. France and Russia could also field Exascale systems in a similar timeframe.

Looking Forward

Looking ahead, there are some technologies and applications that have the potential to provide a discontinuous advancement in the way that HPC is done.

Machine Learning / Artificial Intelligence

Hyperscale companies are using "machine learning" techniques to make significant advancements in artificial intelligence. Deep learning involves two steps: training and inference. In the training step, massive amounts of data are used to analyze patterns. For example, there may be millions of photos that

[16] Intersect360 Research, This Week in HPC podcast, December 13, 2016, https://soundcloud.com/this-week-in-hpc/episode155-hpe-puts-the-machine-in-motion-us-embarks-on-faster-path-to-exascale.

[17] Feldman, Michael, TOP500.org, "First US Exascale Supercomputer Now On Track for 2021," December 10, 2016, https://www.top500.org/news/first-us-exascale-supercomputer-now-on-track-for-2021/.

are tagged to indicate "cat," and millions more similarly tagged, "not a cat." The training algorithm sifts through the data to determine the essential elements of a picture that correspond to *cat* or *not a cat*. When confronted with a new picture, the inference algorithm can then come up with the likelihood that there is a cat in the photo, without human intervention.

Based on advancements in machine learning, artificial intelligence is making great leaps forward for consumers and businesses, in applications such as natural speech recognition and autonomous driving. Within the past few years, machines have beaten human experts at games including *Jeopardy!*, Go, and poker.

Today machine learning and AI are predominant in the domain of hyperscale, not HPC, though there are many similarities. The leading researchers in AI are the dominant hyperscale companies, with one notable addition: IBM, which has invested heavily in its Watson technology for "cognitive computing." Several major supercomputing sites are working on AI, and Japan has announced two publicly funded supercomputing projects with AI focuses.

AI has the potential to touch almost any industry, and there are some it may revolutionize. Some of the possibilities are:

- *Medicine:* This is the most "marketable" of AI advancements, as there is a popular demand for technology that can improve and extend people's lives. AI can be used to look across wide databases of symptoms and patient histories to arrive at more accurate diagnoses, especially for rare conditions, and to design personalized courses of treatment. AI can also monitor symptoms to alert medical personnel to important changes in patients' conditions.
- *Finance:* Although less popular than medicine as an avenue for AI, finance is a hotbed of machine learning, as financial services organizations have troves of data that can be used to optimize pricing and investments. Any financial mechanism—whether it is a credit card, a mortgage, or an insurance policy—has a price, often in the form of an interest rate. Rather than dividing customers broadly into risk categories (known as "tranches"), financial institutions can use machine learning to analyze the individual risk of any consumer, business, or investment, as it changes over time in response to changing inputs. AI can also be used to optimize fraud detection (in credit card transactions, insurance claims, etc.) and to anticipate future changes in market conditions.
- *Retail:* Recommendation engines are already important tools in retail. Most of us have seen messages on our screens with suggestions, "Since you recently bought (or downloaded, or browsed for) *X*, you might also be interested in *Y*." AI can do this more intelligently, across multiple platforms, with a wider array of data, fast enough to include recommendations and special offers at the moment of sale. AI can also be used to analyze and predict sales trends, enabling better inventory management. In the case of food, this can also reduce spoilage.
- *Defense:* Many of the advancements made in AI in research and industry have applications in defense. Most notably, AI can directly improve the analytics of vast amount of intelligence data, which can better enable insights both offensively (where and when to go after a target) and

defensively (detecting terrorist activity and predicting attacks). Autonomous drones, robots, and vehicles have obvious strategic military benefits. And AI capabilities could extend to both cybersecurity and cyberattack strategies, whether planning or preventing assaults based on hacking.

Quantum Computing

Quantum computing represents a potential discontinuous advancement in the way supercomputers could be built. In the current model, all computing is based on “bits”—switches that can be off or on, which translate to the 0s and 1s that are the foundation of computation and logic. Eight bits form a byte, which gathered together form the Gigabytes, Terabytes, Petabytes, and Exabytes of information coursing through supercomputers.

Quantum computers are built on subatomic quantum particles, which have the unusual and important characteristic of “superposition”—they can be in more than one state at the same time. These quantum bits, or “qubits” (pronounced “cubits”) can be equal to 0 or 1, or both 0 and 1, or any probabilistic combination of 0 and 1. A quantum computer can therefore explore a vastly greater solution space, based on fewer inputs.

The potential of quantum computing has been touted for many years, including recognition at the national level. Beginning in 2002, the High Productivity Computing Systems (HPCS) initiative under the U.S. Defense Advanced Research Projects Agency (DARPA) recognized the need for advancements in supercomputing that would “fill the high-end computing technology and capability gap” until the future promise of quantum computing.[18]

There are formidable challenges to building a quantum computer, well beyond mere expertise in quantum dynamics. The quantum particles need to be isolated, held in place, controlled, and measured, free from cosmic interference. To achieve this in a research setting is daunting; to do it commercially is harder still.

In 2007, D-Wave announced the first commercial quantum computer. It is uses “quantum annealing” techniques, which some have criticized as not fulfilling the full promise of a supercomputer based on “quantum entanglement.” In short, the quantum annealing technology is most useful for exploring independent paths in a solution space, as each qubit seeks a low-energy point. (Imagine dropping marbles over an uneven surface. Each marble will roll to a local low point. The more marbles you drop, the greater the chances that at least one of them will find a path that rolls to the lowest point on the entire surface. This point is the “optimal solution” for the space.) D-Wave has sold a few systems, including to Google and NASA Ames Research Center, who are collaborating on the technology. The current D-Wave systems scale up to 2,000 qubits.

---

[18] Graybill, Robert, DARPA/IPTO, “High Productivity Computing Systems,” March 13, 2003, https://science.energy.gov/~/media/ascr/ascac/pdf/meetings/mar03/Graybill.pdf.

In March 2017 (less than two weeks before this testimony date), IBM announced the commercial availability of a “universal quantum computer,” which utilizes “pairwise quantum entanglement,” meaning any two qubits can be linked to each other’s states. According to IBM, a system of *n* qubits is therefore capable of fully exploring a solution space with 2^n possibilities. Its current system of 5 qubits can therefore be programmed to look at 32 (2^5) possibilities in a space. If that seems small, consider that IBM also says it will have systems with up to 50 qubits “within a few years,” which would be on pace to exceed current supercomputing capabilities for some categories of problems, *if* the technology works and it can be programmed.

Even in the most aggressive case, quantum computing will not displace conventional computing in the current planning horizon. At best it will provide a way to solve problem types that are not well-suited to current computing architectures. The first areas for quantum computing will be applications that take relatively few inputs, explore a large possible set of solutions, and provide few outputs. Playing chess is a metaphor for this type of application, but there are potential real-world scientific applications in materials science, biotechnology, and possibly also encryption (or decryption, as quantum computing might excel at factoring large numbers).

HPC INVESTMENT IN THE U.S., CHINA, AND REST OF WORLD

Throughout most of the history of supercomputing, the U.S. has been the dominant leader. Most of the vendors of key technologies have been U.S. companies, and U.S. national labs have been at the forefront of supercomputing research. Throughout industry and academia, the U.S. dominates in HPC usage.

However, access to HPC technologies is no longer rarified. Anyone with the budget (including capital budget, facilities, and human expertise) can build a supercomputer, from component technologies that are readily available. In the past, the U.S. was able to limit access to supercomputers through export controls. Today, individual technologies can be controlled, but there are alternatives available.

The Chinese program to build its national supercomputing efforts comes at a time when the model of how to build supercomputers is changing. With a paradigm shift, it is possible for one region to leapfrog ahead of another, even when it has been behind. As a metaphor, consider the revolution with mobile communications. A nation with limited telephone landline infrastructure could suddenly bound ahead in mobile with a well-timed investment. Such is the potential with supercomputing today. If Exascale systems look different from current systems, particularly in how they are programmed, then it is possible to essentially "come from behind" with timely investment. This section looks at the current supercomputing policy, strategy, and investment in the U.S., China, and the rest of the world.

Supercomputing in the United States

At a national level, current investment in new supercomputing technologies flows predominantly through DOE, including the DOE Office of Science and the NNSA. DOE national labs have been a focal point for supercomputing for decades, and that focus continues through the U.S. Exascale Computing Project.

A current collaboration known as CORAL (Collaboration of Oak Ridge, Argonne, and Livermore) is pursuing three "pre-Exascale" systems, using two different approaches. The supercomputers at Oak Ridge National Laboratory (ORNL) and Lawrence Livermore National Laboratory (LLNL) are based on IBM POWER technology and accelerated with NVIDIA GPUs[19], while the deployment at Argonne National Laboratory (ANL) uses Intel technology, with Cray as a system integration partner.[20] All three systems are planned to deliver over 100 Petaflops of performance, with target power budgets of 10 Megawatts.

These deployments highlight the competitive rift that has formed between the U.S. supercomputing vendors, which are now in two predominant camps. Intel is at the nexus of one camp, with system integration partners that will build scalable systems on Intel technologies, including its processing elements (both CPUs and FPGAs), interconnects (OmniPath and Ethernet), and accompanying software elements. The other camp is centered on IBM, which has its own systems and processors, and partners with other natural competitors to Intel in areas like accelerators (NVIDIA GPUs) and networking (Mellanox InfiniBand). Most technology vendors will feel pulled toward one camp or the other.

---

[19] Intersect360 Research, *This Week in HPC* podcast, November 16, 2014, https://www.top500.org/news/ibm-and-nvidia-pick-up-two-pieces-of-coral-and-a-look-ahead-to-sc14/.

[20] Intersect360 Research, *This Week in HPC* podcast, April 13, 2015, https://www.top500.org/news/intel-gets-final-piece-of-coral-altera-deal-in-doubt/.

Current Program Investments

In the pursuit of Exascale technologies, the DOE Office of Science has synthesized the Exascale Computing Project (ECP). (The ECP expands upon the previous Exascale Initiative, also under the Office of Science, which includes "Design Forward" and "Fast Forward" grants for companies designing next-generation technologies that could enable Exascale computing.)[21] As noted above, the U.S. had planned to field its first two Exaflop systems in 2022 to 2023, based on the CORAL "pre-Exascale" architectures, approximately three years behind China. A newly ratified plan would deliver an Exaflop system in 2021, based on a "novel architecture," presumably different from the two CORAL architectures already planned. (ARM architecture is a strong possibility, which would be similar to Japan's plan, in roughly the same timeframe.)

The ECP has stressed Exa*scale* over Exa*flops*, with focus areas in hardware technology, software technology, application development, and Exascale systems[22]. For the CORAL systems and their follow-ons, the rationale has been that if the U.S. is not going to reach an Exaflop first, then it will at least do it better, with more efficient, general-purpose systems serving a wider range of scientific applications. While this argument is not without merit, it has also been subject to debate, ceding a multi-year head start to other countries, which would not hold still in the interim.

The new novel-architecture plan brings the U.S. timeline closer to China and Japan, but questions arise as to whether any Exa*scale* considerations are being sacrificed with the new machine. A new architecture will have less software readiness than an established one, and it is being introduced a year sooner. Our analysis is that the added deliverable will reduce pressure for the U.S. to deliver an Exa*flop* sooner, while still allowing the CORAL successors to move forward.

Additional national funding for HPC in the U.S. flows through the Department of Defense (DoD), the National Science Foundation (NSF), the National Oceanographic and Atmospheric Administration (NOAA) under the U.S. Dept. of Commerce, NASA, and the National Institute of Health (NIH).

The DoD HPC efforts, through the DoD HPC Modernization Program, are consolidated primarily into four major DoD Supercomputing Resource Centers (DSRCs): U.S. Army Research Laboratory, U.S. Naval Research Laboratory, Wright Patterson Air Force Base, and the Engineer Research and Development Center (ERDC) of the U.S. Army Corps of Engineers. Previously two additional DSRCs received funding—the Maui HPC Center (MHPCC) in Hawaii and the Arctic Region Supercomputing Center (ARSC) in Alaska—but these were dissolved in 2015.

NSF and NIH grants fund HPC at academic sites. Some of the largest and most significant academic supercomputing labs in the U.S. are the National Center for Supercomputing Applications (NCSA) at the University of Illinois, the Texas Advanced Computing Center (TACC) at the University of Texas, and the Pittsburgh Supercomputing Center, which is a joint collaboration between Carnegie-Mellon

---

21 Exascale Initiative web site, http://www.exascaleinitiative.org.
22 Exascale Computing Project web site, https://exascaleproject.org/exascale-computing-project/.

University and the University of Pittsburgh.

Changes in funding can of course happen at any time, particularly with shifts in power between political parties in Congress or in the White House, or in response to changes in national or global economic conditions. That said, supercomputing programs have often enjoyed bipartisan support in the U.S., due to the multi-purpose links to scientific research, to industrial advancement, and to national security.

Foreign Vendors in the U.S.

The U.S. supercomputing efforts are not reliant to any significant extent on technology from vendors based outside the U.S. A complete, best-of-breed supercomputer can be built exclusively from technology from U.S.-based vendors, with multiple options. That said, the major vendors are all multi-national companies. Intel, IBM, HPE, and Dell EMC (among others) all have major operations in China. Processing elements are often fabricated in China.

At the system level, foreign-based companies like Lenovo and Huawei have trouble competing for U.S. government-funded supercomputing acquisitions. However, they compete on more even footing for commercial HPC business.

Supercomputing in China

As established above, China has undergone a surge in supercomputing investment in recent years, to the forefront of achievement worldwide. China currently hosts the two most powerful supercomputers in the world by LINPACK (TOP500) performance, and the Sunway TaihuLight is five times more powerful than the most powerful supercomputers in the U.S. Put another way, the top two supercomputers in the U.S. *combined* achieve only roughly the same performance as the *second-most* powerful system in China.

The Chinese market is notoriously difficult to penetrate—even to monitor it, let alone to sell into it. It is neither a free-press nor free-speech society, and we are often left to make inferences from what we can observe. It is possible that China has other classified supercomputers that are not known to the TOP500 list or to the world at large. (For that matter, this is possible in the U.S. or other countries too.) But in the case of the Chinese market, we believe it is more likely that the supercomputers we know about are also serving government interests. A supercomputer that is configured and advertised to serve weather and climate modeling, for example, might also serve nuclear simulations. Intersect360 Research assumes that these Chinese national supercomputing centers serve both defense and scientific research purposes.

Current Program Investments

The Chinese supercomputing programs are neither as well-communicated nor as well-known as their U.S. counterparts. The Chinese government usually works on 10-year cycles. We initially questioned whether the current Politburo would support supercomputing to the extent of the previous one, which funded the original Tienhe (“Milky Way”) supercomputer and its follow-on, Tienhe-2, which was installed after the changeover in power. Our assessment is that the level of investment has been at least stable, and may be increasing. Under its current administration, China seems determined to be the world leader in supercomputing technologies.

As part of this strategy, China is intentionally decreasing its reliance on imported technologies. The Tienhe supercomputer used Intel processors, integrated by Inspur. (Within China this was viewed as a Chinese system; outside China it was viewed more as an Intel system integrated in China.) Recently the U.S. government blocked certain processing technologies from export to Chinese supercomputing labs, due to the revelation that they were indeed conducting nuclear simulations.[23] These export restrictions included the Intel processors slated for Chinese supercomputing upgrades.

This action by the U.S. government may have had unintended consequences. The planned upgrades were certainly delayed, but in the interim, the Chinese government increased its focus on domestic microprocessor technologies, including the Sunway processor. It is difficult to say for certain whether the TaihuLight system would be more powerful or more efficient using Intel processor technology, but what is certain is that the Chinese initiatives can no longer be thwarted by U.S. export control.

The area in which China may lag the furthest behind other countries is networking. As noted above, the Sunway TaihuLight system incorporated networking chips purchased from Mellanox. Although the official statement is that the Chinese developed a unique network based on those chips, we assume that the technology is effectively InfiniBand, or something very much like it, and that the Chinese government could not have built an efficient, high-performance system interconnect without these chips, at least not in a similar timeframe.

The most important distinction of the Sunway TaihuLight may be that it was *built*, not *bought*. That is to say, the supercomputing centers themselves designed the components and integrated them. It is not clear to what extent the resulting systems might eventually be commercialized for sale inside or outside China. This presents an interesting ramification to consider: When private U.S. companies design supercomputing systems or technologies, they seek to sell them in as broad a market as possible, inside or outside the U.S. Many other countries thereby benefit from the investment. But China is a relatively closed economy, and if the Chinese government designs a supercomputer that is better than any other, even if only for selected purposes, then it is not certain that technology will ever be available to anyone else.

One final point about the Chinese supercomputing strategy is that over time is has leaned more toward centralization than decentralization. Rather than pursuing a strategy that would put HPC resources into individual companies and researchers, we find it likelier that the Chinese government would create programs of access to centralized resources.

Foreign Vendors in China

U.S.-based technology vendors perceive China as a market with tremendous growth potential, and many

[23] Intersect360 Research, *This Week in HPC* podcast, April 20, 2015, https://www.top500.org/news/us-drops-bomb-on-chinese-supercomputing-export-restrictions-threaten-tianhe-2-expansion/.

have invested in strong Chinese presences to capitalize on it. The competitive dynamic mirrors that in the U.S. Companies like IBM, HPE, and Dell EMC can compete for corporate business, but they have little access to government bids versus system vendors based in China. Inspur is the market share leader for HPC systems deployed in China.

Notable Supercomputing Strategies in Other Countries

The U.S. and China are not the only two superpowers in supercomputing. This section provides a brief analysis of some other considerations at national levels.

Japan

Not long ago, Japan (not China) was the dominant supercomputing force in Asia, and Japan is still among the world leaders today. From 2002 to 2004, Japan’s “Earth Simulator,” a multi-agency supercomputer built by NEC and designed specifically for global climate and ocean modeling, was recognized as the most powerful supercomputer in the world. More recently, the “K” supercomputer, built by Fujitsu at the RIKEN Advanced Institute for Computational Science, was the world’s fastest supercomputer in 2012, and the first supercomputer to top 10 Petaflops on LINPACK. The K computer is still the seventh-fastest in the world in the current ranking.

Today Japan is charting its path toward Exascale computing with a “Post-K” architecture from Fujitsu. Previous Fujitsu supercomputers have been based on SPARC processors, a variety of RISC 64-bit processors pioneered and promoted by Sun Microsystems. Moving forward, the Post-K systems will be based on ARM processors, which can be viewed as native Japanese technology since SoftBank’s acquisition of ARM Holdings in 2016. Fujitsu is also noteworthy in that it continues to pursue its own custom interconnect technology, called “Tofu,” rather than relying on Mellanox InfiniBand, Intel OmniPath, or another networking technology.

Japan at one point announced plans to deploy an Exascale system in 2019. Recent delays make 2020 or 2021 a more likely target. At this pace, Japan will likely be the second country with a supercomputing lab at an Exaflop, after China.

France

Among European countries, France is most notable for having a native supercomputing vendor, Bull (now a brand within Atos), that is capable of fielding an Exascale system in the next few years. The likeliest customer would be CEA, the French national atomic energy commission, though Bull could as easily sell its systems in other European countries. At one point, public statements implied that such a system might be deployed as early as 2020.

The Bull architecture leverages processing elements from Intel, but like Fujitsu in Japan with its Tofu interconnect (and Cray in the U.S., with its Aries interconnect), Bull is pursuing its own system networking technologies, called BXI (for Bull eXtreme Interconnect).

Russia

Russia is worthy of special inclusion specifically because it has a native vendor, RSC Technologies, that has stated it would be capable of fielding an Exascale system in a timeframe similar to other national initiatives, if it had a customer. The likeliest buyer would be Moscow State University, which currently hosts the most powerful supercomputer in Russia, but we know of no confirmed, funded plan or timeframe. The RSC architecture uses Intel processors and no custom interconnect. Within Russia, RSC competes with T-Platforms, which previously dominated the Russian supercomputing market, but which was set back greatly by a temporary U.S. ban on its use of American-influenced technologies.

CONCLUSIONS AND RECOMMENDATIONS

Supercomputing is vital not only to scientific research, which benefits the world, but also to the U.S. economy, in areas such as manufacturing, energy, pharmaceuticals, and finance, as well as to national security interests. For most of the history of the HPC market, the U.S. has not only been dominant in both the usage and the production of supercomputing technologies, but also it has had the ability to selectively limit the export of supercomputing capabilities to other countries if desired.

As supercomputing architectures are evolving and specializing, new paradigms need to be developed along with them. Exascale systems will require different programming, different management, and different stewardship than their predecessors. The hyperscale market will influence this path, as will the attendant rise of artificial intelligence. In short, the rules of the game are changing.

The U.S. should not underestimate the capability or potential of Chinese supercomputing initiatives. If the systems are built, many brilliant scientists will go to work to find innovative ways to use them for scientific research, which in turn begets advancement in other areas. Furthermore, the U.S. administration should see that attempts to limit Chinese development through export regulation have been counterproductive; the immediate result was to boost China's own domestic technologies.

While the U.S. still leads by far in the most straightforward market share metrics of production (vendors, supply-side) and consumption (buyers, demand-side), industry indicators show the U.S. is falling behind in the leading edge of advancement, and simultaneously losing the ability to rein in other countries via export control. Chinese leadership has apparently recognized the relationship between HPC and economic growth and has set forth on a program to drive the country into a leadership position. The best response to this new challenge is to continue if not increase national support for HPC at all levels.

The great strength of the U.S. is its economy and the strength of its private sector. National supercomputing efforts are essential to motivating investment at the high end. From that point, U.S. companies excel at seizing opportunities to drive markets forward.

Against these strengths, the top limitations to Exascale deployments are software and skills. If we do build a system, how will we use it? A key feature of the ECP is its emphasis on co-design, finding end-user stakeholders to collaborate on the design of next-generation supercomputing technologies, bolstered by government funding.

Beyond the continuance of ECP, we offer the following recommendations:

- *National initiatives in low-level software tools and programming models, together with stakeholders in industry and academia.* While individual applications must be tailored to specific architectures and may be of interest to a limited audience, there is some software functionality that would be of broader benefit. This includes programming models—the methodologies with which application engineers get their ideas to scale on large machines—and work on common tools and algorithms, such as math libraries, which benefit multiple applications. This type of work is not flashy—it is hard to get the public excited about linear algebra implementations—but the downstream benefit to multiple domains is a major payoff.

- *Government-funded partnerships between industry and academia.* The skills gap is a significant problem across the HPC industry. There is a scarcity of engineers, and much of the talent is more attracted to work in hyperscale industries. If more HPC skills were introduced in academic science and engineering programs, government programs could connect the students with organizations in need of their skills. Coursework could be designed such that the student is working on actual models as part of their course of study, at no cost to the participating company or organization. By the time the students join the workforce, they have learned valuable skills, become knowledgeable in a potential hirer’s products or process, and provided a valuable service, even if they choose to do something else. For participating organizations, they get access to HPC skills (albeit entry-level ones) with little to no cost or risk, and access to a pre-trained employee if they choose to hire.
- *Ongoing pursuit of next-generation technologies.* As noted throughout this statement, supercomputing is an industry of change. Beyond the leading vendors mentioned at various points, there are countless startups in pursuit of game-changing ideas, one of which might turn the industry on its head in five, ten, or 20 years.

Regardless of these recommendations, the HPC market will continue, powering new innovations and ideas around the world. Supercomputers today are close to a million times more powerful now than they were 20 years ago. In another 20 years, they could be a million times more powerful still. The leaders in supercomputing will be the ones that do not rest on their achievements, but rather continue to chase the next challenge over each new horizon.

APPENDIX A: QUESTIONS FROM USCC

Mr. Snell has submitted this statement in response to the following questions from USCC. Intersect360 Research Chief Research Officer Christopher G. Willard, Ph.D., contributed to this analysis. Data from Intersect360 Research surveys and forecasts has been included where relevant.

Question 1

Briefly describe the current status of high performance computing including both hardware and software and its applications. What is driving developments in these areas? How are artificial intelligence, next-generation semiconductors, deep learning, and big data playing a role in further advancements? How will advancements in high-performance computing affect a country's military capabilities and global competitiveness?

Question 2

Compare and contrast U.S. and Chinese technological capabilities and pace of innovation in high-performance computing. To what degree does Chinese high-performance computing demonstrate improvements over foreign systems and breakthroughs in technology? In what areas, is the United States still a technological leader?

Question 3

Briefly describe China's major industrial policies and plans supporting the development of its high-performance computing sector. How is the Chinese government implementing these plans and building its domestic capabilities in high-performance computing? What kinds of support (financial, regulatory, etc.) has the Chinese government provided to its domestic firms, research institutes, and universities? How much funding has the central and local governments allocated to support this sector? What is the role of technology transfer, licensing and other arrangements for sharing intellectual property, overseas investments (angel, greenfield, etc.), acquisitions (mergers and acquisitions or joint ventures), and recruitment of leading academics and overseas talent in enhancing China's advancements? Overall, how successful have those efforts been? What are the remaining challenges?

Question 4

Assess U.S. firms' operations in China and U.S. firms' business strategies to supply China's high-performance computing sector. What share of Chinese high-performance computing market do U.S. firms account for? How dependent are U.S. firms on the Chinese market? Which markets are the greatest opportunities for foreign market participation, and why? Which markets are the most restrictive, and why? Do foreign firms face any unfair or discretionary limitations (e.g., localization requirements, regulations, etc.) or technology transfer expectations? How are U.S. and other foreign firms coping with those restrictions, and what, if anything, should the U.S. government do about it?

Question 5

Assess the implications of China's high-performance computing development for the United States.

How will these developments affect U.S. global competitiveness and technological edge? How will these developments affect U.S. military superiority and U.S. power projection capabilities? What restrictions (export controls, etc.) has the U.S. government placed on U.S. firms competing in China's market, and are these restrictions necessary? How effective have these restrictions been? How should the U.S. government balance its commercial and national security interests in high-performance computing?

Question 6

Assess how the United States can maintain its strategic advantage in high-performance computing going forward. How has the U.S. government supported the development of high performance computing in the United States? How could the U.S. government help the United States maintain its strategic advantage in high-performance computing and ensure high-paying jobs in these fields and research and development centers are located in the United States?

Question 7

The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. Assess the implications of China's high-performance computing for United States. What are your specific recommendations for legislative and administrative action?

APPENDIX B: ABOUT INTERSECT360 RESEARCH AND ADDISON SNELL

About Intersect360 Research

Intersect360 Research was founded in January 2007 as a market intelligence, research, and consulting advisory practice focused on suppliers, users, and policy makers across the High Performance Computing ecosystem. The company operated as Tabor Research, a division of Tabor Communications, until it was purchased from the parent company by its two top executives, Addison Snell and Chris Willard, in 2009.

Intersect360 Research's deep knowledge of HPC, coupled with strong marketing and consulting expertise, results in actionable intelligence for the HPC industry—insights and advice that allow clients to make decisions that are measurably positive to their business. The company's end-user-focused research is inclusive from both a technology perspective and a usage standpoint, allowing Intersect360 Research to provide its clients with total market models that include both traditional and emerging HPC applications.

Intersect360 Research participates in the Advanced Computing Roundtable (previously the "HPC Advisory Committee") of the U.S. Council on Competitiveness, and partnered with the Council on its report, "Solve. The Exascale Effect: The Benefits of Supercomputing Investment for U.S. Industry." For "Solve," Intersect360 Research conducted both quantitative and qualitative research of HPC-using companies to produce a comprehensive report linking federal supercomputing investment to industrial innovation. The "Solve" report can be downloaded from the Council web site at www.compete.org/reports/all/2695-solve.

In addition to its market advisory subscription services, Intersect360 Research offers an array of client-specific services, including custom surveys, white papers, custom analysis, and both marketing and general business consulting. More information on Intersect360 Research is available at www.intersect360.com.

About Addison Snell

Addison Snell is the CEO of Intersect360 Research and a veteran of the High Performance Computing industry. He launched the company in 2007 as Tabor Research, a division of Tabor Communications, and he brought the company independent in 2009 as Intersect360 Research together with his partner, Christopher Willard, Ph.D. Under his leadership, Intersect360 Research has become a premier source of market information, analysis, and consulting for the HPC and hyperscale industries worldwide. Mr. Snell was named one of 2010's "People to Watch" by HPCwire.

Prior to Intersect360 Research, Mr. Snell was an HPC industry analyst for IDC. He originally gained industry recognition as a marketing leader and spokesperson for SGI's supercomputing products and strategy.

Mr. Snell holds a master's degree from the Kellogg School of Management at Northwestern University and a bachelor's degree from the University of Pennsylvania.

OPENING STATEMENT OF MARK BRINDA
PARTNER, BAIN AND COMPANY

MR. BRINDA: Great. Thank you, Commission.

At Bain & Company, in our technology practice, I focus on working with enterprises, global technology firms, on cloud computing, the impact it will have on their core business, how profit pools are shifting, and how they should impact and change their operations based on that. So I come at this question from a very commercial perspective.

I would say cloud computing, it is already a mature, relatively mature market when you compare it to quantum and some of the other emerging technologies that we'll talk about today.

I think it's helpful to start with a foundation of what is cloud? It's an overhyped, overused term, and, at its essence, it simply means the pooling of technology resources, making them available to anyone anywhere and the ability to scale the use of those up or down instantly. That is simply what this refers to. And it's not a completely new phenomenon. It's actually the evolution of prior technology innovation around just simple IT outsourcing. You've heard about grid computing, many other predecessor technologies that have given rise to what cloud is today.

So it's not as though this came from out of nowhere. It's actually been a well-established phenomenon that we've been heading in this direction for decades frankly. And there's already a $200 plus billion market around cloud computing in the world today. Growing very, very rapidly.

There are four segments of the market that I think are worth touching on here. One is infrastructure and platform as a service--the AWS, Amazon Web Services, Microsoft Azure type of an offering; software as a service, which is application software, like CRM, or office applications, email offered as a service; public cloud enabling infrastructure so the server, storage, CPUs, services and software that go into building clouds, public clouds; and private cloud infrastructure, which is the use of similar types of infrastructure to build private dedicated environments.

China overall--it's helpful to understand where we're coming from here. China overall spends a tiny amount of GDP relative to the United States on IT. And they spend a very tiny amount as a portion of that IT spend on software. They're underdeveloped in the markets for software and services, and that impacts their ability to grow and scale a cloud computing industry domestically.

The majority--two-thirds of the IT buying in China is driven by state-owned enterprises, and we'll talk about the relevance to cloud there. State-owned enterprises have legacy systems that are very monolithic and hard to migrate to the cloud without dramatic risk and cost. And so even if the state were not an actor, it would be incredibly hard to shift some of those systems into a cloud environment just by snapping your fingers.

If you look at the United States market, you've got a very large and dynamic emerging technology industry of consumer cloud players like Facebook, Google and the like that are driving innovation and adoption, and then there's just a broader private sector that is not driven by the state and has a much more flexible computing environment than many of the Chinese SOEs.

Let's look at the market for cloud. It's less than two percent of the total in China so China is a very small portion of the total cloud market today, and in, you know, five years time that could grow to three, four percent of the total, but the United States is driving over 50 percent of demand for cloud services across those four categories.

There's a pretty massive lead in terms of size and therefore focus from players in this space.

If you look at the infrastructure as a service market, that's where the local Chinese firms, Aliyun specifically, with over 50 percent share of the local Chinese market, is probably the most notable and most talked about player with global ambitions that is deemed kind of a threat to U.S. superiority in this space. They're less than a billion dollars by revenue annually.

Amazon Web Services, by comparison, is a $13 billion annual business. Microsoft Azure is the second player at two or $3 billion a year. And there are numerous other firms from Google, IBM, Oracle, Salesforce.com, that in that infrastructure as a service space are as big or bigger and growing rapidly relative to Aliyun.

That said, Aliyun is getting a direction--state-owned enterprises are being directed to leverage the Aliyun environment as much as possible given the massive spend that they drive on IT as a portion of Chinese spend in total. That is impacting Aliyun's ability to grow, and there's explicit preference for Aliyun over U.S. competitors that are active in the China market in this infrastructure as a service space.

So I think that is a threat, but as I said, these state-owned enterprises, they're mostly government, financial services, and telcos. That's two-thirds of the SOE IT spend--those three industries. Those are some of the slowest moving industries in any economy, and they have legacy systems that are incredibly, incredibly rigid and simply not movable to a cloud environment without, as I said, massive risk and investment.

In the software as a service market, this is a market where Salesforce.com, Workday, Service Now, and the like are some of the upstart leaders and Oracle, SAP, IBM, Microsoft are some of the legacy leaders.

The Chinese market for software is simply immature. As a share of total spend on IT, software is a fraction of what it is in other markets like the U.S., Brazil, around Europe, and as a result, you're talking about, if a SaaS market were to emerge in China, essentially creating spend on things that they don't spend on today. They're not spending money on package software at the rate that the rest of the world is, and so to have a SaaS market emerge, you're talking about creating essentially new spend.

Public cloud infrastructure, this is a market where actually Chinese firms supply a lot of the basic components. Simple commodity servers and storage actually come from manufacturing facilities. They call them original design manufacturers, ODMs, that are often based in China. This is a very low margin, nonstrategic business from an industry perspective, razor, razor thin margins. What you're really talking about is buying components from other providers--Intel, Qualcomm, and the like, assembling those together and then shipping them off to the source of that demand. And Chinese firms do well there. That is kind of a core capability.

The net of Chinese action in this space--I know I'm running up on time--they are building hubs for innovation around cloud in certain cities, making funding widely available for firms to build out cloud infrastructure. SOEs are trying to divert spend into cloud investments, and they've created some barriers for U.S. firms to enter the Chinese market.

But what will not change as a result of the 13th Five-Year Plan or any of the other initiatives, one, the vast majority of IT profits exist in industries where China is fundamentally weak in software, in services, in chips, microchips, CPUs that run the vast majority of cloud servers.

Second, there's been no demonstrated--there are no proof points of Chinese cloud being exported to the U.S. or any other market. Structural inhibitors, like I said, that the SOEs face, it's very hard to move those monolithic applications, and the environment around ODMs, where they do have a strong advantage, has been in place for decades so there's nothing really changing there.

In terms of recommendations, to wrap very quickly, one, I think our government can do much more to drive cloud adoption for its own internal IT consumption. There are instances of that happening, but we could do more with a concerted effort across government agencies to buy cloud solutions that would create innovation in industry.

Planning for an ODM supply disruption, that is something that I think we should, we should look into. If there were a disruption in the supply chain, as a result of a trade war or something else, that would impact U.S. cloud players and other ODMs.

We should look very carefully at Chinese entry into the U.S. market, either via M&A or organic efforts, and ensure that they're not buying assets that would be a strategic liability if owned by a Chinese firm.

Third, we should ensure that there are no anti-competitive actions by our own leaders. Amazon, Microsoft, Google and the like, they're emerging as an oligopoly in some of these cloud markets, and if that stifles innovation, that would be detrimental to industry, the cloud industry, overall.

And fifth, I think we need to ensure that our leading firms have access to talent, and some of that talent will be homegrown, some of it will not be, and if we through regulation on immigration restrict U.S. firms' ability to get the talent they need, that would be detrimental to their ability to innovate rapidly.

I'll pause there. Thank you very much.

PREPARED STATEMENT OF MARK BRINDA
PARTNER, BAIN AND COMPANY

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

Speaker bio:

Partner at Bain & Company, a global management consulting firm

Global Leader of Cloud Computing Center of Excellence within Bain's Technology, Media and Telecom Practice

Advised leading technology companies in both the U.S. and China on the impact of cloud computing on the enterprise and consumer technology ecosystem, including: impact on industry revenue and profit pools implications for growth strategy winning business model and operating model design alignment of customer segments to offerings and go-to-market approach acquisition strategy and organic investment plans

M.B.A. from the University of Chicago; B.A.s in Economics and Philosophy from New York University

The emergence of cloud computing is one of the most significant forces reshaping the technology industry and will play out over a multi-decade timeframe. We will explore the precise definition of the term cloud computing, but in simple language, the term refers to the pooling of technology resources for the purpose of enabling businesses or consumers to use as much or as little as they need, on demand, anywhere, anytime.

The shift from making fixed investments in technology resources that are owned and managed by the customer to the use of cloud resources that can be made available instantly and scaled up or down instantly is unlocking enormous innovation and efficiency within the global economy. Imagine if companies like Uber, Netflix or Instagram had to buy, install and manage all of the technology resources that deliver their service to customers. In order to support the rapid growth that they ultimately experienced, they would have needed to spend huge sums of money on technology before the business models were proven. Investors would have been far less likely to take a chance on a company with this profile. Instead, these companies were able to use cloud resources and spend virtually nothing on IT in the early days, and then let spend on IT grow in line with demand. Cloud dramatically lowers the bar for entrepreneurs to start a digitally-enabled business, and hence has unlocked a wave of innovation over the past decade.

Because of the broad economic importance of cloud, the Chinese government has made it a significant focus of the 13th Five Year Plan[1] and has launched initiatives like Internet Plus[2]. In this testimony, I will compare and contrast U.S. and Chinese technological capabilities in cloud computing, explore what steps the Chinese government has taken to support domestic firms, and lay out the broader implications of these policies for U.S. technological innovation.

This testimony is organized as follows:

Definition of cloud computing and segments of the market for cloud solutions

Overview of China's cloud landscape

Comparison of cloud in China and U.S.

Implications and recommendations

Definition of cloud computing and segments of the market for cloud solutions

"Cloud computing" is an overused and overhyped term that has lost some of its meaning over the past economic cycle. Companies associated with cloud have seen dramatic valuation growth, hence every company wants to jump on the bandwagon, regardless of the degree to which their offerings actually leverage or enable a true cloud architecture.

The National Institute of Standards and Technology outlines a specific and practical set of requirements for any technology environment to be accurately labeled "cloud"[3]:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)

---

1 Full version of 13th FYP: Full version of the 13th FYP in Chinese can be accessed here (English version not yet available as of April 20th): http://news.xinhuanet.com/politics/2016lh/2016-03/17/c_1118366322.htm

2 Summary of Internet Plus plan: http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm

3 National Institute of Standards and Technology definition of cloud computing: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

There are many computing models that share some of these characteristics and have been around for decades. In fact, cloud is not a dramatic new innovation but a breakthrough that emerged from a steady evolution of computing models. Utility computing, grid computing, virtualization, IT outsourcing and other technologies and delivery models have been enabling businesses to do some of these five elements, just not all of them as part of a single solution. Consequently, many legacy technology companies that have built a business in one or another of these predecessor computing models are now labeling everything they do "cloud", which has confused the market and made it difficult for customers and industry participants to distinguish true cloud solutions.

The NIST goes on to outline three cloud service models (Software as a Service, Platform as a Service, and Infrastructure as a Service) and four cloud deployment models (Private Cloud, Community Cloud, Public Cloud, and Hybrid cloud). For the purposes of this discussion, I will focus on four discrete intersections of these service and deployment models which collectively comprise the relevant cloud market segments:

Infrastructure and Platform as a service (IaaS/PaaS): cloud-delivered servers, storage, information management software and application development/operations tools sourced from a shared, 3rd party-owned data center environment

Leading cloud players: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM Bluemix, Force.com, Aliyun (Note: AWS is the global market leader with ~40% share, followed by Microsoft with just ~5% share)

Leading traditional computing players: Dell, EMC, Cisco, IBM, HP, Microsoft, Oracle, VMWare, Huawei, Lenovo

2016 global market size: ~$20B[4]

2015-20 market growth rate: ~25-30%[4]

Software as a service (SaaS): cloud-delivered application software (e.g. office productivity, customer relationship management, enterprise resource planning, human resource management) sourced from a shared, 3rd party-owned data center environment

Leading cloud players: Salesforce.com, Workday, ServiceNow, Microsoft, SAP, Oracle

Leading traditional computing players: Microsoft, Oracle, SAP

2016 global market size: ~$55B[4]

2015-20 market growth rate: ~15-20%[4]

Public cloud enabling infrastructure, software and services: components, software and services required to build a cloud environment, including processors, servers, storage, networking equipment, infrastructure software, data center power and cooling equipment, and related services

Leading cloud players: Intel, Dell, HP, EMC, Cisco, Pegatron, Compal, Wistron, Quanta

Leading traditional computing players: same leaders

2016 global market size: ~$70B[4]

2015-20 market growth rate: ~12-15%[4]

Private and hybrid cloud solutions: cloud infrastructure and platform environment that is partially or entirely dedicated to a single company or customer; can be built and run by an enterprise for its own consumption or owned/managed by a 3rd party operator

Leading traditional computing players: Dell, EMC, Cisco, IBM, HP, Microsoft, Oracle, VMWare, Huawei, Lenovo

Leading cloud players: IBM, Microsoft, VMWare, Rackspace

2016 global market size: ~$7-20B[4]

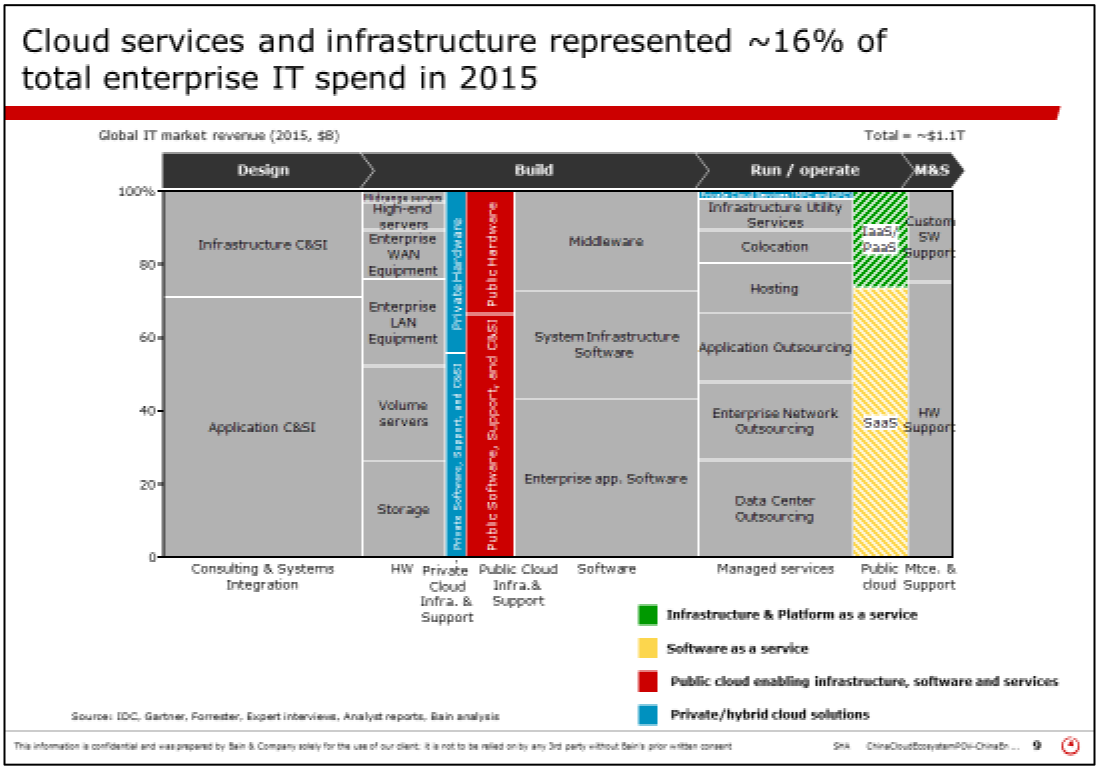
2015-20 market growth rate: ~25-35%[4]

For context, these markets collectively represent ~$180B of the $1.1T global market for enterprise IT. They will drive roughly 60% of the total growth in the technology market from 2015-2020.[4] Thus, while

---

4 2016 “Bain Global Cloud Computing Point of View”, which integrates primary and secondary data from the following sources: Gartner, IDC, Forrester, Bain & Company survey of IT decision markets, literature searches on publicly disclosed statements about cloud usage

it is important to keep in mind the enormous volume of technology spend that is not yet driven by the cloud, the technology industry and governments of countries with a large tech sector recognize the role that cloud will play in future growth and are appropriately focused on creating an environment where domestic firms can flourish.



Overview of China's cloud landscape

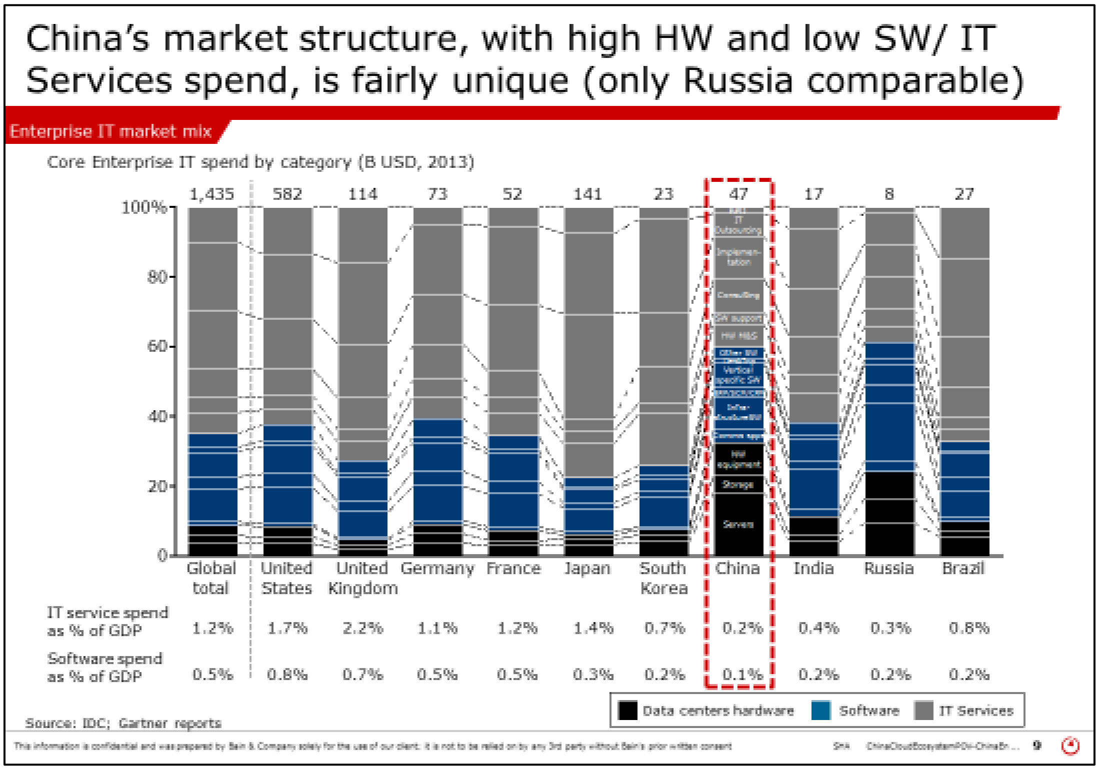
To understand the current state of cloud computing in China, it is essential to start with an understanding of the broader technology market in China. Specifically, a) What types of IT offerings do Chinese companies buy? b) What firms spend that money?, and c) What has been the Chinese government's posture toward both domestic and U.S. technology providers?

The Chinese market for enterprise IT looks quite different from other large economies. First, the total amount spent on IT is significantly lower as a share of GDP. In 2013, the US market for IT was equal to 2.8% of GDP, the U.K. market was 3.0% of GDP and the China market only 0.5%. This is not just an emerging market phenomenon. The Brazilian IT market, for example, was equal to 1.2% of GDP.[5]

---

[5] 2013 "Bain China Cloud Ecosystem Point of View", which integrates primary and secondary data from the following sources: Gartner, IDC, Forrester, Euromonitor, and expert interviews with industry participants

The reason China spends so little is simple: the market for software and services are disproportionately small relative to the market for hardware. Software piracy has long been a common practice for Chinese enterprises and the use of 3rd parties to outsource the build, operation and maintenance of IT is still not standard practice, particularly with State Owned Enterprise.



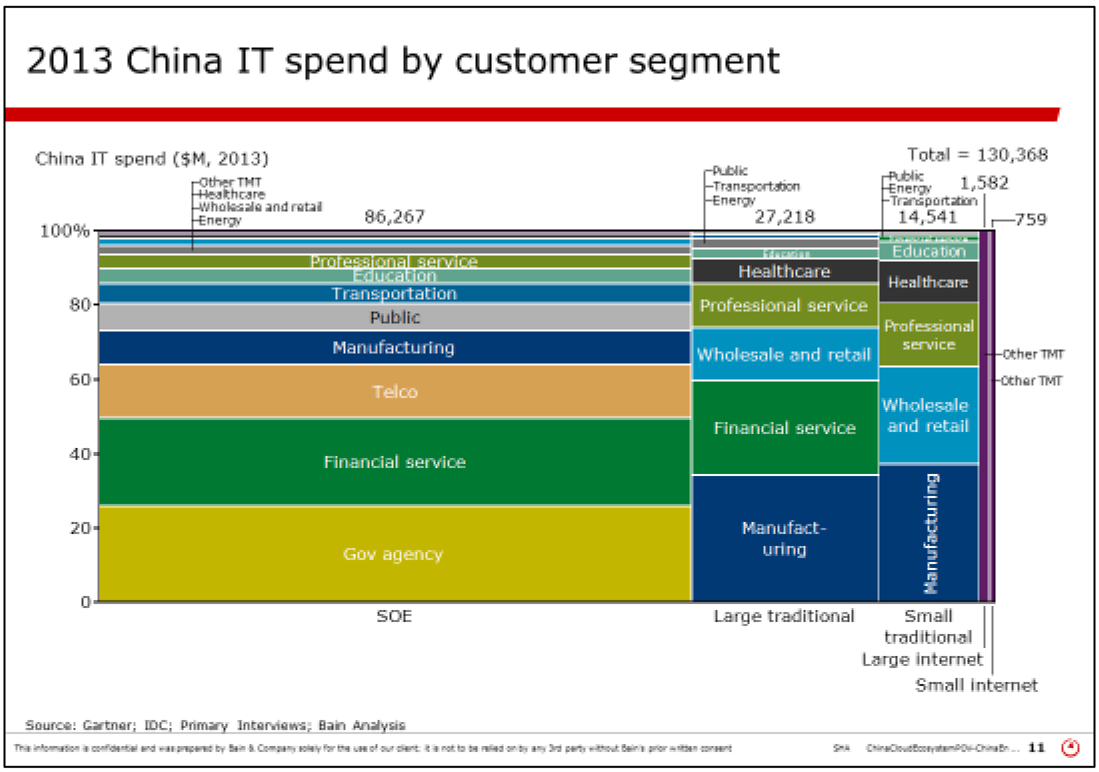
To the second question on who buys IT in China, the answer is that state owned enterprise (SOEs) drive an enormous share of spend. Two-thirds of total IT spend is driven by SOEs, a share so large that the posture of this segment toward the cloud will effectively determine the course and speed of cloud evolution in China.

Historically, SOEs have been very slow to adopt cloud solutions. There are several factors at play here. First, they are large, legacy organizations with a mature IT environments that are both costly and risky to move into a cloud. This fact will not change, regardless of the government posture toward cloud. With few exceptions, legacy systems that run mission critical applications have not moved to the cloud in any economy.

The second factor at play is the business mix of the SOEs. They are over-represented in financial services and telecom, and also include government agencies. All of these sectors of the economy tend to have IT decision makers with more conservative attitudes toward adoption of new technologies, regardless of geography. This is due to data sensitivity, systems rigidity and the mission critical nature of services provided.

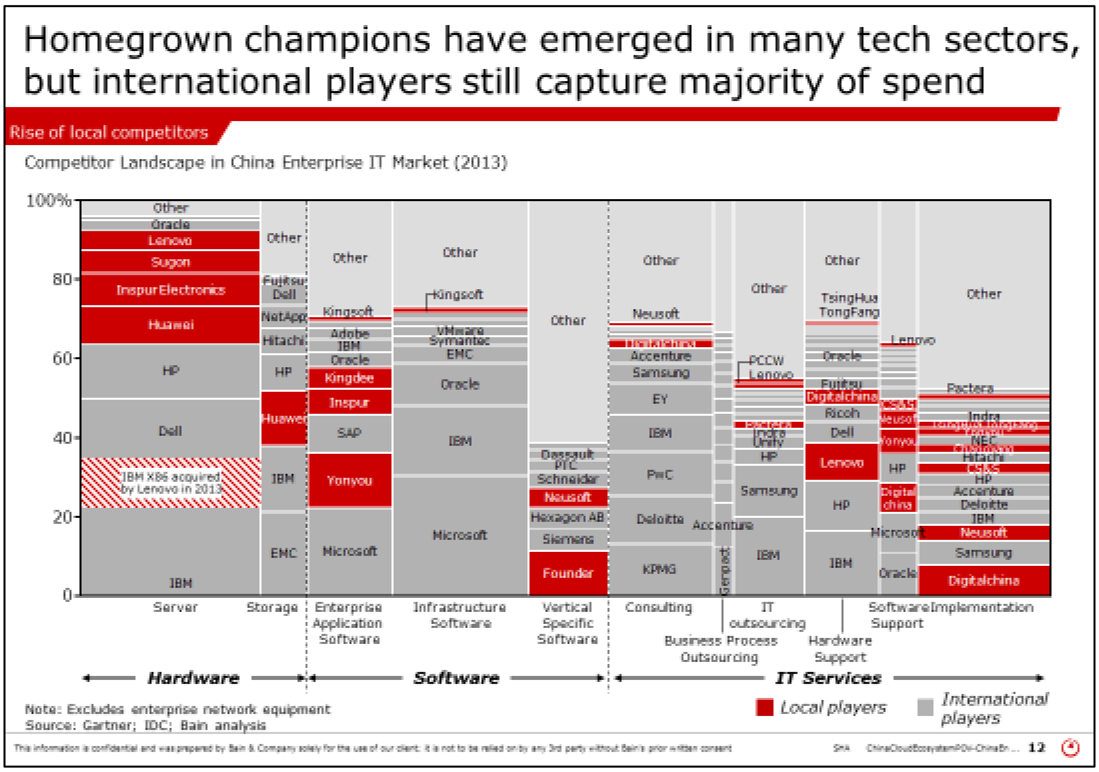
The third factor at play is the role that the government plays in setting the IT agenda at SOEs. In 2014, when Bain conducted extensive primary research into the attitudes toward cloud of different customer segments, SOEs had the lowest share of spend on cloud and the vast majority of that spend was on company-owned/managed private clouds. This is the factor that the government has started to change and is the wildcard in the Chinese cloud market.

Since 2014, the government has made clear the importance of digitization and investment in cloud technology through initiatives like Internet Plus and the 13th Five Year Plan. While the literal translation of these programs are vague, they have quite clearly begun to impact the posture that SOEs have toward cloud, and public cloud in particular. While there has not been a dramatic shift of investment from traditional IT to the cloud at SOEs because of the other factors cited, there has been an increase use of public cloud for new applications, in eCommerce, online customer engagement, and big data, for example.



The final issue to understand with respect to the IT environment in China is around the government's treatment of domestic players vis-à-vis U.S. and other international technology companies.

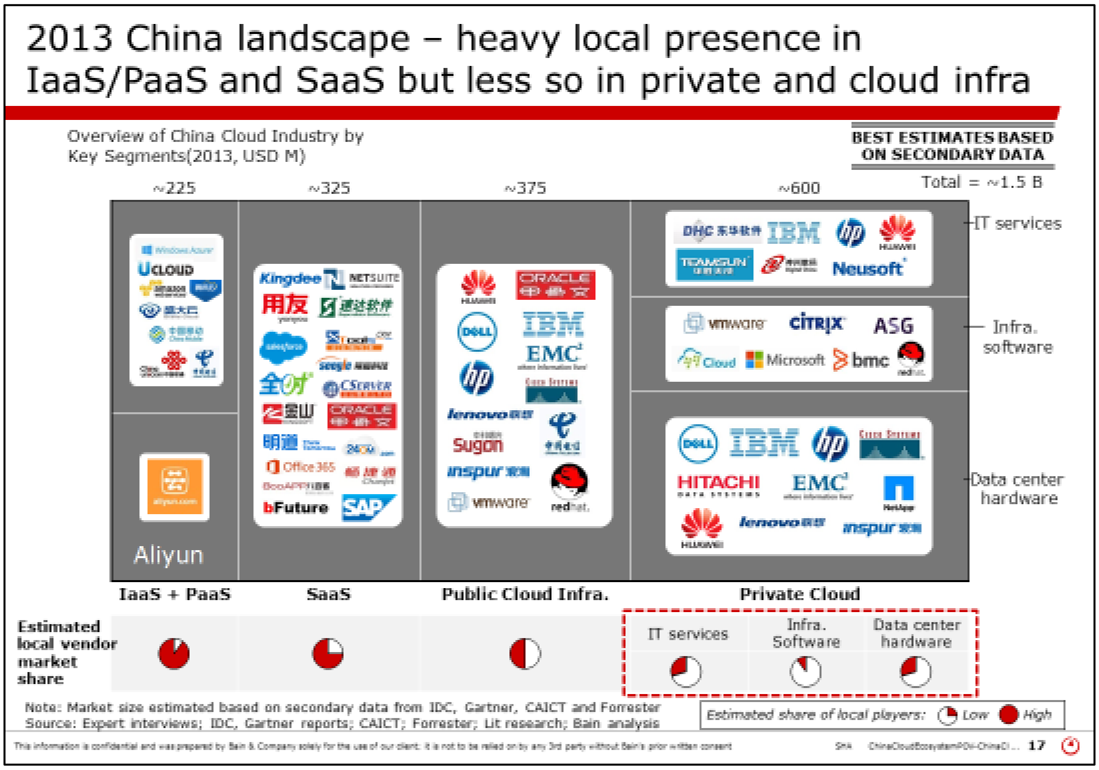
A look at the market share of local vs. international players across the IT landscape reveals that international players make up a significant majority of the market.[5] Despite local participants in almost every category, Chinese companies, including SOEs, have widely used U.S. technology. While there are factors at play in the market for cloud that will drive higher share for Chinese firms in some market segments, international players will continue to play a major role in the Chinese IT market, particularly in categories like CPUs, infrastructure software and IT outsourcing where no commercially viable, scale local alternatives exist. Players in these categories will all capture share of the Chinese cloud market as well.



With that backdrop, we can now look at the current state of the cloud market in China and the role that the government has played in accelerating investment and growth.

In 2013, the total Chinese market for cloud solutions across the four key categories was \$1.5B. This represented just ~1-2% of the total global cloud market.[5] While Bain expects the Chinese market to rise to between 2.5-4% of the total global cloud market by 2020 and grow to a total of \$13B-19B[6], the market will remain relatively small for the near-to-medium term. The factors outlined above are at the root of both why the market is relatively small and why it is growing more rapidly.

[6] 2016 “Bain China Cloud Ecosystem Point of View”, which integrates primary and secondary data from the following sources: Gartner, IDC, Forrester, expert interviews with industry participants and a Bain & Company survey of IT decision makers in China



If we look at the four key segments of the market, the one that is most dynamic and where local players have the greatest share is the IaaS/PaaS market. This is a service that does not face significant language or culture barriers upon export and where there are fewer entrenched legacy players in many markets. Consequently, firms in this space have high hopes for international expansion.[7]

The Chinese cloud company that gets by far the most attention is Aliyun, an IaaS/PaaS provider owned by Alibaba that is considered "the Amazon Web Services of China". Aliyun is growing at >150% per year on a base of ~$800M-1B revenue in 2016. Wall Street estimates expect the business to reach $8B-$9B[8] by 2020. Aliyun has >50% market share in China now, up from ~40% in 2013.[6]

There are numerous reasons for its local dominance. Part of the story is similar to the one we have seen in Chinese consumer web services (e.g. WeChat, TenCent, RenRen, Baidu) where early government protections allowed a local player to achieve scale and meaningfully differentiate vs international competitors. When barriers are lowered, the local firm is able to survive foreign competition. In IaaS/PaaS, this protection came in the form of onerous rules about foreign entry that require international competitors to apply for a license to compete and take on a local partner with a majority

[7] Jack Ma, founder of Alibaba, meets with President Trump in January 2017 and discusses expansion, including cloud: http://www.reuters.com/article/us-usa-trump-alibaba-idUSKBN14T1ZA

[8] Multiple Wall Street analysts forecast Aliyun growth within the broader Alibaba portfolio, including Goldman Sachs (https://static.businessinsider.com/amazon-web-services-threat-alibaba-goldman-sachs-2016-8) and Morgan Stanley (http://unique.finance/3-reasons-why-alibaba-stock-is-a-good-buy-now/)

stake.[9] While Microsoft Azure and AWS are both present in China, neither has been able to achieve the share position they have globally or in the US.

In terms of technology features and functionality, Aliyun is still not at full parity with AWS and Azure, but is close on most core services like compute, storage, and database. What Aliyun has done very successfully is win with the two most critical segments of the cloud market: SOEs and local tech-centric start-ups.

With SOEs, the story is straightforward: when a public IaaS/PaaS solution is appropriate for a given IT workload, there is a clear preference for local firms and Aliyun in particular. The fact that SOEs are leveraging the public cloud more, in line with government directives, including Internet Plus and the 13th Five Year Plan, is a direct boon for Aliyun. In Bain conversations with SOE buyers, they express a clear preference for Aliyun whenever there isn't an obvious reason why a more full featured solution from a larger global player is required.

With tech-centric start-ups, the story is more about a true advantage that Aliyun has created. The company has developed a comprehensive suite of offerings that a small web business would want, inclusive of business financing, turnkey eCommerce, marketing automation, and business productivity software. These offerings go well beyond what AWS or Azure can offer in China and leverage the local dominance of the Alibaba marketplace.

Looking at the SaaS market in China, we see that it is subscale relative to the global SaaS market – it is ~1.5x the size of IaaS/PaaS while the global SaaS market is ~3x the size.[4] [5] This is due to the fact that Chinese firms are unaccustomed to paying for software. In other markets, SaaS spend is capturing share from traditional application software while in China, it is typically net-new spend for a company.

A wide range of local players have emerged in the Chinese SaaS market, in large part because global software players have been slow to invest in creating offerings with local language requirements and that are tuned for the Chinese economy. Those international firms that have made a play are often following multinational corporations that have built or acquired Chinese businesses. The flip side of this story, however, is that Chinese SaaS players are very unlikely to succeed beyond the local market and potentially other geographies of significant Chinese influence.

The private cloud and public cloud infrastructure markets in China look much more like the markets for traditional IT infrastructure hardware and software. U.S. players have much stronger solutions and have deep incumbent relationships with local players. Aliyun, for example, uses a significant amount of gear from HP, Dell and other branded equipment manufacturers.

That is not to say that local firms are not taking share and growing rapidly; they certainly are. There are two flavors of Chinese players in the markets for cloud infrastructure: a) local "branded" infrastructure makers like Huawei and Lenovo that sell a specific set of pre-designed infrastructure solutions which are built specifically for clouds and b) local "white box" manufacturers (Original Design Manufacturers or

---

[9] Overview of ICP requirements for foreign firms in China: https://webdesign.tutsplus.com/articles/chinese-icp-licensing-what-why-and-how-to-get-hosted-in-china--cms-23193

ODMs) that do not design equipment but will build any configuration that a customer wants at razor thin margins, so long as the volume is sufficient to justify the order.

Chinese branded equipment makers are still not at parity with the global leaders like Dell, HP, IBM, and EMC and while they have closed the gap, the bar keeps getting higher and the leaders are spending huge sums to maintain a sizeable lead. The gap is really around the embedded software and surrounding support that U.S. leaders provide, both areas where China is not stocked with the local talent required to catch up. In some circumstances, Huawei and Lenovo win contracts for private cloud deployments within SOEs, but there is still a gap with global vendors. The gap is closing, however, driven in part by SOE preference for local vendors.

The one exception where Chinese branded infrastructure players have managed to build a significant global presence is in telecommunications equipment (the gear that telcos install to build wireless networks) where Huawei and ZTE to a lesser extent have taken significant share. While this is not directly a part of the cloud market, it is work noting because Huawei in particular has leveraged this business into a smaller position in networking equipment (i.e. Cisco's core business) and an even smaller position in servers and storage. They are trying to build a cloud infrastructure business and even an IaaS/PaaS business but have had limited success outside of China to date. Huawei, however, is the biggest threat to U.S. branded equipment makers. Lenovo would be the second most significant following its acquisition of IBM's low-end server business, but is still less competitive in either the private cloud and public cloud infrastructure market.

The market for white box equipment is a very different story. Players like Inspur, Wistron, and Quanta, have built significant global businesses selling equipment to cloud providers. This market very directly leverages China's core strength in manufacturing, supply chain and logistics. This is really more of a manufacturing business than a technology business. There is virtually no IP included in the equipment that these vendors offer. They are simply a low cost way for companies like AWS, Facebook, and Google, as well as branded equipment makers like Dell, EMC and HP to build infrastructure that they have designed themselves. It is similar to the relationship between Foxconn and Apple.

While this is not a particularly attractive business, it is a vital one, not just to cloud but to the entire IT infrastructure market. There are no scale alternatives to outside of China and Taiwan. Should a trade war break out or some other global disruption occur that severs the link between U.S. cloud providers and these suppliers, there would be a significant and sustained disruption in the global IT market.

I will conclude comments on the state of cloud in China by summarizing the impact of government policies and plans on the Chinese cloud market and on the global competitiveness of both Chinese and U.S. cloud providers.

I do not profess to be an expert at deciphering the true meaning of Chinese government proclamations. The relevant comments around cloud computing in policy statements are often vague and not clearly indicative of action. What is clear to me is that Chinese policy is having the following major impacts:

Select cities have been designated as cloud hubs, either by the center or by local leaders, in order to accelerate growth of the domestic digital business and IT vendors

Funding for cloud-related infrastructure buildout is very readily available, to the point that this is not a constraint on growth

Decision makers at SOEs have been steered to digitize their businesses and, where sensible, to leverage local public cloud solutions to do so

International IaaS/PaaS players have been saddled with significant barriers to entry, which has created a protective bubble within which local firms have achieved scale

What policy has not impacted are the following fundamentals of the Chinese cloud market and technology business more broadly:

Vast majority of technology profit pools are in sectors that the Chinese firms are fundamentally not positioned to compete in due to a lack of local talent: CPUs, infrastructure software, and services drive >70% of technology profits and Chinese firms are all virtually absent from these sectors, even in Chinax

While local protections have enabled IP-driven cloud businesses to achieve scale locally (i.e. IaaS/PaaS, SaaS) they have had no success exporting their offerings to date and there are few examples of Chinese success in other attempts to export IP-driven technology

Large, legacy businesses are slow to adopt cloud for structural reasons and two thirds of IT spend in China is driven by these kind of firms

White box infrastructure, the cloud segment where China is globally competitive, is part of a broader segment of custom technology infrastructure manufacturing where China has long been a global leader

Comparison of cloud in U.S. and China

The U.S. is by far the global leader in the cloud market. U.S. companies lead every cloud category across IaaS/PaaS, SaaS, private/hybrid cloud and cloud enabling infrastructure and make up at least 4 of the top 5 providers in every cloud market. The one exception being SaaS where Germany's SAP has a #3 position but no other non-U.S. company is in the top 10 (and even SAP is headquartered in the US with an American CEO).

In this section, I will explore each cloud segment from the perspective of U.S. vendors to understand what they are doing to achieve a competitive advantage, how they are taking that to the Chinese market and what success they are having.

First, let's discuss the IaaS/PaaS market, where AWS is the largest global player with a $12B 2016 business that is larger than all of the Chinese cloud market. The business has a technology lead that is insurmountable in the near term. The AWS cost per unit is lower than any other player, enabling them to earn 20%+ EBITDA margins and reinvest in widening their lead on bringing innovative new services to market. They achieved this position by being first to market, hiring and retaining incredible talent, and continuously investing in growth. The untapped potential to capture demand currently served by traditional data center equipment is vast, many times the current size of the business. There are also many large adjacent markets, most notably SaaS, where AWS has yet to focus.

The #2 player in the IaaS/PaaS market is Microsoft Azure, now a $2B+ business growing >100% y/y, even faster than Amazon. Microsoft has the advantage of a huge base of developers and an enormous installed base of infrastructure software that it has managed to retain and begin transitioning to the cloud. Of the legacy infrastructure HW and SW providers, Microsoft is the lone success story. Hardware vendors, including Dell, HP and Cisco, as well as other infrastructure SW players, notably IBM, have struggled to take share or have failed altogether. By making the Microsoft cloud experience for developers comparable to that of its legacy offerings, but with the flexibility, self-service and other attributes of the cloud, they have become the de-facto cloud provider for the millions of "Microsoft shops" out there.

AWS and Microsoft are threatening to make the global IaaS/PaaS market a two horse race. Many large tech incumbents, including Dell, HP and Verizon, have thrown in the towel on this business after investing significantly. Others, including IBM, Google, and Oracle, are still investing but struggling to keep pace. There is a "long tail" of subscale players, both in the US and internationally who predominantly serve small and mid-size customers with minimally complex needs. However, no international player outside of Aliyun is close to becoming a scale global player.

As previously discussed, Aliyun has achieved near-parity on some competitive dimensions and has actually differentiated on other dimensions that resonate with the Chinese market. While Aliyun has yet to make any significant headway internationally, the business certainly has ambitions to play in both the U.S. and other markets where Chinese technology firms have been successful. Jack Ma has reportedly met with President Trump and the company has considered U.S.-based M&A.[7] The U.S. market will be a challenge. There are no obvious scale acquisition targets and the likelihood is low that a new entrant from China will organically achieve scale in a mature market where the #1 barrier to purchase is data privacy and security.

The more likely scenario is that Aliyun will win in international markets where other Chinese companies have been successful: Southeast Asia, Africa, the Middle East, Eastern Europe. These markets are nascent, however, and total IT spend is minimal. It is likely that the domestic market will be the largest one for Aliyun for the foreseeable future

In the global market for SaaS, U.S. firms are also far ahead and hold a defensible long term position. There has been substantial consolidation in the SaaS market over the past decade, driven both by M&A activity of large software incumbents, particularly Oracle and SAP, and the transition of legacy software franchises to a cloud-based delivery model. Some scale new players have emerged, notably Salesforce.com and Workday, and many other smaller, fast growing competitors exist.

The U.S. has long had a lead in the market for software and the transition to cloud builds on and reinforces the factors that have made the U.S. a leader. A large, highly skilled developer ecosystem is the first essential criteria. Innovation hubs like Silicon Valley where developers, venture investors and acquirers are in close proximity are a second essential criterial. A large domestic market for software is a third criteria – without customers, it is hard to build a successful business.

On each of these dimensions, particularly the third, the U.S. holds a sizeable lead vs. China. The U.S. market for software is ~17x that of China's. The ratio of spend on SW to spend on infrastructure that it runs on is 5:1 in the U.S. and only 1.25:1 in China. It will take well over a decade for the software market in China to mature to scale that an economy of its size should support. When thinking about global competitiveness of Chinese SaaS firms, this difficult-to-influence factor will be a significant headwind. Beyond this, there is friction around adapting software to local language and processes that largely does not impact the Chinese hardware companies that have had international success. Finally, there are the same concerns about data privacy and security. For these reasons, I am skeptical that government declarations on innovation hubs and encouragement of developer education will lead to globally competitive Chinese SaaS firms that rival those in the U.S. anytime in the next decade.

The last two segments, private/hybrid cloud solutions and public cloud enabling solutions, are areas where U.S. firms are marginally more exposed, though even here the U.S. competitors have a sizable lead in most sub-categories. There are a number of sub-segments in these markets where the U.S. has no credible rival in China and Chinese demand will continue to be filled by U.S. firms. Broadly speaking, these are areas where the IP content of the offerings are high, e.g.: CPUs that go into cloud infrastructure, cloud infrastructure software, "cloud in a box" systems (certain types of what are called converged systems in IT jargon).

These are markets where decades and hundreds of billions of dollars of accumulated demand give the U.S. firms in these categories a massive edge. For example, since 2006, the Chinese government has backed an alternative CPU architecture from the Jiāngnán Computing Lab. After more than a decade of sustained investment, there is no enterprise-ready CPU available from a Chinese manufacturer. Chinese clouds, just like those in the U.S., run on Intel x86 processors. The reason that all of this investment has not led to an alternative is that the entire enterprise IT ecosystem is designed to run on CPU architectures that only U.S. firms are capable of designing. Only in a completely closed system with entirely proprietary software and surrounding components could a home-grown alternative be viable, which is what we have seen in the supercomputer space where the Sunway TiahuLight has become the world's fastest supercomputer leveraging a the CPU architecture from the Jiāngnán Computing Lab.

This is just one example of a market where there is significant IP content that an entire ecosystem has been built around and it is not enough to simply create an alternative. Moving an entire economy from one IT standard to another is far harder than building a prototype that works in a lab. We are still more than a decade away from a world where Chinese clouds can run entirely on home grown componentry instead of CPUs, software and hardware from the U.S.

The segment of this market where the U.S. is not only less competitive but non-competitive is that of manufacturing custom designed hardware at scale. This is a market where the Chinese and Taiwanese lead globally and U.S. firms have not attempted to compete. Profit margins in this business are razor thin and global supply chains for many of the heaviest components (e.g. server chassis, motherboards, SSDs) originate in Asia, advantaging Chinese firms relative to a potential U.S. entrant.

There are significant geo-political risks that the broader U.S. technology market is exposed to as a result of this dependency; cloud certainly shares that exposure. This is not a market where U.S. firms should play based on economic fundamentals alone. However, this exposure creates a point of strategic weakness that could be exposed in trade negotiations or other conflict with China, particularly if Taiwan is involved. The damage that the U.S. would incur from a shock to the IT hardware supply chain would be much larger than the shock that China would experience, creating a potential point of leverage.

Implications and recommendations

Against this backdrop, where U.S. cloud firms have a commanding lead globally, where there are significant challenge facing Chinese firms who would aim to compete on a global basis and where Chinese firms are still significantly dependent upon technology from U.S. firms to build and run cloud environments, I would offer the following recommendations:

Encourage aggressive use of cloud by government agencies – The U.S. Government represents a sizeable share of domestic IT spend, enough to impact the pace of innovation in some sectors of the cloud market. There are notable examples where the Government has embraced the cloud (e.g. the CIA use of AWS for select applications) but use has been slower than other industries. The stated rationale for the slow pace of migration is around data privacy and security. However, this is a red herring.

The U.S. Government represents such significant spend and such an important reference for cloud providers that they will invest heavily to co-create solutions tuned for the unique needs of government. The AWS-CIA example is a perfect one. That solution was entirely custom built for the CIA, but by using it, AWS gained enormous credibility in the market and has substantially changed the perception that it is an offering just for startups on a budget.

Another area where the government could impact innovation and adoption in the market is around private cloud. A multi-billion dollar investment in private clouds, which would enable government agencies to be far more agile on how they build and scale custom software, would go a long way toward addressing an innovation gap in this space. Enterprises want private cloud but for the right price. Today’s private cloud solutions are still expensive and complex. But a scale investment in private cloud, coordinated across government agencies, would drive considerable investment in innovation that could then be taken to the private sector.

Collaborate with industry on a supply chain disruption mitigation plan – I have highlighted the structural risk stemming from dependency on Chinese and Taiwanese ODMs. There are many plausible scenarios where Taiwan the flashpoint in a U.S.-China conflict and the global IT hardware supply chain is severely disrupted. This is a risk that would certainly impact the broader technology ecosystem, so I would not be surprised if there is a mitigation strategy already in place. If there is not, the government and the largest ODM customers, which would include AWS, Facebook, Google, Apple and others beyond the legacy IT hardware players, should collaborate on a mitigation plan.

Maintain a very high bar on Chinese acquisition of U.S. cloud companies and on IP-sharing ventures between U.S. and Chinese companies – Chinese technology companies have access to investment and there are many U.S. cloud technology firms, some of which are small, that could be bought. Any potential acquisition should continue to face significant scrutiny, even if small in terms of revenue. Similarly, there should be significant scrutiny of IP sharing agreements between U.S. and Chinese cloud firms where there could be a short term boon for a U.S. company seeking access to the Chinese market.

Monitor anti-competitive activity by cloud leaders to ensure an environment where disruptors can continue to enter the market – In both the IaaS/PaaS and SaaS markets, competition is on the decline. AWS and Azure are the largest players in IaaS/PaaS and are gaining share. SaaS is not a monolithic market, but the aggregation of many application categories where SaaS has taken hold. Within these categories, software incumbents have taken share by aggressively acquiring independent SaaS players. Ensure that the FTC has appropriately defined the competitive landscape and is monitoring anti-competitive activity. This has not stifled innovation to date, as evidenced by start-ups like Docker and Digital Ocean that would like to unseat AWS, but could become an issue over time.

Evaluate and reset barriers to Chinese IT participation in U.S. markets to ensure equivalent impact vs. Chinese barriers to U.S. firms – U.S. firms have not played on a level playing field in the Chinese market and have lost share that they would have surely gained in an entirely open market. Trade regulators should have a view on what the economic impact of these policies has been on U.S. cloud providers and ensure that an equal response is in place to advantage U.S. firms domestically.

Grow the cloud-enabled talent pool in the short term through immigration policy and over the long term through sponsored training programs – There is a sizeable talent shortage when it comes to building and managing cloud environments. In a Bain study completed in 2016, cloud-enabled employees were cited by IT decision makers as the leading technology talent gap, ahead of data scientists, devops, or specialized programing language proficiency.

Cutting off the supply of cloud-enabled talent from regions that have it would have a very negative near term impact. In fact, the door should be opened even wider to satisfy the short term demand for this talent.

Over the longer term, cloud-enabled IT professionals can be home grown more rapidly through state sponsored education programs. In the 1990's, government-backed loans enabled rapid growth of Microsoft- and Cisco-certified professionals who were essential to the growth of the technology architecture of that era (client-server). We need the equivalent of that now around AWS and Azure-enabled professionals.

The U.S. cloud industry has flourished with limited government support or intervention. The "do no harm" principle is actually the most important one. Elected officials need to take appropriate caution when setting technology policy, for there can be far reaching implications that go well beyond the objectives of a piece of legislation. The cumulative impact of all these actions could be wiped out by one well-intentioned but poorly executed law around cybersecurity, net neutrality, or any number of broad-reaching technology issues that the Government has recently waded into.

OPENING STATEMENT OF JOHN COSTELLO
SENIOR ANALYST FOR CYBER AND EAST ASIA, FLASHPOINT

MR. COSTELLO: Good morning to the commissioners and thank you for inviting me and giving me the opportunity to speak on quantum information science. It's a fun topic, and I look forward to talking about it.

We are in the midst of a second quantum revolution, and one that enables disruptive new technologies that have potential to change long-held dynamics in commerce, military affairs, and strategic balance of power.

Within the foreseeable future, the realization of quantum computing will result in revolutionary computational capabilities with wide-reaching implications. The employment of quantum cryptography can create quantum communication systems that are theoretically unbreakable and unhackable. Quantum sensing enables the capability to conduct extremely precise accurate measurements for new forms of navigation, radar and optical detection.

These are still nascent technologies, but they are emerging, and they're emerging very quickly. Under leadership of Xi Jinping, China's prioritization of quantum information science has intensified substantially. From the Chinese leadership's perspective, quantum technologies have become integral to national security, particularly information security, and to strategic competition.

Chinese researchers have consistently drawn a direct line from the Snowden links to China's development of quantum technologies. Additionally, China believes that this is one area where the leapfrogging strategy will pay off as United States' dominance in information technologies today don't necessarily confer an advantage in this critical technological sector.

Quantum information science's high level prioritization has been found in China's 13th Five-Year Plan where it's listed as a key area of research. This is followed in the 13th Five-Year National Science and Technology Innovation Plan and National Key R&D Plan.

The progress of China's program is most obvious in the field of quantum encryption, an area where it appears it leads the United States. Last year China launched the world's first quantum satellite, Micius, or Mozi, a joint project between China and Austria. The technology would allow theoretically unhackable communications over long distances. China is looking to scale this up globally by 2030.

Domestically, China is building a nationwide quantum key distribution network with the first trunk between Beijing and Shanghai to be completed this year. Other efforts in quantum information science on the part of China are more muted and lag behind U.S. efforts. China's quantum computing efforts, for instance, are still fairly nascent, and the biggest initiative they have is between Alibaba and Aliyun and the Chinese Academy of Sciences. Comparative efforts at IBM, Google, and other western firms are sort of pretty far ahead.

China has claimed to have tested a quantum radar, which can supposedly defeat stealth, although it's been met with skepticism. It's unclear if China's approach with a combination of state-level R&D investment, international cooperation, and overseas scholarships can translate equal success to quantum computing and sensors that they have had in encryption so far.

Reports from the Massachusetts Institute of Technology in 2015 and the White House last year note that the U.S.' lead on quantum information science is slipping. They signaled a lack of consistent funding, coupled with lack of--excuse me--inconsistent U.S. funding with a lack of--with consistent

Chinese funding abroad may persuade researchers to collaborate with China on larger projects or pursue their research in Chinese institutions.

Inconsistency of funding in European institutions, in part, led to China's most prestigious and ambitious project to date, Micius. Pan Jianwei, considered to be the father of Chinese quantum information science and a lead on the satellite project, partnered with his mentor and erstwhile rival, Austrian scientist Anton Zeilinger. Although Zeilinger had the technical know-how and expertise, he had been unable to secure funding in Europe to launch and operate a quantum satellite.

Pan's connections with the Chinese Academy of Sciences proved beneficial, and the satellite only became a reality through Chinese state funding.

The balance of power between the U.S. and China is due, in part, to the former's long-held preeminence in information technologies and technological innovation. Indeed, the United States is the birthplace of IT, the Internet, and both the civil and military information revolutions. China's rise as a leader in quantum and related emerging technologies would therefore signal an eastward shift in the locus of international innovation.

There are certainly military implications for these technologies as well. Pan Jianwei has claimed--again, he's the father of Chinese quantum information science--that China is fully capable of leveraging quantum communications in a regional war. The national quantum infrastructure they have built is considered to be dual use.

The widespread adoption of quantum encryption in communications would shield much of their communications from intelligence surveillance and reconnaissance. This would be especially pronounced in military signals intelligence, particularly in the East, and maritime operations in the East and South China Seas.

Quantum computing may play a significant role in military strategy by virtue of its potential to provide substantial source of processing power. Data processing may become one of the foremost resources for warfighting in the near future, comparable in importance to the role that data plays in the information age, and the role that oil, coal, wind and horsepower have played in previous eras of warfare.

Quantum radar, which China claims to have developed, could overcome superior U.S. stealth capabilities if operationalized, enabling the PLA to undermine this critical pillar of U.S. power.

The commentary and PLA media at the time highlighted quantum radar as the nemesis of today's stealth fighter planes that will have remarkable potential in the future battlefield.

Simply put, the United States cannot allow itself to fall behind in these critical emerging technologies. Simply to stay competitive, the United States needs to keep ahead or apace of China's efforts for scientific, academic, commercial and military applications of quantum information science.

Some of the few, though critical, advantages the United States still possesses are dominance in emerging technologies, world-class academic and research institutions, and a central position in information and Internet technologies. If continued Chinese investment in these areas are not met with an appropriate U.S. response, these factors will shift likely at the expense of the United States, and the strategic balance of power will continue to tilt in China's favor.

I make four recommendations in my written testimony that focus on measures Congress and the U.S. government may take in the near term. Most importantly, the U.S. needs to use tools currently at its disposal such as the Government Accountability Office and the Office of Net Assessment to get a better handle on the problem. Treatment follows diagnosis.

Secondly, we need more available public interest research into China's development of these emerging technologies. There's not very much. And for something so critical, public debate and public policy shouldn't be limited by such a dearth of information.

Third and fourth, the U.S. government should explore options that increase its capacity to both detect and inform itself of new and emerging technologies and their implications, perhaps through reestablishing or reorganizing the Congressional Office of Technology Assessment and a method to apportion strategic R&D investment through an all-of-government approach, perhaps through a more formal interagency working group.

That concludes my testimony, and I look forward to your questions. Thank you.

PREPARED STATEMENT OF JOHN COSTELLO
SENIOR ANALYST FOR CYBER AND EAST ASIA, FLASHPOINT

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

We are in the midst of a "second quantum revolution," one that enables disruptive new technologies that have the potential to change long-held dynamics in commerce, military affairs, and strategic balance of power.[1] Within the foreseeable future, the realization of quantum computing will result in revolutionary computing power, with wide-reaching applications. The employment of quantum cryptography can create quantum communications systems that are theoretically unbreakable and unhackable. Quantum sensing enables the capability to conduct extremely precise, accurate measurements for new forms of navigation, radar, and optical detection.

Although the future trajectory of quantum technologies is hard to predict, their revolutionary potential and promise has intensified international competition. The U.S. remains at the forefront of quantum information science, but its lead has slipped considerably as other nations, China in particular, have allocated extensive funding to basic and applied research. Consequently, Chinese advances in quantum information science have the potential to surpass the United States.[2] Once operationalized, quantum technologies will also have transformative implications for China's national security and economy. As the United States has sustained its preeminent position in the international affairs due in part to its technological, military, and economic dominance, it is critical to take swift action to reverse this trend and once again establish leadership in emerging technologies like quantum information science.

This testimony will address the following topics:

- Part I offers a basic overview of the underlying technology, applications, current status, and challenges in quantum computing, quantum encryption, and quantum sensing.
- Part II details drivers behind China's investment in quantum information science, national R&D plans, and efforts and milestones.
- Part III compares U.S. and Chinese efforts and delineates the critical factors in play.
- Part IV details the commercial and strategic implications of quantum information science technologies.

---

[1] Jonathan P. Dowling and Gerard J. Milburne, "Quantum Technology: the Second Quantum Revolution," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 361, no. 1809 (2003): 1655-1674, https://arxiv.org/pdf/quant-ph/0206091.pdf

[2] This testimony builds upon prior research and writings by the author, including: Elsa Kania and John Costello, "Quantum Leap (Part 1): China's Advances in Quantum Information Science, *China Brief*, December 5, 2016. Elsa Kania and John Costello, "Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies, *China Brief*, December 21, 2016.

- Part V provides a conclusion and final thoughts on the information presented.
- Part VI gives recommendations to the U.S. Congress on how the United States may regain its lead in quantum information science and other critical emerging technologies.

Part I. Overview of Quantum Information Science Technologies:

Quantum information science harnesses the power of uncertainty and the strange – often counterintuitive – properties of quantum states. Taken together and scaled, these technologies establish exciting new paradigms in every aspect where information is used, stored, processed, or collected, providing vastly more powerful instruments of computation, security, and measurement.

General Principles

Quantum information science can be broadly broken up into quantum computing, quantum encryption, and quantum sensing. While each of these technologies differ wildly in technological basis and applications, all rely on two fundamental properties of quantum phenomena:
superposition and entanglement. Superposition refers to the ability of a particle, like a photon, to exist in all possible states at the same time. Entanglement refers to sharing this state across two or more particles. Observing the particle will "collapse" the state, resulting in its reversion to one of the two states. So too, for entangled pairs, even if separated across a great distance, the observation of either particle will "collapse" the state, immediately reverting one particle to one state and the other to a corresponding, opposite state. It is these strange properties of superposition and entanglement, the latter of which Einstein famously referred to as "spooky action at a distance," that give these technologies their unique power.

Quantum Computing

Traditional or "classical" computers perform calculations using standard "bits" which exist in states 1 or 0. Quantum computing, through its employment of "qubits" (i.e., a quantum analogue of the "bit," which simultaneously exists in a superposition of the states of 0 and 1), will convey an extreme advantage in computing power. Qubits, which exist in a superimposed state and entangled together are able to execute vast numbers of calculations simultaneously. In the future, quantum computers will be able to resolve complex algorithms, including those integral to most standard encryption methods. Computations that would be impossible or infeasible for classical computers to perform can be performed by quantum computers at sufficient scale.

The commercial promise of a full-scale general quantum computer is largely driving both statelevel and commercial funding into these technologies. The commercial and military applications of these technologies are nearly endless, appropriate wherever speed and processing power are at a premium. Some commercial applications that have been suggested include large-scale simulations for weather, complex and chaotic systems, protein folding and modeling, genomics, big-data, intelligence processing, and artificial intelligence. For the military, as the information age ends and a new age based on automation and machine learning takes hold, the processing power of quantum computers promises to play a critical role.

Currently, a general-purpose, full-scale quantum computer does not exist. D-Wave, a Canadabased company, does produce what has been called the world's first quantum computer. However, this computer uses "quantum annealing" a form of computation that, strictly defined, is not considered "true" quantum computing. Google, IBM, and NASA, among others, on the U.S. side and Alibaba and Chinese Academy of Sciences (CAS) on the Chinese side are each establishing public-private or private research groups with the object of developing a general-use quantum computer. The goal is to achieve "quantum supremacy" or a quantum computer that is able to outperform a traditional, or classical computer in every way.

There are significant technological barriers that need to be overcome to realize a fully capable quantum computer. It will be challenging but necessary to scale quantum computers to achieve quantum supremacy. In addition, designing the algorithms and software on which these calculations could be run presents a further challenge. Since quantum computers do not perform calculations like classical computers, newer approaches to software and programming are another factor to consider in developing the capacity necessary to exploit these technologies.

Nonetheless, security researchers have become concerned that quantum computers could undermine certain prevalent encryption standards currently in use. Using Shor's algorithm, a quantum computer of sufficient scale would be able to crack encryption keys for many modern forms of encryption, an endeavor that by today's classical computing standards would be impossible or infeasible within a practical time frame. In 2015, likely in response to progress in quantum computing, the National Security Agency (NSA) updated their "Suite B" encryption methods towards ones that focused on "quantum resistant" encryption, or encryption standards that would be beyond a quantum computer's ability to break.[3] The National Institute of Standards and Technology (NIST) has also launched a competition in response to develop a set of "quantum resistant" encryption standards.[4] Other forms of encryption, such as lattice-based encryption, are less efficient but resistant through cracking from quantum computers.

Quantum Cryptography:

There are three qualities of quantum states that give quantum encryption and communications their protective power, according to SANS.[5] First, the "no-cloning" theorem states that an unknown quantum state cannot be copied. Second, in a quantum system, which is a complex of two or more particles in a shared "entangled" state, an attempt to measure or observe will disturb the system, revealing an eavesdropper to the sender and recipient. Third, disturbing the system is irreversible, meaning an interloper wouldn't be able to cover up evidence of the interception.

[3] Bruce Schneier, "NSA Plans for a Post-Quantum World," Lawfare, August 21, 2015, https:// www.lawfareblog.com/nsa-plans-post-quantum-world

[4] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, "Report on Post-Quantum Cryptography," *National Institute of Standards and Technology Internal Report* 8105 (2016).

[5] Bruce R. Auburn, "Quantum Encryption–A Means to Perfect Security," *SANS Institute*, 2003, https:// www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986

Quantum key distribution can be accomplished through fiber-optic networks as well as over the electromagnetic spectrum in “free space” quantum communications. Sending through fiber-optic networks limits range of QKD, while quantum free-space communications allows for more longdistance key exchange but opens it open to other forms of interference, such as debris, noise, and jamming. These technologies have considerable technological and logistical challenges and, according to some researchers don’t confer enough information security advantages to warrant the added complexity necessary for their use. The Air Force Scientific Advisory Board stated that classical alternatives offer the same advantages without the headache of additional equipment and complexity.[6]

Concerns over information security and privacy of communication may be driving significant state-level investment in this field. China, in particular, has drawn a direct line between statelevel programs in quantum encryption and revelations of massive U.S. espionage alleged by Edward Snowden. These technologies have apparent, but untested, military applications as well. Quantum teleportation and communication not only conceals the content of the message, but also alerts the recipient and sender if the signal is intercepted. This is a major potential disruptive feature in the world of global intelligence, surveillance, and reconnaissance capabilities.

Quantum Sensing

Quantum sensing, broadly defined, is the ability to use quantum phenomena like entanglement for extremely precise and accurate measurements, also known as quantum metrology. This discipline of quantum information science is a collection of techniques and applications of quantum metrology in sensors, rather than a specific technology in its own right. More accurate quantum clocks, quantum imagery, radar, navigation, and compasses are all discussed under this discipline.

Quantum sensors for use in gravimetric readers have commercial and military applications in subsurface sensing and detection (such as in oil-drilling) and inertial navigation systems, which would allow for high-precision navigation without global position satellites (GPS). This socalled “quantum navigation” or “quantum compass” would be useful for submarines and other maritime platforms. Quantum radar could nullify stealth technologies and advanced forms of radar jamming. Quantum imagery can allow for more precise optical capabilities that would have applications to space-spaced intelligence, surveillance, and reconnaissance and awareness in the space domain.

Of quantum information science disciplines, quantum sensing has the most direct and obvious military applications. As such, there is comparatively little openly available research on these topics when compared to quantum computing and encryption, which appear to be largely privatesector and academic affairs, respectively. As further research into this field evolves, more information will give a better picture of the relative progress made by the United States and China in the development of these technologies.

---

[6] USAF Scientific Advisory Board, “Utility of Quantum Systems for the Air Force,” August 19, 2016, http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

Part II. Chinese Quantum Information Science Efforts:

Under the leadership of Xi Jinping, China's prioritization of quantum information science has intensified. From the Chinese leadership's perspective, quantum technologies have become integral to national security, particularly information security, and to strategic competition. This research agenda has taken on increased importance ever since the leaks by former NSA contractor Edward Snowden. In fact, this incident was so fundamental to Chinese motivations that Snowden has been characterized as one of two individuals with a primary role in this scientific 'drama,' along with Pan Jianwei himself.[7]

There are three fundamental factors driving China's investment into quantum information science R&D:

1. Information Security: The use of quantum encryption and communication for information security is a primary driver for China's increased investment in that field. Chinese scientists and media have drawn a direct linkage between the need for progress in quantum information science and the Snowden leaks. As Chinese authorities grow more concerned about potential for spying in their ICT systems, the advantages that quantum encryption confers will be se This will be especially critical as Chinese society grows more informatized and connected, potentially making it even more vulnerable to foreign adversary spying, sabotage, and influence.

2. Economic Competition: There is a recognition that current U.S. dominance in information technology may not confer any substantial advantages in pursuit of quantum information science, essentially placing China on par with the United States and putting it in a unique strategic position to corner the market on these technologies. If so, China would benefit from first-to-market advantage that, when coupled with its manufacturing and human capital base would allow it to achieve and sustain global leadership in quantum information solutions and the next information revolution.

3. Strategic Military Competition: Quantum computing has very real military applications in the fields of big data analytics, artificial intelligence, complex systems simulation, and advanced robotics. The widespread adoption of quantum technologies for military or government communications would hinder an adversary's ability to conduct surveillance and signal intercepts, as any attempt to do so would be detectable. Additionally, use of quantum sensing for inertial navigation, stealth detection, high-resolution space-based surveillance and reconnaissance, and submarine detection each challenge current military paradigms built on technological and intelligence superiority, although in different ways. These would disrupt current military paradigms in which the United States has a distinct advantage.

---

[7] "China Will Establish a Global Quantum Communications Network By 2030" [中国将□力□争在2030年□前后建成全球量□□子通信□网], *Xinhua*, August 16, 2016, http://news.sina.com.cn/c/sd/2016-08-16/doc-ifxuxnpy9658879.shtml.

For these reasons, quantum technology has attracted the attention of the Chinese leadership at the highest levels, and Xi himself has emphasized the strategic importance of quantum technologies to national security and particularly cyber security. In September 2013, Xi Jinping and other Politburo members visited Anhui Quantum Communication Technology Co. Ltd. for a collective learning session, meeting with Pan Jianwei and the company's general manager, before viewing a demonstration of quantum communication technology.[8] In November 2015, at the 18th Party Congress' 5th Plenum, Xi Jinping included quantum communications in his list of major science and technology projects that are prioritized for major breakthroughs by 2030, given their importance from the perspective of China's long-term strategic requirements.[9] In April, Xi visited the University of Science and Technology of China, where he met with Pan Jianwei and praised his progress.[10] During the 36th Politburo study session on cyber security, Xi also emphasized the importance of advancing indigenous innovation in quantum communications and other critical cyber information technologies.[11]

Chinese National R&D Planning

At the highest level, the 13th Five-Year Plan (2016-2020), formulated in the aftermath of the Snowden leaks, intensifies the prioritization of quantum information science, including "quantum control" in the category of "basic research related to national strategic requirements."[11] Following from this, China's national research and development plans for science and technology have translated the increasing national prioritization of quantum technology into action through funding research in this domain. The National Key R&D Plan (国家重点研发计划), a large-scale reorganization of China's national-level research and development planning, including the consolidation of the 863 and 973 plans, has strengthened and focused development of quantum

[8] "Anhui Quantum Communications Innovation Successfully Featured in Politburo Collective Learning Activities" [安徽量□□子通信创新成果 亮相中央政治局集体学习活动], Quantum CTek, September 30, 2013, http:// www.quantum-sh.com/news/146.html.

[9] "Xi Jinping: Explanations Regarding the "CCP Central Committee Suggestions Regarding the Formation of the National Economic and Social Development Thirteenth Five-Year Plan" [习近平:关于《中共中央关于制定国□民经济和社会发展第□十三个五年□规划的建议》的说明], *Xinhua*, November 3, 2015, http://news.xinhuanet.com/ politics/2015-11/03/c_1117029621_3.htm.

[10] "Xi Jinping Inspected USTC: Must Advance Independent Innovation in the Process of Opening" [习近平考察中科□大：要在开放中推进□自主创新], *Xinhua*, April 27, 2016, http://news.xinhuanet.com/politics/2016-04/27/ c_1118744858.htm [11] "Xi Jinping: Accelerate the Advancement Independent Innovation in Cyber and Information Technology, Unrelentingly Strive towards the Objective of Constructing a Cyber Power" [习近平：加快推进□网络信息技术□自主创新 朝着建设□网络强国□目标不不懈努□力□], *Xinhua*, October 9, 2016, http://news.xinhuanet.com/politics/ 2016-10/09/c_1119682204.htm

[11] ""Thirteenth Five-Year" Plan Guidelines" ["□十三五"规划纲要], *Xinhua*, March 18, 2016, http:// economy.china.com/news/11173316/20160318/22110334_all.html

information science.[12]

Although the Chinese focus on quantum technology can be largely attributed to information security concerns, this also reflects the successes achieved through the research undertaken so far. This has become a self-reinforcing cycle in which national-level interest in quantum technology has proceeded alongside and been reinforced by progress that Chinese researchers have achieved.

National Key R&D Plan

In February 2016, the National Key R&D Plan (**国家重点研发计划**) included quantum control and quantum information among its prioritized projects. [13] The available guidance for the project in 2016 and 2017 emphasized six particular research tasks: related electronic systems, small quantum systems, artificial band-gap systems, quantum communications, quantum computing and simulations, and quantum precision measurement.[14]

13th Five-Year National Science and Technology Innovation Plan

In August 2016, the new 13th Five-Year National Science and Technology Innovation Plan (**国家科技创新规划**), urged China to seize the "high ground" (**制□点**) in international scientific development, included an intensified focus on multiple forms of quantum technology.[15] The plan included quantum control and quantum information as among the top "major strategic prospective scientific issues" and called for China to achieve breakthroughs in quantum communication and the quantum anomalous Hall effect.

---

[12] "Quantum Control and Quantum Information Key Special 2016 Annual Project Reporting Guidelines" [量□□子调控与量量□子信息"重点专项2016年□度项□目申报指南], Ministry of Science and Technology, February 16, 2016, http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2016/201602/t20160214_124104.htm

[13] "Quantum Control and Quantum Information Key Special 2016 Annual Project Reporting Guidelines" [量□□子调控与量量□子信息"重点专项2016年□度项□目申报指南], Ministry of Science and Technology, February 16, 2016, http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2016/201602/t20160214_124104.htm

[14] Quantum Control and Quantum Information Key Special 2017 Annual Project Reporting Guidelines and Suggestions [量□□子调控与量量□子信息重点专项2017年□度项□目申报指南建议], Ministry of Science and Technology, August 1, 2016, http://service.most.gov.cn/2015tztg_all/20160801/1146.html

[15] "Notice of the State Council on the Printing and Distribution of the Thirteenth Five-Year National Science and Technology Innovation Plan" [国务院关于印发"□十三五"国家科技创新规划的通知], State Council, August 8, 2016, http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm |

For the 2030 timeframe, the plan also called for choosing a new round of major science and technology projects that "embody national strategic intent," including quantum communication and quantum computing. In particular, this major project was to include metropolitan and intercity free space quantum communications technology, the development and manufacture of common-use quantum computing prototypes, and the development and manufacture of actualuse quantum simulators. To develop air and space exploration, the plan called for advancing technologies for quantum navigation and also "the completeness of quantum mechanics."

Made in China 2025

China has also made the commercialization of these technologies as a priority. As of May 2015, the new "Made in China 2025" (**中国制造**2025) plan included advances in quantum computing among its priorities, in the category of the "next generation information technology industry."[16] The extent to which these efforts may hinder foreign quantum computing efforts ability to compete against Chinese firms within China is unknown.

Chinese Quantum Milestones

Currently, the PRC is hurtling headlong towards the quantum era, placing its bets on the disruptive, even revolutionary potential of quantum technology. These recent breakthroughs have been preceded and enabled by long-term efforts and investments in quantum information science, all enthusiastically backed at the highest levels of Chinese leadership. As a result, Chinese scientists have succeeded in progressing towards the operationalization and commercialization of unhackable quantum communications, while seeking supremacy in quantum computing and concurrently progressing in quantum sensing.

Quantum Computing

While Chinese advances in quantum cryptography have achieved multiple world records and seemingly outpaced parallel global efforts, Chinese quantum computing efforts remain relatively nascent. Nonetheless, Chinese scientists have increasingly kept pace with global progress in quantum computing and also achieved notable advances in this domain.[17] As leading quantum scientist Guo Guangcan has emphasized, "Chinese scientists have been going all out to win the worldwide race to develop a quantum

---

[16] "The State Council's Notice on the Printing and Distribution of "Made in China 2025" [国务院关于印发《中国制造2025》的通知], Ministry of Industry and Information Technology, May 19, 2015, http://www.miit.gov.cn/ n11293472/n11293877/n16553775/n16553792/16594486.html

[17] "Present Status and Development Trends of Quantum Computers" [量□□子计算机的发展现状与趋势], CAS, 2010, http://www.bulletin.cas.cn/ch/reader/view_full_html.aspx?file_no=20100507&flag=1

computer."[18] For instance, in August, USTC scientists announced their successful development of a semiconductor quantum chip, which could enable quantum operations and information processing.[19] Later that month, researchers also from USTC announced their breakthrough in the preparation and measurement of six hundred pairs of entangled quantum particles.[20] In October, USTC researchers announced significant progress in quantum control that could enable future advances in quantum computing based on more precise quantum logic gates.[21] As Pan Jianwei has noted, the eventual development of a quantum computer with 50 qubits could achieve "quantum supremacy" (量□称霸), including the capability to overcome most conventional encryption capabilities.[22] However, Pan anticipates that the creation of a "truly programmable, universal" quantum computer might ultimately require between 30 and 50 years.

Relative to quantum communication, China's quantum computing efforts have a much greater degree of private sector involvement and investment. This phenomenon is mirrored in Western nations where there is heavy private sector involvement in research on quantum computing. In China, the most visible and mature effort has occurred at the Alibaba Quantum Computing Lab, a collaboration between Alibaba's cloud computing arm, Aliyun, and CAS that was established in 2015. According to Pan Jianwei, who also serves as its chief scientist, the team will "undertake frontier research on systems that appear the most promising in realizing the practical applications of quantum computing." Their pursuit of quantum computing will take advantage of "the combination of the technical advantages of Aliyun in classical calculation algorithms, structures and cloud computing with those of CAS in quantum computing, quantum analogue computing and quantum artificial intelligence, so as to break the bottlenecks of Moore's Law and classical computing."[23] For quantum computing, the Alibaba Quantum Computing Lab has articulated equally ambitious goals. Their team seeks by 2020, to achieve the coherent manipulation of 30 qubits; by 2025, to develop quantum simulation with calculation speeds

---

[18] Zhu Lixin, "Progress made in development of quantum memory," *China Daily*, August 20, 2016, http:// usa.chinadaily.com.cn/epaper/2016-08/20/content_26559829.htm

[19] "China Successfully Develops Semiconductor Quantum Chip," Chinese Academy of Sciences, August 12, 2016, http://english.cas.cn/newsroom/news/201608/t20160812_166433.shtml.

[20] "China Makes New Breakthrough in Quantum Communications," Chinese Academy of Sciences, August 26, 2016, http://english.cas.cn/newsroom/mutimedia_news/201608/t20160826_166818.shtml.

[21] "Our Nation's Scholars Achieved the "Fastest" International Quantum Control, Laying the Foundation for Multi-Bit Quantum Computing" [我国学者实现国际"最快"量□□子控制 为多□比特量□□子计算基础], *Xinhua*, October 26, http://www.81.cn/gnxw/2016-10/26/content_7328567.htm

[22] "Pan Jianwei: "Quantum Supremacy" Will Become a Milestone in Physics and Computer Science" [潘建伟:"量□□子称霸"将会成为物理理学和计算机科学的□里□程碑碑], *Science and Technology Daily* [keji ribao | 科技□日报], November 6, 2016, http://www.stdaily.com/index/kejixinwen/2016-11/06/content_310018.shtml

[23] "Aliyun and Chinese Academy of Sciences Sign MoU for Quantum Computing Laboratory," Alibaba, July 3, 2015, http://www.alibabagroup.com/en/news/article?news=p150730

that match those of today's fastest supercomputers; and by 2030, to succeed in the "comprehensive realization of common-use quantum computing functions" through a quantum computer prototype with 50 to 100 qubits.[24]

Quantum Cryptography and Communications

The launch of the world's first quantum satellite, *Micius* (墨□) in August 2016 drew international attention to the PRC's rapid progress in quantum communications.[25] *Micius* established a quantum key distribution network with the transmission of quantum information between the satellite and multiple ground stations. [26] This recent launch is a component of Quantum Experiments at Space Scale (QUESS), a roject initiated in 2011, which has involved collaboration between a team led by leading Chinese quantum scientist Pan Jianwei from the University of Science and Technology of China (USTC), the Chinese Academy of Sciences (CAS), and the Austrian Academy of Sciences. The *Tiangong*-2 space station, launched in September, will also engage in quantum key distribution experiments.[27] As of mid-October, *Micius* was reportedly in good condition, with experiments ongoing and expected to be completed in November.[28] The satellite has successfully completed links with multiple ground stations, as well as teleportation optical links. *Micius* is only the first of what Chinese scientists intend will be a future constellation of multiple quantum satellites.[29] According to Anton Zeilinger of the University of Vienna, one of the lead scientists involved in the project, this is not only the initial test of the feasibility of quantum communication via satellite but also constitutes a "a very significant step towards a future worldwide quantum internet."[30]

---

[24] Chinese Academy of Sciences, Hand in Hand with Alibaba Will Establish a "Quantum Computing Laboratory" in Shanghai" [中国科学院携□手阿□里□巴巴在沪建□立"量□□子计算实验室"], *Xinhua*, July 31, 2015, http:// news.xinhuanet.com/2015-07/31/c_1116104188.htm. "Chinese Academy of Sciences - Alibaba Quantum Computing Lab" [中国科学院—阿□里□巴巴量□ 计算实验室挂牌], Chinese Academy of Sciences, September 2, 2015, http:// www.bsc.cas.cn/gzdt/201509/t20150902_4419884.html.

[25] "China Will Establish a Global Quantum Communications Network By 2030" [中国将□力□争在2030年□前后建成全球量□□子通信□网], *Xinhua*, August 16, 2016, http://news.sina.com.cn/c/sd/2016-08-16/doc-ifxuxnpy9658879.shtml.

[26] Ibid.

[27] "Tiangong-2: Lays a Foundation for China's Space Station Age" ["天宫□二号"：奠基中国空间站时代], *People's Daily*, September 18, 2016, http://military.people.com.cn/n1/2016/0918/c1011-28720954.html

[28] "Our Nation's Quantum Satellite Smoothly in Orbital Testing, Will Start Scientific Testing in Mid-November" [我国量□□子卫星在轨测试顺利利 11 □月中旬开始科学实验], *Xinhua*, October 12, 2016, http://www.81.cn/jwgz/ 2016-10/12/content_7297405.htm

[29] "China Will Establish a Global Quantum Communications Network By 2030" [中国将□力□争在2030年□前后建成全球量□□子通信□网].

[30] "China launches world's first quantum science satellite," Physics World, August 16, 2016, http:// physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite

The *Micius* satellite reflects the culmination of nearly two decades of steady progress on free space quantum teleportation, which uses the transmission of quantum states "over-the-air" to distribute quantum cryptographic keys. In 2005, Pan Jianwei's team first confirmed the feasibility of a quantum satellite in the world's first free space quantum communications experiment.[31] Since then, Chinese scientists have progressively increased the distance at which free space quantum communications can be operationalized, breaking several world records in the process. In 2010, a team of researchers from Tsinghua University and USTC published a paper describing their successful demonstration of quantum teleportation across 16 kilometers of free space.[32] Then, in 2012, Pan Jianwei and his colleagues demonstrated successful quantum teleportation and entanglement across 100-kilometer free-space channels.[33] These experimental achievements have since extended beyond the laboratory, with the launch of *Micius*, and this gradual, sustained progress in techniques for quantum entanglement and quantum teleportation continues. In September 2016, a paper by Pan Jianwei and his team described their success in the "full" quantum teleportation of photons through an optical fiber network 12.5 kilometers apart, such that the teleported photons were destroyed in one laboratory and recreated in another.[34][35] This research reportedly constitutes a notable step towards the development of a future "quantum Internet," which would be radically more secure than existing systems.

Concurrently, since ground-based fiber-optic quantum communication networks have reached a much more advanced stage than their free space counterparts, the Chinese leadership is engaged in a massive effort to operationalize these technologies in order to secure their most sensitive networks. In 2009, USTC's CAS Key Laboratory of Quantum Information (量□信息重点实验室) established what it characterized as the world's first "quantum government network" (in Wuhu, Anhui.[36] Notably, in 2012, for the 18th Party Congress, Pan led a team of researchers to create quantum communications networks that securely connected the venue hosting the meeting, the delegates' hotel rooms, and *Zhongnanhai*.[37] At the local level, metropolitan quantum communication

---

[31] Cheng-Zhi Peng et al., "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication," *Physical Review*, April 22, 2005, http://journals.aps.org/prl/ abstract/10.1103/PhysRevLett.94.150501

[32] Matthew Luce, "China's Secure Communications – A Quantum Leap," *China Brief*, August 19, 2010. Xian-Min Jin et al., "Experimental free-space quantum teleportation," *Nature Photonics*, May 16, 2010, http://www.nature.com/nphoton/journal/v4/n6/full/nphoton.2010.87.html

[33] Xian-Min Jin et al., "Experimental free-space quantum teleportation," *Nature*, August 8, 2012, http://www.nature.com/nature/journal/v488/n7410/full/nature11332.html

[34] Qi-Chao Sun et al., "Quantum teleportation with independent sources and prior entanglement distribution over a network," *Nature Photonics*, September 19, 2016, http://www.nature.com/nphoton/journal/v10/n10/full/nphoton.

[35] .179.html

[36] "USTC Establishes the First Quantum Government Service Network in Wuhu" [中国科技□大学在芜湖建成□首个量□□子政务□网], *Guangming Daily*, May 20, 2009, http://www.gov.cn/fwxx/kp/2009-05/20/content_1319699.htm

[37] Yu Dawei, "In China, Quantum Communications Comes of Age," *Caixin*, February 6, 2015, http:// english.caixin.com/2015-02-06/100782139.html

networks have been constructed in Hefei and Jinan.[38] As of 2016, Tianjin also planned to establish a metropolitan-level quantum encryption communication network in order to enhance the city's level of cyber security.[39]

At a larger scale, China has been building and will soon complete the world's largest ground quantum optical fiber communications system. The "Quantum Beijing-Shanghai Trunk" (量□京沪□线) will stretch approximately 1,240 miles between Shanghai and Beijing.[40] This project was enabled by prior research under the 863 Plan involving the demonstration of an integrated quantum communication fiber optic network.[41] According to Pan Jianwei, who is involved in the project, this quantum communications network will be used for the secure transmission of information in government, finance, and other sensitive domains.[42] Within the next several years, the "Beijing-Shanghai Trunk" may be expanded nationwide and linked with multiple metropolitan-level quantum communications networks. China intends to create a quantum communications network between Asia and Europe by 2020 and ultimately a global network in 2030.[43] Future quantum communications networks will probably involve both terrestrial wide area networks and quantum satellites linked with ground stations.[44]

---

[38] "Hebei Establishes the First Metropolitan Quantum Communications Testing Demonstration" [合肥建成□首个城域量□□子通信试验示范□网

Science Net, February 21, 2012, http://news.sciencenet.cn/htmlnews/2012/2/260041.shtm.

"Jinan Quantum Communications Test Network" [*Jinan liangzi tongxin shiyanwang* | 济南量量□子通信试验□网], Shandong Quantum CTek, November 21, 2013, http://www.quantum-sd.com/index.php? m=content&c=index&f=show&catid=3&l=1&id=5.

[39] "Tianjin Will Build a Quantum Secret Communications Metropolitan Network" [天津将建量□□子保密通信城域□网], *Tianjin Daily*, July 22, 2016, http://www.tianjinwe.com/tianjin/tjsz/201607/t20160722_1031311.html.

[40] ""Quantum Beijing-Shanghai Backbone" To Be Built This Year, Quantum Internet Can Be Expected" ["量□□子京沪

□干线"今年□建成"量□□子互联□网"可期], *Xinhua*, March 3, http://news.xinhuanet.com/politics/2016lh/2016-03/03/ c_1118225683.htm.

[41] "National 863 Project "Optical Fiber" Quantum Communication Integrated Application Demonstration Network"

Project Successfully Received Acceptance" [国家863计划"光纤量量□子通信综合应□用演示□网络"项□目顺利利通过验

收], SAICT, November 23, 2015, http://www.saict.org/kygl/kyjz/11/35053.shtml

[42] Quantum Beijing-Shanghai Backbone" To Be Built This Year, Quantum Internet Can Be Expected" ["量□□子京沪

□干线"今年□建成"量□□子互联□网"可期].

[43] "China to build global quantum communication network in 2030," *Xinhua*, November 2, 2014, http:// news.xinhuanet.com/english/china/2014-11/02/c_127169705.htm.

[44] "Our Nation Will Strive to Construct a Quantum Communications Network Around 2030" ["我国将□力□争在2030 年□前后建成全球量□□子通信

□网], *PLA Daily*, http://jz.chinamil.com.cn/n2014/tp/content_7209383.htm.

Quantum Sensing

Within a longer timeframe, various forms of quantum sensing, including quantum radar, may take advantage of quantum entanglement to enable highly sophisticated detection of targets, regardless of stealth.[45] Notably, in September 2016, a team of Chinese scientists from China Electronics Technology Group Corporation's (CETC) 14th Research Institute's Intelligent Sensing Technology Key Laboratory (智能感知技术重点实验室) publicized their progress towards creating a single-photon quantum radar that is capable of detecting targets up to 100 kilometers away with improved accuracy.[46] Their research was undertaken in collaboration with a team led by Pan Jianwei from the University of Science and Technology of China, CETC's

[45] In general, there are three primary forms of quantum radar, single-photon quantum radar (单光□子量□□子雷□达), interferometric quantum radar (□干涉式量□□子雷□达), and quantum entanglement radar (以及纠缠态量量□子雷□达) that may be under development by Chinese scientists. Although there is limited information available, there have been patents filed for a "laser radar based on the principle of strongly correlated quantum imaging," quantum radar and target detection methods, and a "quantum entanglement radar."

[46] "The Coming of the Quantum Radar That Makes Stealth Fighter in Profile" [让隐形战机显形的量量□子雷□达来了□], *Science and Technology Daily*, September 13, 2016. "China's First Single-Photon Quantum Radar Successfully Developed," [中国□首部单光□子量□□子雷□统研制成功], CETC, September 18, 2016, http://www.cetc.com.cn/ zgdzkj/_300931/_300939/445284/index.html

27th Research Institute, and Nanjing University.[47] The reported range of this quantum radar, which takes advantage of entanglement between photon pairs, is supposedly five times that of a laboratory prototype jointly created last year by an international team of researchers.[48]

Since the research openly published and available in international peer-reviewed journals likely only reflect a limited subsection of this research, it is difficult to evaluate the progress of this aspect of China's advances in quantum technology, especially the potential military applications, which may remain highly classified. For instance, CETC's release of information regarding its quantum radar may have been an overstatement or understatement of its actual capabilities. Potentially, the announcement of this advance in official media might have been intended as a signaling mechanism.[49] Nonetheless, the possibility that certain aspects of Chinese research on the military applications of quantum science could have advanced further than has been disclosed cannot be wholly discounted.

[47] "CETC's First Single-Photon Quantum Radar System Successfully Developed" [中国电科□首部单光□子量□□子雷□达系统研制成功], CETC 14th Research Institute, September 7, 2016, http://wmdw.jswmw.com/home/content/? 1174-3887947.html.

[48] "New research signals big future for quantum radar," Phys.org, February 26, 2015, http://phys.org/news/2015-02big-future-quantum-radar.html.

[49] "Quantum Radar: "Clairvoyant" with Insight into the Future Battlefield" [量□□子雷□达：洞□察未来战场"千□里□眼"], *PLA Daily*, September 22, 2016, http://jz.chinamil.com.cn/n2014/tp/content_7271314.htm.

Part III. Comparing Chinese and United States Advances in Quantum Information Science:
The United States was once the leader in quantum information science, but the lack of funding, structural and institutional issues, and lack of government coordination have reduced both the levels and consistency of support that are necessary to maintain capacity in this critical research area. The resulting void has caused the locus of research in certain quantum information science areas – most notably quantum cryptography – to shift to other countries where funding and support for basic research are more reliable.

Among the major limitations that the U.S. faces is the lack of high-level or long-term R&D plans and of a more comprehensive approach to scientific funding. China's current quantum information science programs reflect an "all-of-government" approach, whereas the White House has noted the lack thereof in the U.S. as a key factor for why the United State's funding levels are inconsistent. Indeed, China's quantum information science program is proceeding in lockstep with larger, national R&D and informatization plans, with a corresponding long-term strategy for commercialization of these technologies. This approach allows for more consistent levels of funding over time and is a clarion call to any scientists who hope to acquire funding for basic research - a mainstay for their careers.

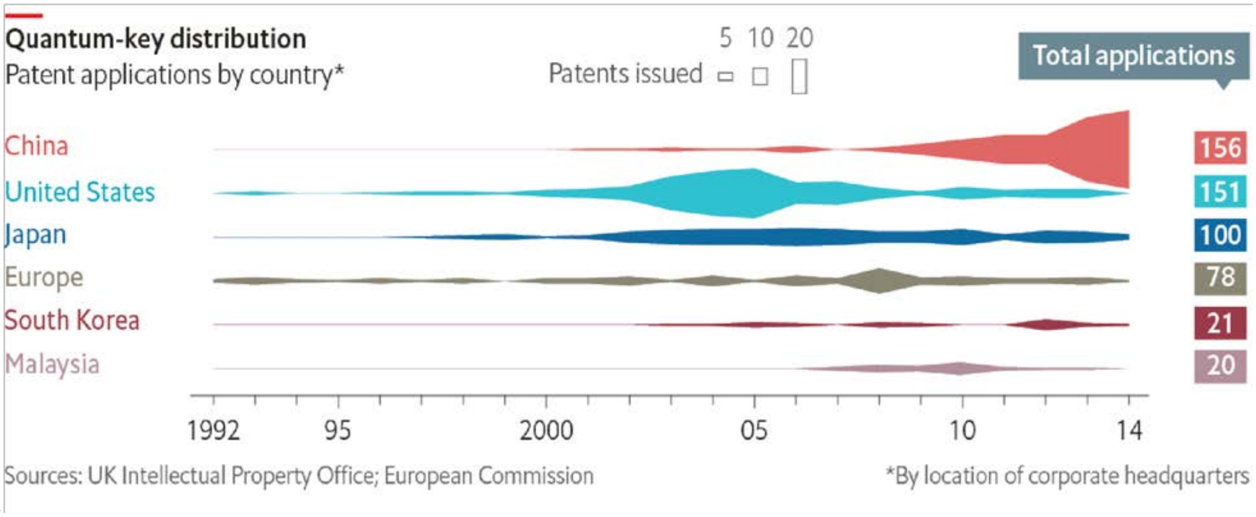
Overview:

One report from Massachusetts Institute of Technology (MIT) in 2015 reviews the state-of-play for emerging technologies, quantum included, and notes the U.S. lead has slipped considerably.[50] The report, titled "Future Postponed" studied critical areas where the United States was losing its technological dominance and leadership. The study suggested that a reduction in R&D funding threaten an "innovation deficit" with the U.S. lagging behind in emerging technologies. Quantum information science was listed as one of these critical areas, with the report noting that "U.S. leadership is not assured, especially given recent budget constraints, while the potential outcomes seem quite important both strategically and commercially."

A recent feature by the *Economist*, which offers a more comprehensive look at the state-of-theart of quantum information science and comparative efforts internationally, gives useful metrics in the shift of QIS innovation to China.[51] While the U.S. has made considerable advances in quantum computing, encryption, and sensing, the economist report show the overall pace of innovation has slowed allowing other countries like China to catch up and in some ways pass the U.S. China's rapid advances in quantum encryption, for instance, are demonstrated below. The increase in patent applications is a function of increased funding and meaningful indicator for progress in Chinese programs, which, in this author's view has surpassed that of the United States.

---

[50] A Report by the MIT Committee to Evaluate the Innovation Deficit, "Future Postponed: Why Declining Investment in Basic Research Threatens a U.S. Innovation Deficit," April 2015, https://dc.mit.edu/sites/default/files/ Future%20Postponed.pdf
[51] "Here, There, and Everywhere," *The Economist*, March 9, 2017, http://www.economist.com/technology-quarterly/ 2017-03-09/quantum-devices



!

Limitations on Progress in U.S. Quantum Information Science

A 2016 White House report titled "Advancing Quantum Information Science: National Challenges and Opportunities" gives an overview of the state of federally-funded quantum information science programs and challenges that remain in further progress in the field.[52] In addressing why this gap has narrowed, the report's recommendations provide a useful framework to compare the role of U.S. and Chinese structural and institutional factors.

According to the report, there are five major factors that need to be addressed to solidify and further U.S. dominance in this field: institutional boundaries within academic institutions, education and workforce training, technology and knowledge transfer, materials and fabrication, level and stability of funding. While a more comprehensive analysis of these factors in the context of U.S.-China economic and strategic competition is beyond the scope of this testimony, there is one factor in particular stick out as areas where China has a distinct advantage compared to the United States: stability of funding.

The report states that significant progress in quantum information science in the U.S. has been hindered by long-standing instability in both level and consistency of R&D funding. This has "negatively impacted both the pace of technical progress and development of a QIS workforce." According to the report:

Fluctuations in Federal and other U.S. funding led to discontinuities in university-based research programs and contributed to promising young as well as senior researchers choosing to pursue alternate careers or look for opportunities outside the United States.

[52] National Science and Technology Council (NSTC), "*Advancing Quantum Information Science: National Challenges and Opportunities,*" July 22, 2017, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/ images/Quantum_Info_Sci_Report_2016_07_22 final.pdf

The lack of consistent funding at home, coupled with ample Chinese funding abroad, may persuade researchers to collaborate with China on larger projects or pursue their research in Chinese institutions. Inconsistency of funding in European institutions in part led to China's most prestigious and ambitious project to date, *Micius*, the world's first quantum satellite. Pan Jianwei, father of Chinese quantum information science and lead on the satellite project, partnered with his mentor and erstwhile rival, Austrian Scientist Anton Zeilinger. Although Zeilinger had the technical know-how and expertise, he had been unable to secure funding in Europe to launch and operate a quantum satellite.[53] Pan's connections with the Chinese Academy of Sciences (CAS) proved beneficial, and the satellite only became a reality through Chinese state funding.

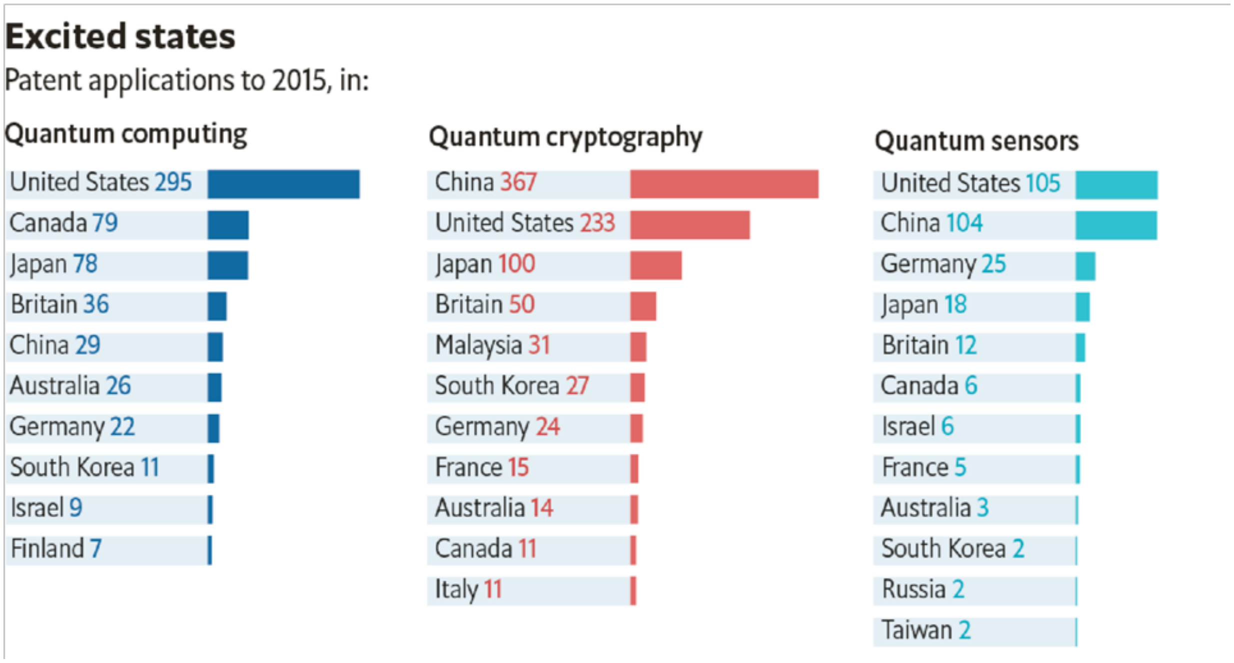
It should be noted that these factors do not account for the substantial advantages the U.S. enjoys over China in the area of overall quality and number of academic institutions, venture capital investment, industrial and technological base, and quality and speed of private innovation. However, these advantages are narrowed considerably by China rising economic dominance, multiple forms of tech transfer, talent recruitment programs, and comprehensive state-level R&D funding programs. Despite structural disadvantages in state-level funding, the United States has seemingly maintained its lead in quantum information science in general, but, as noted, this gap is narrowing.

Comparisons of U.S. and Chinese Progress

There is a general sense that China missed the first "information revolution" in the first Gulf War and has since struggled to catch up and surpass the United States. The leapfrogging strategy it has employed that uses a combination of state investment, technology transfer, and espionage has enabled only limited success in realms where the U.S. had traditionally been dominant, such as information technologies. This may not hold true for quantum. As such, quantum information science is one area where China feels it has a strategic advantage, and its leapfrogging strategy may pay off in commercial and military contexts. This has so far been true for quantum encryption, but it's unclear if that same success can be found in computing and sensing, which present different technical challenges.

---

[53] Elizabeth Gibney, "Chinese satellite is one giant step for the quantum internet," *Nature*, August 16, 2016, http:// www.nature.com/news/chinese-satellite-is-one-giant-step-for-the-quantum-internet-1.20329



In quantum computing, China lags behind the United States both in progress as well as scale and size of effort, according to information available in open sources. The joint Alibaba-CAS effort is still nascent and is behind more mature efforts on the part of D-Wave (backed by In-Q-tel), Google, IBM, NASA, and LogiQ (an IARPA effort). This doesn't account for sizable efforts from Europe and the U.K. Unlike the quantum encryption program, it's not clear if academic exchanges, cooperation, and increased R&D investment will breed the same success in quantum computing as it has in quantum encryption. This begs the question whether China will have to pursue other means to achieve advances such as increased infusion of venture capital, foreign mergers and acquisitions, or commercial espionage. China benefits from high-levels of state funding and a growing venture capitalist market that is behind that of the United States. This is one area where the United States has a distinct financial advantage. The clear market applications of quantum computing have driven substantial amounts of private investment in these areas. As China's private investment ecosystem continues to mature, however, this U.S. advantage may narrow considerably.

China is the preeminent leader in quantum encryption and communication technologies. The combination of state R&D investment, academic exchanges, and commercial applications have placed it ahead of the United States. In the last few years, Chinese researchers have taken steps to overcome the very real technical and logistical hurdles preventing practical use of quantum encryption. In the last year alone, Chinese researchers have been able to execute "measurement device independent" quantum key distribution (MDI QKD) to overcome a potential vulnerability and have also solved the so-called "nocturnal problem" which limited free-space communication's use to nighttime.[54] China appears to be resolving the problems of scale and complexity endemic to large-scale quantum key distribution through creating a national quantum key distribution network that allows critical infrastructure companies, government agencies, and the military to plug in for their own super-secure quantum encryption networks.

Quantum sensing is perhaps the most unknown of these technologies, in terms of both the technological hurdles China may or may not have been able to surmount and how these efforts compare to those of Western nations like the United States. What is known is that both nations appear to recognize the applications that these technologies have in both commercial and military realm. While China claims to have tested the world's first quantum radar, it's not clear whether Chinese researchers have yet been able to surmount the technical problems that limit the technology's range and reliability. Otherwise, the United States and other Western countries, such as the United Kingdom certainly have an advantage in this area, already having realized basic quantum sensors for use in commercial and military applications.

[54] Stephen Chen, "Chinese scientists solve quantum communication's 'nocturnal curse', paving way for sending of secure messages 24/7," *South China Morning Post*, January 3, 2017,http://www.scmp.com/news/china/article/ 2054219/chinese-scientists-solve-quantum-communications-nocturnal-curse-allowing

Part IV. Strategic Considerations:

The balance of power between the U.S. and China is due in part to the former's long-held preeminence in information technologies and technological innovation. Indeed, the United States is the birthplace of information technologies, the Internet, and both the civil and military information revolutions. China's rise as a leader in quantum and related emerging technologies would therefore signal an eastward shift in the locus of international innovation.

This testimony focuses largely on the military and strategic implications of China's quantum information science efforts. However, the economic impact these technologies are likely to have once matured and commercialized is substantial enough to have major implications for strategic competition. It is clear that for each of these technologies, the first-to-market advantage will be immense. For quantum computing in particular, any nation which first develops a general purpose, large-scale quantum computer will have nearly intractable market dominance, able to offer a high-powered, big data solution that are equally applicable in all industries where processing power would be useful. There are already commercially available solutions for quantum encryption to secure data at rest, and limited solutions for protecting data in transit. The effects in quantum sensing will be comparatively much less pronounced in the commercial domain, and may hold higher dividends in scientific research. The exact of quantum sensors commercial applications are not fully clear, though may extend to oil-drilling, resource detection, neurology, and other areas. Due to the relative immaturity of these commercial markets, there doesn't appear to be currently substantial threat from China in usurping U.S. dominance in these areas.

If the United States does not maintain or regain its edge in these vital areas in the context of the pace and scale of China's research, China may eventually edge out the United States and dominate commercial sales of these technologies. This would be a major paradigm shift in today's information technology environment, where the locus of power is firmly planted in the United States.

Quantum Computing

Quantum computing may play a significant role in military strategy by virtue of its potential to provide a substantial source of portable processing power. Increasingly, military strategists and planners recognize that data processing may become one of the foremost resources for warfighting in the near future – comparable in importance to the role that data plays in today's information age, and the role that oil, coal, wind, and horsepower have played in previous eras of warfare.
The information age, which has put a premium on collection, processing, a dissemination of data and intelligence, may subside as traditional reliable areas of collection such as computer network and electromagnetic spectrum become more contested or unavailable through technical means. Quantum encryption, information security, and quantum sensors only accelerate this trend further. A corresponding increase in processing power brought through advancements in quantum computing and

classical computer science will shift the focus of military advantage towards speed, precision, and timeliness of analysis and action in a limited information resources environment. Indeed, as a brilliant colleague of mine, Peter Mattis once observed, “analysis is the tool of last resort when efforts to collect the necessary information for decision-making have failed. Regardless of whether analysis sifts signals from noise or connects the dots, analysis attempts to provide by inference what cannot be known directly.” As we shift from the current information age to a machine age of warfare, these dynamics will become more pronounced. In this regard, the portable processing power of quantum computing coupled with artificial intelligence represents a critical capability in this new paradigm.

Finally, though valid, concerns over quantum computing’s ability to crack modern-day encryption are largely overblown. While estimates vary considerably, experts predict the first general purpose quantum computer will not be made available at least within the next decade, allowing standard bodies, public, and private sector plenty of time to innovate new methods that put encryption beyond quantum’s reach. If anything, the rapid advancement of quantum computers demonstrate the need to move on to quantum resistant forms of encryption sooner rather than later. As such, military communications should use quantum-resistant encryption at a bare minimum, and operate at wider bandwidths to accommodate for less-efficient, though more secure algorithms.

Quantum Encryption and Communication

The widespread adoption of quantum encryption and communication would undercut U.S. advantages in intelligence surveillance and reconnaissance, potentially shielding some Chinese forces from intelligence collection. This would be especially pronounced in military signals intelligence, particularly of Chinese maritime operations in the East and South China Seas. Chinese space-based quantum communications networks enabled by satellites like *Micius* would ideally allow eavesdrop and hack-proof communications worldwide. This type of shield could extend to closed Chinese government and military fiber-optic networks, providing additional obstacles to executing computer network exploitation of these targets for strategic and operational intelligence and, more hypothetically, presenting a barrier to certain forms of computer network attack. The real operational implications of quantum encryption are unclear as a majority of these technologies are untested in a military context and have yet to be implemented in any practical way.

Utilizing these technologies does come with tradeoffs. It’s not clear how quantum encryption would hold up in an operational context. The systems upon which it relies tend to be fragile and delicate. Quantum communications are also highly vulnerable to disruption and jamming as they relies on sensitive detection mechanisms to work properly. While there are methods to mitigate against jamming, they are unproven experimentally. Therefore, for radio communications and free-space quantum key distribution, these networks may only be useful for peacetime purposes and unable to meet the hard realities of an electromagnetically contested environment expected during war and conflict. For its part, the U.S. Air Force believes that both quantum encryption and communications “yield limited benefit...while adding significant complexity."[54] Quantum encryption "provides little advantage over the best classical alternatives."

Also, as noted before, the vulnerabilities of encryption - or any form of secure technology - are not derived from the theoretical concepts underpinning the technology, but rather the reality of their implementation. These systems would still be vulnerable to social engineering, side-channel attack, software vulnerabilities, and other forms of computer espionage that do not directly target the physical properties that give quantum encryption its advantage. SANS Institute perhaps put it best, stating:

> *Long encryptions keys might be compared, in military terms, to a mile-high mountain that that has an enemy behind it. The attacking army could go straight over the mountain to reach the enemy, or it might attack by going around the mountain. It has been said that quantum cryptography merely creates a higher mountain, and that the enemy has been concentrating for a long while not on defeating encryption schemes, but in attacking in other ways.*[55]

Despite these problems, there is no doubt that quantum encryption would hinder a highlysophisticated, large-scale, global intelligence surveillance regime like that of the United States, if implemented at sufficient scale.

Quantum Sensing

As the electromagnetic spectrum becomes potentially crowded in times of peace and contested in times of war, the ability to ensure trust in sensors and operate independently of the spectrum's limitations will be critical. The Air Force Scientific Advisory Board specifically points out quantum clocks and quantum sensors as two areas that warrant further investment. The study states, "Better timing precision would enhance Air Force missions/capabilities such as signals intelligence (SIGINT), counter-DRFM (digital radio frequency memory), electronic warfare (EW), and more robust communications."[56] Regarding quantum magnetometers, which enable quantum navigation, the study states that "[these] sensors can be an important part of achieving GPS-denied advantage. Quantum inertial sensing (e.g., cold atom IMUs) can provide extremely low drift rates and is not susceptible to jamming."

Quantum imaging, a related technology to quantum radar just focused on the visible range, can substantially increase satellites optics, either for space object surveillance and identification (SOSI) or ground-based target tracking. The technology is able to reduce noise and loss caused by debris and

---

[54] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," August 19, 2016, http:// www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

[55] Bruce R. Auburn, "Quantum Encryption–A Means to Perfect Security," *SANS Institute*, 2003, https:// www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986

[56] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," August 19, 2016, http:// www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

weather. Researchers from the University of Missouri have suggested that these type of quantum sensors can be operationalized for use in the both space and maritime domains.

Quantum radar, which China claims to have developed, could overcome superior U.S. stealth capabilities if operationalized, enabling the PLA to undermine this critical pillar of U.S. military power. The commentary in PLA media at the time highlighted quantum radar as the “nemesis” of today’s stealth fighter planes that will have “remarkable potential” on the future battlefield.[57] Additionally, other, more theoretical descriptions of quantum radar suggest that it would be able to defeat radar jamming techniques such as digital radio frequency memory (DRFM) jammers which spoof a radar’s broadcasted signal to conceal an aircraft’s true location. However, it remains difficult to evaluate the timeframe within which quantum sensing will become a reality beyond the laboratory in a military context or whether that would be made known in open sources.

Part V. Conclusion and Final Thoughts:

The United States cannot allow itself to fall behind in these critical emerging technologies. Simply to stay competitive, the United States needs to keep ahead or apace of Chinese efforts for scientific, academic, commercial, and military applications. Due to the pace of innovation and economy, the first-to-market advantage here is exponential and will yield near intractable market dominance. The United States is already challenged by the industrial might and growing human resource base of China’s emergence on the world stage. Some of the few, though critical, advantages the United States possesses is dominance in emerging technologies, world-class academic and research institutions, and a central position in information and Internet technologies. If continued Chinese investment in these areas are not met with an appropriate U.S. response, these factors will shift, likely at the expense of the United States, and the strategic balance of power will continue to tilt in China’s favor.

This is not a call for the U.S. to deny Chinese researchers access or to take punitive action against Chinese firms. Rather, it’s a clarion call that the United States should leverage its advantages to restore itself as the innovation powerhouse in this area as it has in many other areas in the past. The shift towards China for quantum information science isn’t the end result of intellectual property theft, espionage, or mergers and acquisition; rather, it largely reflects the high-level support from government, high and consistent levels of funding, and a corresponding lack of these forces in Western countries, including the United States. If these systemic factors are corrected, the U.S. may restore its traditional leadership in this critical technological domain.

To remain dominant in the current information age and coming machine age of warfare, the U.S. military will need to find ways to integrate these technologies where appropriate and establish new technological and operating paradigms to adapt to the potential disruptive changes they bring. This requires staying ahead of foreign efforts, monitoring their progress, and ensuring procurement, acquisition, and planning are properly preparing for contingencies where these technologies are use. Finally, it is apparent that the golden age of intelligence is likely over. Quantum encryption is just one

[57] “Quantum Radar: “Clairvoyant” with Insight into the Future Battlefield” [量量□子雷□达：洞□察未来战场“千□里□眼”].

example of many that show the growing lockdown and securitization of information flows that U.S. national security community and military have taken for granted and leveraged to great effect. Quantum sensing, in its way, also accelerates this trend further. The United States will need to adapt to an information-denied environment both in peace and conflict, one with lowered quantity, quality, granularity, and actionability of information. This puts a premium on processing power and analysis, highlighting why the United States needs to maintain its dominance in quantum computing, artificial intelligence, and machine learning - all of which are critical technologies for this capability.

Part VI. Recommendations:

Technological innovation is at the center of military strength, economic competitiveness, industrial might in the calculus of national power, as evident in the case of quantum technologies. U.S. Congress should first seek to understand the disruptive effects of these technologies and where the U.S. progress stands in comparison to its most important strategic competitors, such as China and Russia. Where possible, the United States should seek to encourage public private partnerships, strategically apportion state-level R&D funding in pursuit of strategic goals, and enable a regulatory environment that guides and supports rather than quashes innovation. The overall intent of this should be to restore and ensure the U.S. lead in technological innovation and military capability.

My recommendations are as follows:

(1) U.S. Congress should leverage tools already available to it to better understand emerging technologies in general, and quantum in particular. Congress should direct the Government Accountability Office (GAO) to prepare a comprehensive technology assessment to study the impact of quantum information science, current areas of federal R&D funding, potential commercial applications, ability for U.S. to maintain its technological edge, and potential legislative and policy options. In the military realm, Congress should direct the Department of Defense's (DoD) Office of Net Assessment (ONA) to conduct a study on strategic implications of widespread adoption of quantum technologies on the part of potential adversaries, including China. In the long term, it may be worth directing the DoD to prepare a yearly report to Congress on status of emerging and disruptive technologies like quantum and artificial intelligence and their potential impact on U.S. operational capabilities.

(2) Congress should consider funding more public-sector research that can shed light into China's development of emerging technologies in the disciplines of cybersecurity, quantum information science, machine learning, and artificial intelligence, for both commercial and military use. Currently, there does not exist a public-interest think-tank on the scale of China Maritime Studies Institute (CMSI) or China Aerospace Studies Institute (CASI) that conducts and publishes public research focused on these information and intelligence aspects of China's rise. For an issue that has received so much attention and stands at the center of U.S. and China strategic balance, policy and public debate should not be so limited by a dearth of information. Congress should direct the Department of Defense or the U.S.-China Economic and Security Review Commission to partially or fully-fund a think-tank by which to study these issues more comprehensively both for the U.S. government as well as the public interest.

(3) Congress should consider restoring funding to the Office of Technology Assessment (OTA), which between 1972 and 1995 assisted Congress by providing in-depth assessments of emerging technologies and relevant, comprehensive legislative and policy options for lawmakers. Current congressional support agencies like the GAO and the Congressional Research Service (CRS) have not been able to fully fill the void in technical expertise left by OTA. Think-tanks, private institutions, and lobbyists offset this lack of expertise to some degree, but are unable to provide the same level of peer-reviewed assessment with the comprehensiveness, timeliness, and depth that OTA once provided. It should be

noted that while Congress has reduced this role, other nations, including China, have promoted the role and influence of parliamentary science and technology advisory bodies. For China at least, this approach has has paid considerable dividends in apportioning state funds towards R&D efforts in support of long term economic and military objectives.

(4) U.S. Congress should direct the Federal Government to establish an interagency Commission for Investment in Strategic Emerging Technologies (CISET) that will be better able to appropriately assess U.S. R&D funding efforts, deliver recommendations to Congress, and coordinate amongst relevant federal agencies in investment into strategic technologies. The White House has previously acknowledged that U.S. progress in quantum information science is limited due in part to institutional boundaries as well as an inconsistency in funding and opportunities for research in this field, largely stemming from poor interagency coordination and lack of unitary direction. Formalizing interagency working groups and giving them the oversight and support of Congress would allow for greater synergy in budgeting for and achieving longterm strategic technological goals and ensuring continued U.S. dominance in these fields. More importantly, it would restore consistency in funding and employ a “whole of government” planning, nullifying advantages of the Chinese approach.

Challenges in tech transfer, recruiting top talent overseas, and workforce and education programs have also been cited as systemic issues that are holding back U.S. efforts in quantum information science. These components strike at the heart of U.S. technological and strategic dominance and are dependent on a complex array of social, financial, and political factors. This reality makes policy recommendations particularly difficult. As such, these issues warrant further study before any sort of concrete recommendations can be proposed to address them in the context of bridging gaps in U.S. development of quantum information science.

PANEL I QUESTION AND ANSWER

HEARING CO-CHAIR TOBIN: Thank you all.

Now we'll turn first to a question from Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for being here, and this is a very wide-ranging topic, a lot of questions but limited time.

So a couple of questions. First, Mr. Brinda, help me, if you can. You say the cloud is mature. We're hearing now about the fog, IoT, et cetera. Where do you see that going? What is the space for that? Have we now sort of maximized the cloud development and it's becoming almost a commodity like, and we're moving on to the next phase?

MR. BRINDA: I would say if you look at the total spend on enterprise IT, it's about a trillion, 1.1, $1.2 trillion of enterprise IT. The cloud drives about 16, 17 percent of that. So I would say mature relative to say quantum computing drives virtually no enterprise. The percentage of that that goes towards quantum solutions in enterprise is zero. So it's mature in that sense.

It is rising. I mean we should see the cloud share of total spend on IT go up to 25, 30, 35 percent over the coming decade. So there is ample room for continued growth, continued innovation. The way that clouds are architected is continuing to evolve, but I think it's more on an evolutionary path than a revolutionary path where we'll see, you know, the kind of step change, dramatic shakeup that you might see happen in computing architecture as if you shift from say a silicon-based computing environment to a quantum computing environment. I don't think the cloud will undergo that kind of transformation.

So there is definitely room for growth. There will be continued innovation, but to put it in perspective, I don't think it's the same as kind of some of the other innovation we're talking about likely to occur.

COMMISSIONER WESSEL: But IoT, et cetera, where do you see that? Is that going to displace or it's going to be compatible? How does all that work?

MR. BRINDA: So IoT, the cloud is foundational to IoT. I think of IoT as the intersection of mobile, of cloud and of big data where you've got devices out there equipped with mobile information sharing capability connected to a cloud so they can access as much processing power and storage as they need, anytime, anywhere, all the time, with, on top of that, analytic solutions that allow you to get realtime insight into the hands of people that want to make decisions based on whatever that data is telling them.

COMMISSIONER DORGAN: Would Commissioner Wessel yield? You're talking about the Internet of Things.

COMMISSIONER WESSEL: Correct.

COMMISSIONER DORGAN: I wonder if we might have a definition of the Internet of Things?

COMMISSIONER WESSEL: Please.

MR. BRINDA: Yeah, it's a poorly defined term as well.

[Laughter.]

MR. BRINDA: So the Internet of Things I think is simply the existence of connected devices out there in the world, trillions of them potentially, and it's fuzzy because while we've always had connected devices out there in the world--we had cellphones around--and so you could say that the Internet of Things began with the advent of a mobile phone, but now you're putting those same kind of telecommunication capability on cars, on satellites, on people, on any number of other things, on our pets, right, and so the Internet of Things simply refers to that network of connected devices that exists and is growing rapidly.

There are industry specific or vertical segments within the IoT market. There's connected buildings, connected cars, connected cities, connected hospitals, so on and so on and so on. But it's all kind of fundamentally distributed, web-connected devices.

COMMISSIONER WESSEL: And it can't exist without support from the cloud or integration is what you're saying as well?

MR. BRINDA: You need the cloud in order to enable all that data to come in, be crunched rapidly, scale up and down.

COMMISSIONER WESSEL: Okay. Mr. Snell.

MR. SNELL: If I could just make a short comment on that with regard to the maturity and disconnect. You know Mr. Brinda's comments have been appropriately focused on cloud. That's what he was asked about. And when you're looking at the providing of these computational resources out to people, those were--his comments were, but where the disconnect might happen is when you look at what are now called these hyperscale companies that have Internet applications that face the web, which spans, you know, Google and Facebook and Microsoft--these are huge conglomerates--where you really get the potential disconnect we were all talking about before our comments is in artificial intelligence.

And a lot of that development is going on primarily at these hyperscale companies, and that does tie into cloud as well as into Internet of Things because now you have this wealth of data that is so massive that it's hard to have any kind of intentional human strategy as to how you're going to approach it.

But if you have a computational approach, an artificial intelligence working on it, then who knows what kinds of insights start dropping out of having my intelligent sprinkler heads connected to the cloud; right?

COMMISSIONER WESSEL: Okay. If there's another round, I'd--thank you.

HEARING CO-CHAIR TOBIN: Great. Next we'll hear from the Commission Vice Chair, Mr. Shea.

VICE CHAIRMAN SHEA: Thank you, Dr. Tobin. Thank you all for being here.

I'm glad, Mr. Snell, you finished your answer with making connections between different disciplines because that's one of the questions I'm going to ask. I'm going to ask two questions, get them all out, and see if we have any time.

But could you just explain the connection between HPC, supercomputers, quantum computing, and artificial intelligence? I mean, for example, will we reach the limits of silicon-based supercomputers and then require quantum-based computers to be the supercomputers? If there are so many different--if we reach new levels of calculations per second, will that machine become self-aware and artificially intelligent at some point? So I'm trying to understand these connections.

And then on the issue of--help us understand why this is really important to the U.S. economic--I'm talking about HPC, supercomputing particularly--why this is important for U.S. economic and national security.

My understanding is that supercomputers are shifting the paradigm. Before we--we historically have done experimentation where we grabbed things, tinker with them, see how they work, and that's how new products get developed. But now we move from an experimentation to more of a simulation approach with these supercomputers, which radically reduce the time to do work, to make decisions, and to bring products, new products, to the market.

So why is this important, really important, to the U.S., both on the security side and the economic side?

MR. SNELL: Thank you.

There are a few different questions in there, and I'll try to just step through them. Starting with the role of HPC and industry, the industrial competitiveness. I'll refer you to an excellent report that was handed out along with the testimony. It's called the Solve report from the United States Council on Competitiveness.

Intersect360 Research worked with the Council on that report, and it directly relates to how the investments in supercomputing at a national level have downstream positive effects on industry, and that includes specific examples of industrial applications for exascale levels of computing.

We were talking about those quintillions of calculations per second and could you really do anything with it? The answer is yes, you can make any of these models higher realism, you can refine the model, you can do more with them until one day we wake up and realize we've reached the end of science, and, you know, we finish that. There is always going to be a harder problem to solve, and that's why we need this level of computing.

With regard to HPC and how it relates to quantum computing and AI, first of all, quantum computing, it does represent a new approach to how these computers could be built, and I think as that is realized, and one of the leaders in commercializing that has been a company called D-Wave in the Canada. They've had some quantum computers out there. People are trying to figure out how to program them. IBM now has some initiatives in this space.

They're going to excel, at least at first and for a long time, in new types of applications that traditional computers have struggled with, in particular, ones where you have a small number of inputs, but have to explore a very large solution space potentially. So good examples are in material science, for example. You have only a certain number of places a molecule might interface with another molecule, but a large number of--sorry--only a small number of molecules, but a very large number of ways that they might interface with each other, and a quantum computer might provide an advancement in how that gets done.

I don't think they'll displace what you'd call conventional computers any time within our planning horizon, but you should still keep going after them because they could really excel in a new area.

And then finally with respect to artificial intelligence, self-awareness is just a tricky concept, and for me I believe that the computer does what you teach it to do. We can probably create computers that will mimic intelligence quite well. When it mimics intelligence to where you can't tell whether it's actually intelligent enough, now you have a philosophical question here that I'm not prepared to answer in this testimony.

But with regards to AI, most of the research has happened so far at what we call the hyperscale companies. That would be the Googles, Microsoft, Facebook. There are some in China--Alibaba, TenCent, and Baidu--that have pushed a lot of the research. Those applications have a lot in common with high-performance computing, and they use high-performance technologies in addressing what they refer to as the training and the inference of these AI models.

There are people who would like to count that as part of that HPC market. We look at that in great detail and count it as part of the hyperscale market today. That might change in the future, but we see it as part of the hyperscale market. Now it is related because you see technologies coming from companies like Intel and NVIDIA and others that are going into those AI applications at the hyperscale companies. There's going to be a wealth of development in AI over the next couple of years. It's going to be one of the biggest changes in IT that you'll see over the next decade.

VICE CHAIRMAN SHEA: Thank you.

MR. COSTELLO: If I may jump in from the quantum side. So quantum has a number of applications, and just I'll piggyback off of Mr. Snell's comments. Quantum computing is a different type of computing, not a sort of end evolution of traditional forms of computing. And it has to go through that development cycle. It's pre-competitive. We're still on basic fundamental research and applied research right now.

But, and as a sort of form of computing, it does have applications to the cloud. D-Wave is certainly a company that is doing that right now with a type of quantum annealing, which is not quite full quantum computing capability, and IBM right now apparently has a five qubit quantum computer that you can play with over the Internet to develop algorithms for.

There is such an idea as quantum AI, which let's not even get started on that. That's a whole separate thing. But, you know, also, quantum, one thing that sort of hasn't been, wasn't touched on in my testimony because it gets into very complex topic is also quantum simulation, the ability for a quantum computer to simulate large-scale systems, which include classical computers.

So essentially building, simulating a standard computer within a quantum system. That is also additionally another application of quantum computing.

VICE CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR TOBIN: Great.

Commissioner Slane.

HEARING CO-CHAIR SLANE: Thank you.

Mr. Snell, if I understand your testimony, it now appears that China is the leader in HPC, and following up Commissioner Shea's question, I'm trying to understand what that means for our country. Does it really make any difference whether we're second or close first or--can you help me with that?

MR. SNELL: Yes. Thank you.

First of all, with regard to leadership, I think it depends on how you measure leadership. China certainly has the two largest supercomputers in the world right now or two most powerful, and I think that's undisputed right now. The U.S. still leads in terms of the most technology sold, the most technology used, but it's that apex of the industry where China has really made its investments.

Does that matter? Yes, absolutely, it matters a great deal, and not just for national security but in terms of how these technologies eventually get commercialized. Now there's certainly the possibility that China or the United States or any other country, for that matter, is in possession of technologies that are not being commercialized because they're protected for national interests. They become classified systems.

And that's another interesting feature of this Sunway TaihuLight system in that it's built entirely from these indigenous technologies that are currently noncommercial. When the U.S. Department of

Energy, for example, buys a supercomputer, it's buying the technology from companies like IBM or Intel or others that have every intention of commercializing that technology and selling it in other places, and they would hope to sell it even beyond the U.S., in other countries as well.

That same dynamic might not be at play in China right now. If China is developing these supercomputing technologies, and it seems they are, it's not clear at this point to what extent those technologies will become commercially available, certainly worldwide or even within China.

It's not as free a society. It's not as free an economy. It's certainly not as free speech or free press so it's hard to monitor exactly what's going on behind all of those walls. I think it does matter a great deal, and it becomes more and more difficult to assess to what extent the Chinese technology leadership is currently ahead or in a position to go ahead in the future.

HEARING CO-CHAIR SLANE: Is the ability for us to stay in the lead, is that a function of R&D and funding?

MR. SNELL: Yes, it's a function of R&D and funding. Now one advantage that the United States has is in its economy and the wealth of small startup companies that are all chasing the next great idea that will really be a game changer in high-performance computing or hyperscale or artificial intelligence or other markets, and these companies either get grants from the DoE or they might get bought by a larger company and improve their--improve their exposure. Or some of them just start making commercial sales.

I could point to several small supercomputing companies that are nevertheless extraordinary in having unique technologies that are not mimicked by their larger cousins in the industry, and the U.S. has a disproportionate amount of that.

HEARING CO-CHAIR SLANE: Mr. Costello, your testimony was more disturbing.

[Laughter.]

HEARING CO-CHAIR SLANE: Really for us to stay ahead, I think one of the things you're suggesting is to increase funding DARPA, another one of our agencies.

MR. COSTELLO: I'm suggesting a consistent level of funding. What you've seen is, is China has created a positive consistent capacity that has been like a flame to moths frankly for anyone who is willing to undertake this research.

I think that, you know, our private sector is, are engines of innovation. There is no doubt about that. But that's where, only in sectors where there's sort of I think anticipatory commercialization of technologies. Government is there to kickstart that innovation in certain areas, and I think quantum, specifically certain fundamental research and applied research for quantum technologies is one of them.

You need some basic level of R&D funding to create a capacity that the private sector can then commercialize and allow a sort of VC, a venture capitalist, to take over in the type of entrepreneurial spirit. But unless that sort of foundational capacity is there, I don't think you're going to get there.

I mean so the White House report last year was very informative in understanding why sort of the U.S.' lead in quantum has dropped off. It's honestly from a lack of coordination. Certain programs, as agencies, as programs at certain agencies have fallen over time, there have been gaps or holes or varying levels of consistency in funding. It's forced people to look elsewhere or to change their careers.

HEARING CO-CHAIR SLANE: Thank you.

HEARING CO-CHAIR TOBIN: Senator Dorgan.

COMMISSIONER DORGAN: Thank you very much.

I was interested, Mr. Snell, in your testimony, you described to us teraflops and petaflops, and I was thinking in, I used to chair the appropriations committee that funded National Laboratories and was at Sandia one day, some many years ago, when they had announced the teraflop.

MR. SNELL: Teraflop, yes.

COMMISSIONER DORGAN: And I believe they said it was a trillion discrete functions per second.

MR. SNELL: Yes, a teraflop is a trillion.

COMMISSIONER DORGAN: And they said so we have a teraflop, we've done a teraflop, and they said some day we will do a petaflop.

MR. SNELL: Yes.

COMMISSIONER DORGAN: And I said what is that? They said that's a thousand trillion discrete functions per second.

MR. SNELL: Right. A thousand teraflops.

COMMISSIONER DORGAN: And my question was how would you know?

[Laughter.]

COMMISSIONER DORGAN: But they assured me they would know. And then I watched. I watched as we had what was considered the most powerful supercomputer in the world when they finished the Roadrunner at Los Alamos, which was quite exciting for about two months or maybe three months, when we were told that it is no longer the most powerful supercomputer in the world.

So I was looking at your testimony, and, you know, you describe a circumstance where the National Computational Center in China has computing capability of 125 petaflops. The Oak Ridge has 27. That's about one-fifth of what they have at the National Computing Center in China.

And I also noted that the three systems you described as the top systems in the U.S. are largely driven by defense interests, by our defense interests--Oak Ridge National Laboratory, Lawrence Livermore, Lawrence Berkeley, Los Alamos, and so on.

And then I see on the list other systems, and included there is Switzerland. Now obviously Switzerland doesn't have a big defense commitment to try to drive high performance computing. So I'm sorry for the lengthy question, but it occurs to me that we're driving this largely in this country on defense issues, which is, I mean that gives us great progress. Is China driving it largely for defense purposes as well? And describe to me how Switzerland gets in the mix.

MR. SNELL: Okay. Sure.

COMMISSIONER DORGAN: And anyone of you can comment on that as a pretty general proposition.

MR. SNELL: And yes, you're right. This does race ahead very quickly. For any supercomputer to stay on top of the heap for longer than a year, year-and-a-half, is rare. Now, China has managed that trick twice in a row now, first with the Tienhe-2 system and then getting exceeded by the Sunway TaihuLight system, which is why the number one supercomputer in the world has been in China for the last four years, and likely will continue, at least on the next semiannual list.

How does Switzerland get into the mix? That's a system at CSCS, which is a research center in Switzerland. If you put me to what it stands for, it's something in French, Computation Scientifique something, something. It's tied in some extent to CERN, which is in Geneva, and the particle acceleration that they do there.

The top supercomputers are often related to investments in energy. The ones that you mentioned in the United States certainly have DoD interests, but they're at Department of Energy labs. The largest one in France, for example, is at CEA, which is the Atomic Energy Commission. It's just backwards because it's in French, Commission Energie Atomique--right--in France. We see that quite a great deal.

In China, the largest industry that's going to be using supercomputing is, again, energy. There are oil and gas interests in China, and they need those supercomputing efforts. There are also very large meteorological supercomputers.

Now the number of supercomputers in China that they say are dedicated to meteorological research, they probably don't really need that many weather supercomputers, and we can infer that there's a lot of national and military defense research going on those supercomputers. That was, in fact, behind the relatively recent U.S. export ban on certain processing technologies that were going into the planned upgrade for Tienhe-2 system for those chips.

I'm sorry. You had a follow-up.

COMMISSIONER DORGAN: I was just going to say, I mean I soaked up most of my time with my question, but when they talk about 125 petaflops versus 27 at Oak Ridge, it's a five-to-one advantage. Should that mean something to us? I mean I understand if we were close, but a five-to-one advantage is pretty substantial.

MR. SNELL: It is substantial. Another way to look at it is that the top two United States systems combined would only equal the computational performance of the single second largest supercomputer in China. It is a substantial advantage at the top of the supercomputing market, yes.

COMMISSIONER DORGAN: And what accounts for that, do you think?

MR. SNELL: Investment. And the fact that developing a Chinese national supercomputer has now become an internal affair where they weren't buying it commercially. The money was going to developing it internally. So we've seen a price tag of $300 million for the R&D effort, but that can't be thought of as a retail price for a supercomputer because nothing was bought. They built it internally. They're paying people.

So that's entirely different from buying a supercomputer from somewhere. It's hard to even track where would we put that money in our overall market model. They didn't buy anything.

COMMISSIONER DORGAN: Let me apologize for the time. Perhaps as we go along this morning, you might answer the question, most of us have seen the inability to protect intellectual property with respect to doing business in China, and I'm wondering whether the ability to build in a high- performance computing area has in anyway related to the acquisition of intellectual property through other than developmental means in China? So just you might want to comment on that as we move along.

MR. SNELL: I know Mr. Brinda had a comment.

MR. BRINDA: No, no, you go ahead and please respond to that.

MR. SNELL: Sorry. With regards to the protection of intellectual property, so traditionally a supercomputer was a relatively self-contained device, and if you wanted to control export of U.S. technologies to other countries, you could say, well, Cray or IBM, you can't go export that supercomputer, and you put a limitation on it.

The cluster revolution we are talking about in the mid-'90s, starting in the mid-'90s, changed that a little bit because people could built a network of computers on some interconnect, and that made supercomputing more accessible to anybody with the wherewithal and the budget.

You could still control individual technologies like individual processing technologies or networking technologies, but now ever since that most recent export ban, China accelerated its own indigenous efforts to where most of that computer, the Sunway TaihuLight, was entirely internal technologies.

The most significant area where I'd say China is behind the United States is in networking technologies. For the Sunway TaihuLight system, they did buy networking silicon chips from a company called Mellanox, which provides InfiniBand technologies. It's a dominant networking technology for supercomputer systems.

Now, they built something of their own from them, but we can infer that the network for that system is inherently something like InfiniBand, and that they probably wouldn't have been able to build it without the silicon they acquired, at least not in the same time frame.

MR. BRINDA: Sorry. The quick comment I was going to--I mean I've always likened the HPC race to sort of who's got the tallest building, and mine is two stories taller, and yours is now five stories taller. It doesn't really matter who's got the tallest one. The concern here is that because of the proprietary homegrown chip architecture they've invested in, and I'm sure the advantage around the networking side they're working to close, that they eventually sort of now can build buildings with a different set of materials, right, that allow them to build five times as tall and just stay permanently ahead.

That to me, the shift that we've had in the last couple of years with the Sunway system and the fact that it's homegrown, are we going to see a more permanent edge by the Chinese in the HPC space? And I don't have the answer frankly. But I do think there's a fundamental difference.

HEARING CO-CHAIR TOBIN: We have more questions. Commissioner Chairwoman Bartholomew.

CHAIRMAN BARTHOLOMEW: Thanks very much, and thank you to all of our witnesses.

Once again, it feels like we're in a room filled with rocket scientists, and we are struggling, struggling to keep up. I would note that I never really expected that I would be referencing Mark Cuban here, but Mark Cuban, of course, has recently said that he thought that the first, the world's first trillionaire will be coming out of the AI community. So I think that he's really definitely focusing on the importance of that.

There's so much to talk about here. Mr. Brinda, thank you, in particular, for noting the impact of immigration restrictions. I mean again it's recently come out that 83 percent of America's top high school science students are children of immigrants, and we are cutting off our nose to spite our face when we are going to crack down on immigration on these issues.

I, also from my colleagues, I know a little bit about annealing because of metallurgy, but Mr. Costello, I just used my handy computer to look up quantum annealing, and I don't have a clue. So that's a separate thing--the concepts that you guys bring in.

But I guess what I really wanted to ask about, when we scheduled this hearing, we did not know that the president's budget was going to be coming out today. And I would like to understand more building on what Commissioner Slane asked about how important is the role of the U.S. government in ensuring that we have any competitive advantage in any of these sectors because if you look at what the president is proposing budget-wise, funding for science and tech is just going to be slashed.

So what is our future and how important is the U.S. government role in basic science and all of these things? For any of you. For all of you.

MR. BRINDA: I'm happy to comment first. In cloud, I don't think it's very important, and it's I think a different answer from my colleagues on the panel here. The government is not funding innovation in enterprise cloud computing. It's really a private sector led initiative, and cloud can actually help save the government money by making IT more efficient, and investments in leveraging cloud technology actually could be a source of very modest savings on the scale we're talking about.

But I don't think that we're at risk of sort of damaging that industry through just spending cuts alone, but let me let others comment because I think the answer is different elsewhere.

MR. COSTELLO: I'm not going to comment on the president's budget, or proposed budget rather, but I will say this as a general matter. Technology innovations stand at the core of national power, economic and military, and science and technology is a huge part of that.

A new approach is required, I think, than one that we've had before. We do need greater R&D funding for basic stuff, things that are--that are precompetitive, things that don't have sort of apparent commercialization.

I think that certainly needs to continue, and everything I've read and research that I've seen discusses that the consistency and reliability of funding is absolutely paramount in that. So--and not just for defense purposes but also for broader science and technology efforts.

MR. SNELL: In supercomputing, the government investment is critical. That's where it comes from at the top, and I have not seen the new budget today. I've been traveling to get here. But I had heard a discussion that the ASCR budget under the Department of Energy might be reduced to levels to about ten years ago.

Now, ten years ago wasn't the dark ages, but ten years ago, a lot of U.S. supercomputing was also joint funded by DoE and DoD through DARPA and the Distributed Shared Resource Centers, the Major Shared Resource Centers.

So today it's funded primarily through DoE so if you're also reducing that budget back and not replacing it elsewhere, it would have a substantial impact on supercomputing at the high end. These top supercomputers are all at DoE labs, and if you refer to the Solve report that I mentioned before, there's a lot of discussion in there about how that technology transfers from the National Labs to U.S. industry and how reliant they are for that level of investment.

CHAIRMAN BARTHOLOMEW: Thank you.

Mr. Costello, one thing, as you talk about consistency of funding, I want to tweak your message just a little bit that there needs to be consistency of funding with funding, not consistency of funding--because you can do consistency of funding at a very low or insignificant level, and I understand that consistency is important for research purposes, but the funding piece of that equation also is important.

MR. COSTELLO: Oh, excuse me. Consistency and level of funding.

CHAIRMAN BARTHOLOMEW: And level of funding.

MR. COSTELLO: Yeah.

CHAIRMAN BARTHOLOMEW: Okay.

MR. COSTELLO: I think, yes, definitely.

CHAIRMAN BARTHOLOMEW: Okay. All right. Thank you.

HEARING CO-CHAIR TOBIN: Great. It's my turn, and I have a wish that we had a blackboard like in the old days where you could put all those zeroes behind it because, as you said, Commissioner Bartholomew, there's a lot of learning that is going on for us regarding the science.

The quantum area is what I want to focus on. Reading your material, we understand that quantum computing doesn't rely on what we're used to--the zero and one--that it can kind of move in between. I'm going to ask two things. Can you describe that a little bit more clearly so that those of us learning this area can better understand, and, secondly, talk specifically about how that would serve us in terms of cybersecurity because that to me sounded like, one, an area where we could use it to prevent access, and number two, that is an area where we might well get funding.

So, Mr. Costello, I direct that to you on quantum, please.

MR. COSTELLO: Quantum computing allows, due to entanglement and superposition, using qubits to perform calculations. You can perform a number of parallel calculations at the same time that enables exponential increase in processing power. That can be used for a variety of different applications. Mr. Snell mentioned a few. I won't go further into that.

The question of whether it's applicable to cybersecurity, that's not entirely clear. The total number of applications for quantum computing haven't even been thought of because I think there are so many. The type of capabilities it sort of enables haven't been fully thought out, the full implications of which have yet to be seen. It's still a very nascent science, and applied technologies here are proceeding very slowly, but I suspect that in ten, 15 years, they will begin to proceed very rapidly as basic engineering questions are answered.

If you'll forgive me, what was your second question?

HEARING CO-CHAIR TOBIN: Now I have a third question for you. If there is quantum computing occurring here, say at Department of Energy, and quantum computing occurring in another location of the Department of Energy, is it the same? Do you use software to think about this too or is it just the CPU power?

MR. COSTELLO: So there is engineering issues with just creating qubits. So you have to understand that qubit is an idea. It's not a specifically engineered. It's not sort of a complete concept. You have to engineer a qubit, and there's different ways to do that. Scaling up--

HEARING CO-CHAIR TOBIN: That's helpful.

MR. COSTELLO: --is the problem.

Now, for cybersecurity, I will say--and then on top of that, you have to figure out correct algorithms in order to actually be able to harness those qubits in any sort of meaningful way. So there's a software problem as well.

So I mean we're creating an entirely--people are creating an entirely separate, you know, computer science ecosystem in that everything from, you know, base hardware all the way up needs to be created on top of that.

As far as cybersecurity, quantum encryption does hold promises for cybersecurity, but there are challenges there both technically and logistically. Technically, there are some issues with quantum key distribution, with--there's some just very heavy technical issues China is trying to surmount. Logistically it's hard to scale meaningfully.

You cannot--there's such a thing called the no-cloning theorem, and I won't, just for the record, I'm not a quantum physicist.

HEARING CO-CHAIR TOBIN: Yes.

MR. COSTELLO: But there's such a thing as a no-cloning theorem, which you cannot copy a quantum state. Now our fiber-optic networks use repeaters to boost a photon traveling over that is carrying--the signal driving all that carries information. It gets very complicated when you need to copy a quantum state and then forward it on because technically, you know, by the laws of physics, you can't do that. There are ways to go around doing that, but that opens up vulnerabilities.

HEARING CO-CHAIR TOBIN: So perhaps you could think about, not here for this moment, but by getting back to us, what you said about consistent level of funding, what might that be in terms of quantum computing? How would you try to narrow where you would want that investment to be made?

MR. COSTELLO: Absolutely. So I think as far as private funding goes, quantum computing is pretty healthy. Could definitely stand to benefit from more. I think any area in which there is no clear commercial--anything that's not going to be attractive to investors essentially, the United States can play sort of a key role--underlying foundational technologies, other research in quantum encryption and quantum sensing, which will bear dividends for quantum computing, you know, I think engineering, sort of the engineering level.

The problem is we don't have the answers, and you cannot give a treatment without the diagnosis. This does need more research in what sort of role the government can play.

HEARING CO-CHAIR TOBIN: Got it. And that's why you suggested the assessment. Okay. Now let me--we have so many questions. Senator Talent.

COMMISSIONER TALENT: Thank you.

If the three of you could summarize what you believe the strengths of the Chinese system and its weaknesses are in your areas. You've each touched upon them in various fronts. I think it would be helpful for us in our report if you summarized it.

Second, Mr. Costello, you've made a distinction between funding basic research and research that's aimed at some commercialization. And you feel that the government has an important role to play in basic research, with which I agree, but I also, it's my experience over the years both in the Congress and out that basic research should be funded with some end in mind, not commercialization but some problem that seeks to be solved. Otherwise it's pretty inefficient. Would you agree with that?

In other words, it's not just okay except maybe in some mathematical sorts of pursuits. It's not some kind of brain game, and so the government is seeking the solution to some problems. And not commercialization, but some problem. I want to refine our recommendation on this, if you agree. So whichever order you guys want to take. The first question was for all three, if you--

MR. SNELL: So with regards to the Sunway TaihuLight system, in particular, which is the Chinese technology, the most interesting thing about it is the processing element itself designed by Sunway. If memory serves, it's a 260 core processor. They refer now to processor cores, how many processing elements you put on a die. That's been going on throughout the computing industry here.

COMMISSIONER TALENT: I wasn't clear enough, I think. When I said the Chinese system, I mean the Chinese system for making funding decisions.

MR. SNELL: I beg your pardon. Sorry.

COMMISSIONER TALENT: Yeah. In other words, it's a, it's a more state-dominated system that works through SOEs. It's a more closed system. I mean there are certain aspects of it that are obviously different, and clearly they've been doing a lot with that system. But if you could step, go to 30,000 feet and say--

MR. SNELL: Sure.

COMMISSIONER TALENT: --going forward, this is, this is where we think the Chinese system will benefit them in your areas and this is where we think it will make it more difficult.

MR. SNELL: I beg your pardon, Senator, for misunderstanding your question. Yes, the Chinese system for investment, one key differentiation there is that we do see a trend toward centralization. The Chinese government seems to prefer fewer centralized systems as opposed to enabling technologies to be distributed throughout the economy.

So rather than seeing individual high- performance computing systems proliferating through Chinese manufacturers and oil companies, I think they would probably prefer to see a centralized investment where they have a single huge supercomputer and then provide access to it. That allows them to control investment and access a little more tightly, and that is in contrast to a U.S. model that's going to be a little more around commercialization.

I would like to make one brief comment from the previous question with regards to supercomputing, quantum and cybersecurity, that's reflected in my statement, which is we kind of talk about with cybersecurity. Supercomputing certainly is involved in cybersecurity, but it's actually a little more related to cyber-attack.

You can use quantum computers and supercomputers to hack systems and break passwords, and I think there's a lot of potential there.

MR. BRINDA: With respect to cloud strengths and weaknesses, let me start with weaknesses actually or areas where the U.S. has an advantage.

One is just the lack of talent and immaturity of the Chinese market around software and services. These are where the profits are. There is just, because of the piracy that has been mentioned previously, Chinese companies don't spend on software. There are therefore a dearth of developers, and for clouds to really work within an enterprise, you need that skill set. You also need service providers to go and implement and manage those cloud environments, and this service sector, IT services sector, in China, is also quite immature.

The second weakness I would say is there's a lack of a middle market and SMB segments of the market that in the United States are among the first to adopt cloud. They tend to be newer businesses with less inflexible systems of record that have been around for decades and decades that can't be moved to the cloud, and that is spurring innovation in the U.S. and in other markets where those kinds of firms exist.

What I think the Chinese system does do well is, one, it's a very large economy that theoretically could support very large volumes of IT spend, and they have very tight controls around participation within that market, and so you've seen, Aliyun is a good example where some early protections create an environment where a local player could grow, get to scale, and now actually I think holds its own on certain dimensions versus global players like Amazon and Azure and so forth.

So the potential for a domestic market, and there is a scaled domestic market for that infrastructure layer in China where Aliyun participates, the potential to protect local players and create that, I think that's a key difference in strength that, you know, we typically don't establish such rigid protections, if that's helpful.

MR. COSTELLO: So I'd sort of turn your question on its head a little bit. I will talk about what China's advantages are and how those are also disadvantages. China's approach to R&D funding is very centralized. It's very comprehensive. It's very long-term. They've got easy tech transfer mechanisms of state-owned enterprises, but this makes them inflexible. It makes their program incredibly opaque, and frankly it creates a level of distrust when undergoing international cooperation, not only in how certain technological and research advancements may be commercialized but where they may end up.

As far as objective, I take your--you're absolutely correct. We shouldn't, I don't believe the U.S. government should ever throw, sort of throw money at a problem. I think that, you'll note in my testimony, I think the United States, the government, needs--with Congress, I mean the federal government and Congress need to take a comprehensive look at what long-term objectives are, how the United States wants to, key areas, technological areas, where the United States wants to be a key leader, and then look at strategic emerging technologies, how it can partner with a private industry, and how it can apportion R&D funding strategically to support both economic growth, technological innovation, and, where appropriate, military applications of these technologies. But again all this follows through priority and objectives.

COMMISSIONER TALENT: Thank you, Madam Chair.

Yeah, that's the point I was getting at, and it's one of the reasons I think that DoD R&D and DARPA funding has synthesized this process so well because obviously they don't have market objectives, but they have objectives, and so I think that kind of funding tends to work more effectively. And then, of course, you get enormous unanticipated spinoffs to the rest of the economy. That was the point I was making.

Thank you.

HEARING CO-CHAIR TOBIN: Thank you, Senator. Thank you, gentlemen.

Now to Commissioner Stivers.

COMMISSIONER STIVERS: Thank you all for being here this morning.

Each of you have made recommendations calling for U.S. government support to investors or continued support for your sectors in some manner.

Can you kind of describe what happens if the U.S. were to pull back in those areas or not fully fund those areas? Can you quantify for us the consequences of doing that vis-a-vis China in each of your areas?

MR. SNELL: Well, from a U.S. perspective, it would stifle innovation in some sense. Now high-performance computing will continue to go forward, and that's true in industry. It's true in academic research, and it's hard to quantify what happens when you slow down scientific research.

In essence, you get to your next "aha" insight and great scientific achievement slower; right? And that's hard to measure exactly what effect that has on people's lives or the economy or what have you.

Now what will happen in the long run is that those technologies will come from, to a greater extent, from countries outside the United States. So if you have Chinese or French or German companies who are building supercomputing technologies, then U.S. companies will want to acquire those technologies somewhere else, and you'll also have more scientific achievement coming from other countries relative to the United States.

What that means from a national security perspective I'll leave that to the National Security Council and others to comment on what happens if other countries have better supercomputing capabilities than the United States has.

I'm not at war with any of these countries myself. I have clients in all different countries so from that sense, from a professional perspective, I'm not on any particular side. But, you know, there would be a significant long-term deleterious effect on national competitiveness without leadership in high-performance computing.

COMMISSIONER STIVERS: Thank you.

Mr. Brinda.

MR. BRINDA: The nature of the government investment in cloud is I think different than in these other sectors, right? We're talking about the government leveraging cloud solutions for its own internal computing needs. That's really the main nature of investments that the government makes into cloud. It's not like we're funding early stage research or coordination across players in industry. That's all happening by the private sector and should continue to happen.

I think, look back at the CIA's use of Amazon Web Services, there was a contract put out to bid in 2014, I want to say. AWS won that against IBM and a number of others. That was a turning point for the public cloud industry.

So I don't want to say that the U.S. government investing in cloud solutions to solve its own IT problems is not important. It absolutely is and was in that case and I think can be going forward. And there's a win-win scenario here. I mean we should be leveraging private and public cloud solutions in our government IT environments as much as possible, and that will create proof points for industries, for companies that might be hesitant because of security or privacy concerns. Well, if it's good enough for the CIA, it's got to be good enough for me is kind of the logic.

And the amount of spend that the government makes on IT solutions for its own computing needs is enormous, and that can spur innovation in particular sectors. I would say private cloud in particular is one that that would be the right solution for many government problems in IT, and there has been a dearth of private sector--the innovation in the private sector has not solved all the problems of industry around private cloud, and the government, you know, putting a concerted effort around investing there to build out private clouds could create solutions that would be more--that would be applicable and usable across industry.

COMMISSIONER STIVERS: Thank you.

Mr. Costello.

MR. COSTELLO: What the effect will be with regards to China, I go into I think pretty, pretty good detail in my written testimony on strategic implications, particularly military.

I think as a more general note, I think pulling back R&D funding, I'm not entirely certain what that effect would be on quantum computing. I think the market applications are so obvious and honestly so attractive that I think it would continue to get plenty of investment and innovation may continue.

Innovation, pace of innovation may slow down, but I think it will continue even most likely ahead of Chinese efforts.

But as far as quantum encryption and quantum sensing, it's not entirely clear. I think first-to-market advantage here for any country or any corporation that is able to, you know, sort of bring these technologies to market I think will be incredibly immense for quantum computing.

So I suppose the real question is, is the United States sort of pulls back R&D funding and another nation, for instance, China, who certainly has the funds and the willpower and the objective to be a leader in some of these fields, if they get to first-to-market advantage, they'll be able to sell those technological solutions to our firms and to us, and that will put them definitely in a huge economic advantage in what very may be a new and burgeoning field of information technology.

COMMISSIONER STIVERS: Great. Thank you.

HEARING CO-CHAIR TOBIN: Thank you.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all.

Let me go into, if I can, more the national security related concerns here. And Mr. Snell, as I understand it, you know, at the, not the top end but the commercial end, let's say the commercial space for high-performance computing, you know, you have your Cray, IBM, et cetera. You also have Huawei and some Chinese players.

My understanding--correct me if I'm wrong--is that each manufacturer, each developer, has to have some unique software development that applies to its machine. It's not like a basic Dell versus a Gateway, HP, whatever, that you can run Windows 10, et cetera. That to make these things work, there is certain discrete designs around those.

That to me raises enormous cyber concerns. I don't know that, you know, based on former, previous work by the House of Representatives on Huawei, the threats of Huawei, I don't know that I'd want to have a Huawei HPC in a U.S. company where its intellectual property is its crown jewel because of the sales and follow-on servicing that would be unique to the HPC, the Huawei HPC. Am I correct in that in terms of the unique nature and the ability, the source code, all the various other issues?

MR. SNELL: Right. So thank you for the question.

Throughout the industry, the dominant operating system, first of all, for high-performance computing is the Linux operating system.

COMMISSIONER WESSEL: Understand.

MR. SNELL: As opposed to Windows.

COMMISSIONER WESSEL: But it is tailored to each machine; correct?

MR. SNELL: It can be. That is becoming more true again now. We really have gone through different eras of architectures, as I mentioned before. We had an era where supercomputers were largely self-contained but architecturally distinct, and an IBM was very different from a Cray, was very different from Sun or something.

And then the cluster revolution brought us to an era where the technology was disaggregated into industry standard components.

COMMISSIONER WESSEL: And that was the parallel.

MR. SNELL: Right. I build a parallel computer--

COMMISSIONER WESSEL: Right.

MR. SNELL: --from a lot of Intel or AMD servers, and I run Linux on it so now it's disaggregated and all architecturally the same. I might have exactly the same setup on all of them.

Now with specialized processing elements coming in, the different types of multi-core and many-core processors, ARM processors, POWER, the Sunway system, FPGAs, GPUs, we're really going into what from a programming standpoint is kind of the worst of both worlds. It's still technologically disaggregated and it's architecturally distinct.

So it's going to become harder and harder to compare performance on one custom architecture versus another because they might be set up for very different purposes.

COMMISSIONER WESSEL: But in the national security related field, to me, that would magnify the concerns about the home country of the producer and cyber concerns that might come out--the ones we've been having of late.

MR. SNELL: It does. Huawei and also Lenovo are major HPC providers that sell on an international level. Within China, Inspur is probably the largest provider, but they don't sell as much outside of China.

Now we also had this level of national discourse when IBM sold its PC and printer division to Lenovo, and everyone said at that time that it was the last PC that IBM or that division would ever sell into the U.S. government. And that remained true for roughly seven years before you started seeing Lenovo PCs starting to show up in U.S. government.

Commercial largely doesn't care. If commercial used to buy IBM and now those Intel-based servers have been sold to Lenovo, which happened recently, well, I'm just as happy to buy from Lenovo, but if they weren't on my vendor list, you have to recompete, right, to go get the business.

So Lenovo, Huawei and others will compete for commercial and even academic business. It will be very difficult for them to compete for government business in the near term, for exactly the concerns that you brought forward. I think people are very worried about that.

COMMISSIONER WESSEL: Let me just in closing, for the Lenovo comment you just made, that's true for the non-secure parts of the U.S. government.

MR. SNELL: Understood, yes.

COMMISSIONER WESSEL: DFAR regulations were changed to allow the procurement authorities to look at the home country of the producer no matter what system was going on at DoD.

MR. SNELL: It's also important to note--I appreciate your comment-- that even among these large American companies, they're multinational organizations.

COMMISSIONER WESSEL: Right.

MR. SNELL: An Intel processor might be fabricated in China.

COMMISSIONER WESSEL: Understand.

MR. SNELL: There's a large complicated supply chain for any of these companies, and it becomes increasingly difficult to think of them as exclusively American or exclusively Chinese companies. The Lenovo high-performance computing group is all still based in North Carolina.

COMMISSIONER WESSEL: Yes, but the patching, et cetera, all occurs, as you know, out of China.

MR. SNELL: Yes, I'm aware.

COMMISSIONER WESSEL: That's the first thing they changed when they bought IBM is, before they needed to, moved all the patching to Shanghai.

MR. BRINDA: There does seem to be some inconsistency in this of we won't allow telecom equipment from Huawei to be deployed by Verizon, but we will allow certain other technologies to be used in sensitive parts of the economy or the government.

I'm not an expert on the security risks posed by different technology segments in different applications of the economy, but from my vantage point, it does seem like there's inconsistent standards.

MR. SNELL: You raise an excellent point, Commissioner, and that is a significant concern from a security level as to where the components come from, where the parent provider is located, and it is becoming as difficult for the U.S. based vendors to compete in China as it is for the Chinese vendors to compete in the U.S.

COMMISSIONER WESSEL: Understand. Thank you.

HEARING CO-CHAIR TOBIN: Thank you, Mr. Snell, Mr. Brinda, Mr. Costello. Oh, one further thought to Commissioner Wessel.

MR. COSTELLO: One further thought. I would be remiss. Mr. Snell, I got to hand you credit for bringing up the encryption cracking issue. This has been one of the biggest--as you noticed, my oral testimony did not get into use of quantum computing to crack encryption. That's for one major reason: I think that is way, way, way overhyped.

I think it is a call to increase our own domestic encryption standards. I think it was 2015 or 2016, the NSA sweeping encryption, said we need to move towards quantum resistant encryption, such as lattice-based encryption or higher forms of encryption. I think that's true.

But if you look at even the most generous estimates for a general use quantum computer to be able to crack modern forms of encryption, it is still within a timeframe by which we can evolve to better standards of encryption. So while I think that is something that we should talk about, we should not have this spooky danger of quantum computing, you know, cracking all the encryption everywhere. I think it just means that we need to move towards better encryption standards.

HEARING CO-CHAIR TOBIN: Once again, thank you, gentlemen. I come away from this morning's first panel saying we as a country have to hold up the mirror, keep our eye on the ball. We'll be able to showcase your recommendations going forward. Thank you very much.

We'll reconvene in ten minutes at 11:15 for a discussion on robotics.

MR. BRINDA: Thank you.

MR. SNELL: Thank you.

[Whereupon, a short recess was taken.]

PANEL II INTRODUCTION BY COMMISSIONER DANIEL M. SLANE

HEARING CO-CHAIR SLANE: So we're back in session for our second panel, which will assess China's development of industrial, military, and nanorobotics and their impact on U.S. competitiveness and national security.

We'll start with Henrik Christensen. Dr. Christensen is the director of the Contextual Robotics Institute and a professor of computer science at UC San Diego. He has led robotics policy discussion in the United States and the European Union, most recently serving as the principal investigator for the 2013 and the 2016 U.S. Robotics Roadmap, the Army Research Laboratory's Micro Autonomous Systems and Technology Collaborative Technology Alliance, and the Robotics-Vo.

His research has involved collaboration with numerous leading global robotics firms and customers such as ABB, KUKA, iRobot, Apple, Boeing, General Motors, BMW, et cetera, and led to more than 300 contributions across robotics, vision, and artificial intelligence.

Next, we'll hear from Jonathan Ray, who is an associate deputy director at Defense Group Inc. He specializes in China's science and technology industry developments, to include research on semiconductors, hypersonic weapons, robotics, unmanned systems, nuclear weapons, and space military doctrine.

Mr. Ray co-authored a Commission-contracted report that was released in October 2016, entitled China's Industrial and Military Robotics. This report can be found on our website at uscc.gov.

Finally, we have Dr. Patrick Sinko. Dr. Sinko is a distinguished professor of pharmaceutics and drug delivery and an associate vice president for research at Rutgers University. Dr. Sinko has served on numerous scientific advisory and review panels in China, Korea, Europe, and the United States, as well as on editorial advisory boards for many scientific journals.

His current research focuses on nanobiotechnology drug delivery with specific applications to the treatment or prevention of HIV/AIDS, breast and lung cancer, chemical terrorism countermeasures, and tuberculosis.

Gentlemen, please keep your remarks to seven minutes. Dr. Christensen, we'll start with you.

OPENING STATEMENT OF HENRIK I. CHRISTENSEN DIRECTOR, CONTEXTUAL ROBOTICS INSTITUTE AND PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA, SAN DIEGO

DR. CHRISTENSEN: Thank you. Thank you for this opportunity to address the Commission.

I'll start initially by talking about industrial robotics. It's an area that was invented in the U.S. We were in many respects the innovation leader. Today very little of industrial robotics is actually made in the U.S. Made elsewhere, we developed it and we send it elsewhere. It was invented primarily for the car industry, and that's still the primary market for industrial robotics. About 42 percent of all industrial robots are used in the automotive sector.

We were the main market for robotic sales until about 2013. So if you looked at where did you want to go and sell your robots, you would go to the U.S. first. 2013, we lost that leadership position to China. Today, the Chinese market is 240 percent larger than the U.S. market so in a very short time span, we've seen tremendous growth in China.

One of the reasons for that, of course, is that 30 percent of all cars manufactured today are manufactured in China, whereas in comparison, only six percent of all cars are made in the U.S. So for that reason we've seen this, if you want to become a member of the middle class in China, you have to own a car. So there's a tremendous need for this. They're mainly built manually today. So they need to be able to use robots to improve the quality. At the same time, we've seen that the salaries in China have gone up by about 350 percent over the last ten years. That's not been true in the U.S.

So in comparison we're seeing that they're not so competitive in terms of labor as they were ten years ago. To compensate for this, they're introducing more and more robots to make sure that they can remain competitive in this market.

We are seeing that the main suppliers have been from Japan. It's FANUC. It's been from Switzerland. It's ABB. And it's been from Germany. It's been KUKA. They are sort of the big three robotic providers.

More recently we've also seen some Chinese companies come up. Siasun in China is probably the fastest growing company. It came out of the Chinese Academy of Science. Initially it was a systems integrator, started building up all the expertise to understand how do we do this robotics thing. Once they knew where the opportunities were, they became a robotics provider. They are considered the fastest sort of growing today in China.

If we look at the commercial market, in the U.S., it grows about ten percent a year. And that's been true since 2009. In China, it grows 50 percent a year, and that's been true since 2009. So we're seeing tremendous amount of growth. That also implies that if you're an international company, and you're looking at where I should make my investments today, you're going to make them in China because that's where you'll see the big growth.

In China, it's all the companies have been operated by joint ventures. So it's been these--we're now starting and sort of been predicted for China to become competitive, they needed to figure out how do we become a member of the first division rather than being a fast follower. They've had problems with gears. They've had problems with software. They are now starting to catch up with us. To become part of the first division, the Chinese company Midea last year acquired KUKA in Germany for $4 billion, and basically that way became one of the big three.

That deal is getting closed right now. So we will see that it's Switzerland, Japan and China that are right now the big three in that area. And you should expect to see this continue. So China has this very ambitious plan in manufacturing, 2025, where they're looking at right now they are a big manufacturer. They want to become one of the world leaders, and by 2049, they want to become the world leader in manufacturing. So their idea is we should be coming to a place where they are the dominant player in the world for any kind of manufacturing, not only in terms of automotive.

If we look at other areas like, for instance, the UAV market of drones, there in terms of the commercial market, China is already the leader. The biggest supplier of some commercial small scale drones is DJI today. And on the military market, it's still the U.S. It's Northrup Grumman, it's General Dynamics, and it's General Atomics that are sort of the big players in this. Boeing, of course.

So we're still leading in terms of drones and the military, but in terms of the commercial utilization--and we are seeing the commercial robots being utilized, for instance, in Syria and in other places to deliver sort of improvised explosive devices. It's a very easy way to stuff a bomb onto a commercial grade robot, and you can fly it. So it poses a threat to us in terms of this type of technology.

If we look at U.S., we're still the innovation leader. It's still true that if you want to get the best education, if you want to do this, we are the innovation leaders today. Kids will want to go to Silicon Valley and similar ecosystems to do this.

That's also why we're seeing all of the big Chinese companies having innovation centers in the U.S.--Baidu, Huawei, DJI. All of them have their big R&D centers in the U.S. There are still cultural and language differences to go to China so instead of doing this, we're seeing these R&D centers being set up here. But the commercialization is not happening in the U.S. It's happening elsewhere. And that poses a threat to us.

And I would argue that the current export control regulations and the current ITAR regulations has not caught up with the latest technology developments so it's way too easy to export this technology without having to worry about current regulations. So I think that's important, something to consider. It's also important to consider that in the U.S. today, our estimate is that we are only investing about 20 percent of what China is doing in terms of robotics and artificial intelligence.

They're already investing five times more than we are, and that poses a big challenge to us. In the future, the innovation centers will move to Southeastern Asia unless we try to address this very specifically.

I would still say it's our opportunity to lose, but we need to react relatively quickly, both in terms of making sure that we control our innovation system, we maintain it here, we commercialize it here, and in terms of making sure that we have the right investments. And with that, I'll say thank you.

PREPARED STATEMENT OF HENRIK I. CHRISTENSEN
DIRECTOR, CONTEXTUAL ROBOTICS INSTITUTE AND PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA, SAN DIEGO

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

1. Introduction

Robots as a technology was invented in United States about 55 years ago. The initial application was in the automotive sector, which is still the dominant application of industrial robot technology today. Present applications are typically divided into industry, service and defense/security applications. For the service domain, we further subdivide into professional and domestic applications.

The use and sale of robotics is captured in the publication "World Robotics" which is published annually by the International Federation for Robotics (IFR)1. The statistics is gathered by the German VDMA through survey data obtained from robotics companies worldwide. The publication is considered a trusted source by the industry. The numbers used throughout this report are adopted from the 2015 edition of the report, unless otherwise noted.

The distribution across application domains of industrial robots is shown in Figure 1. The statistics represent use of robots by 2015.

[1] http://www.worldrobotics.org

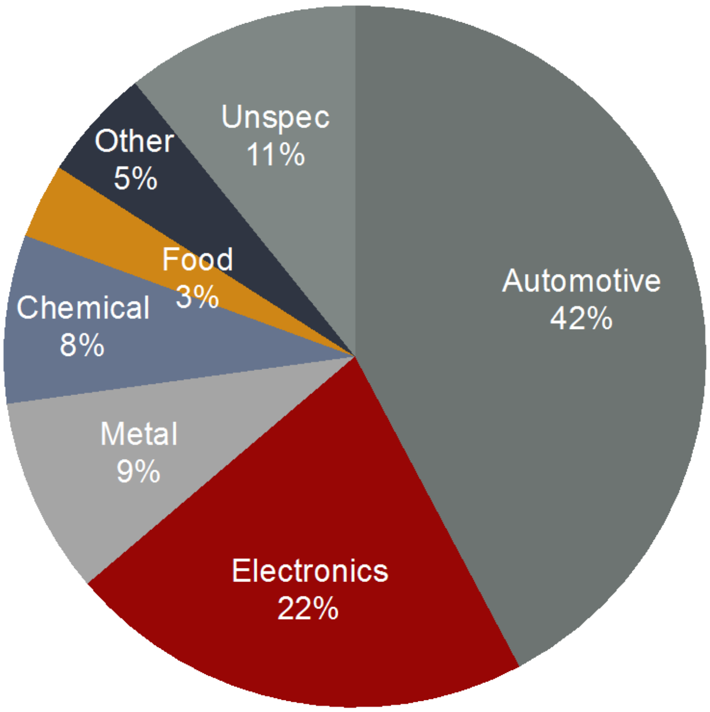


Figure 1: Application domains for industrial robots by 2015, according to World Robotics

China is seeing major growth in manufacturing of cars. During 2015 they saw a 6% growth. Close to 31% of all cars manufactured worldwide are made in China2. In comparison about 6% of cars are manufactured in USA.

The prototypical view of an auto-manufacturing facility is shown in Figure 2. It is important to note that even the most highly automated factories still have 8 workers for every robot. The factory will utilize a high degree of automation in the plate, the welding and the paint-shop, but the rest of the factory, which includes the main assembly line will have limited automation.

[2] www.oica.net - 2015 production statistics


Figure 2. The prototypical image of automotive manufacturing.

Recently there has also been a pickup of robot technology for aerospace manufacturing. The two main applications have been layup of composite material and drilling of holes and insertion of rivets. The motivation has been a need to increase manufacturing volume and reduce backlog.

The industrial robotics industry has an annual turnover of ~$30.5B of which $20B are in systems integration and approximate $10.8B are from direct sales of robot units.

The entire industry has a consolidated annual growth rate (CAGR) of 17% since 2009. The Asia region saw a 41% annual growth 2014-2015 and is by far the fastest growing region worldwide. A total of 254,000 industrial robots were sold during 2015. The predicted growth rate for 2017-2020 is expected to be at the same level.

In terms of defense / security applications the most obvious area of interest is Unmanned Aerial Vehicles (UAVs). The largest commercial provider of UAVs is DJI which is based in China. The biggest providers of UAV for military applications are General Atomics, General Dynamics and Northrup Grumman Corporation, all of whom are US based. UAV technology will soon find a much broader user-base for inspection, crop dusting, … but also for use in asymmetric warfare. In Syria, there were news reports during February 2017 that a majority of (improvised) aerial bombs were delivered using low-tech UAV systems.

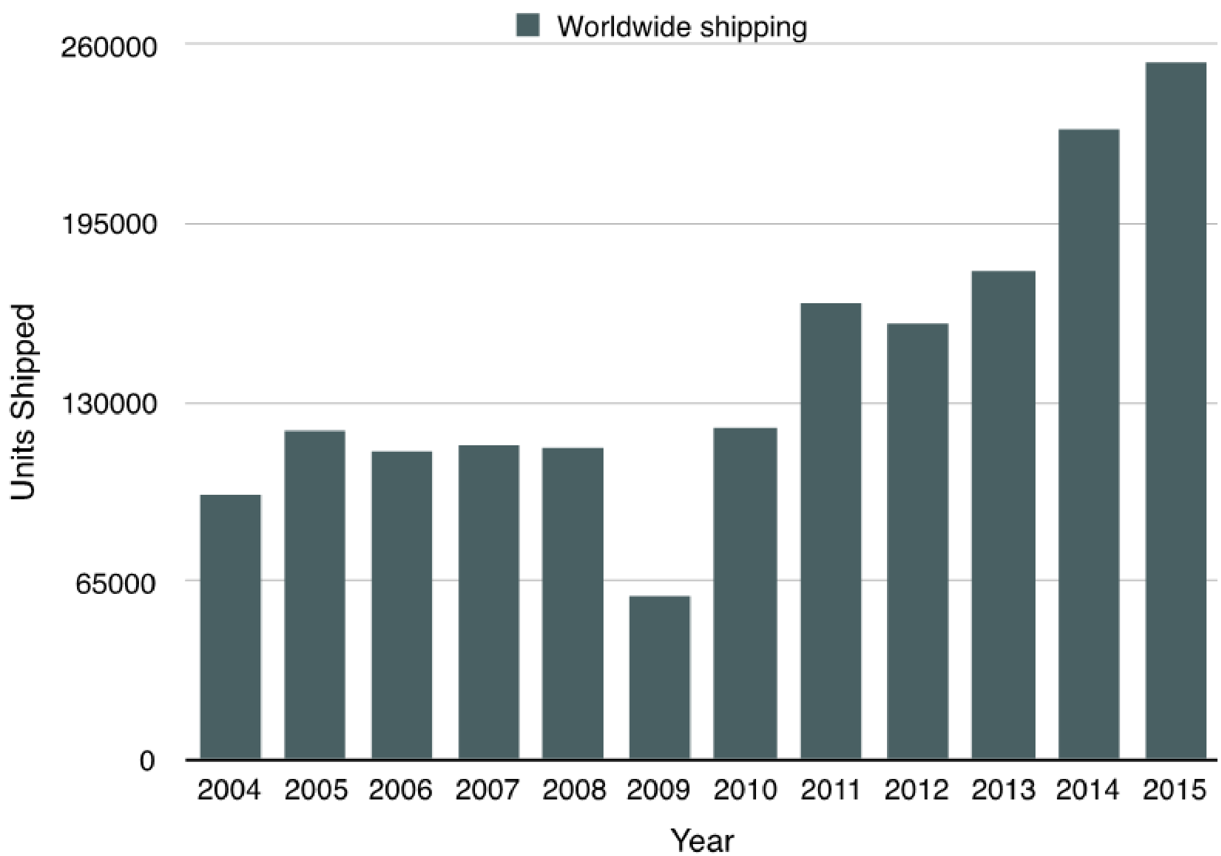


Figure 3: The number of robot units shipped worldwide [World Robotics 2015].

2. Robot use in US and China

Until recently the main market for industrial robots was USA across all segments. USA was the leader in utilization of industrial robotics technology until 2013, where China took over as the main market for robotics and automation. By now Japan and Germany have also overtaken USA in terms of number of robots sold per year. During 2015 China purchased 27% of all robots worldwide.

Typically, the market maturity is determined by the number of robots deployed per 10,000 workers. The highest use of robots is in Republic of Korea where more than 500 robots are used per 10,000 workers or about 1 robot for every 20 workers. Singapore is second and Japan third with 395 and 305 robots / 10,000 workers, respectively. USA has 176 robots / 10,000 workers. The world average is 64 robots / 10,000 workers. China is utilizing 49 robots / 10,000 workers and is significantly below average in adoption of robots for manufacturing.

If the comparison only considers the automotive market, Japan has the highest with 1,400 robots / 10,000 workers. Germany, USA and S. Korea have equal penetration ~1,150 robots / 10,000 workers.

China is at 392 robots / 10,000 workers. To match the others for the automotive market China would have to triple its acquisition of robots.

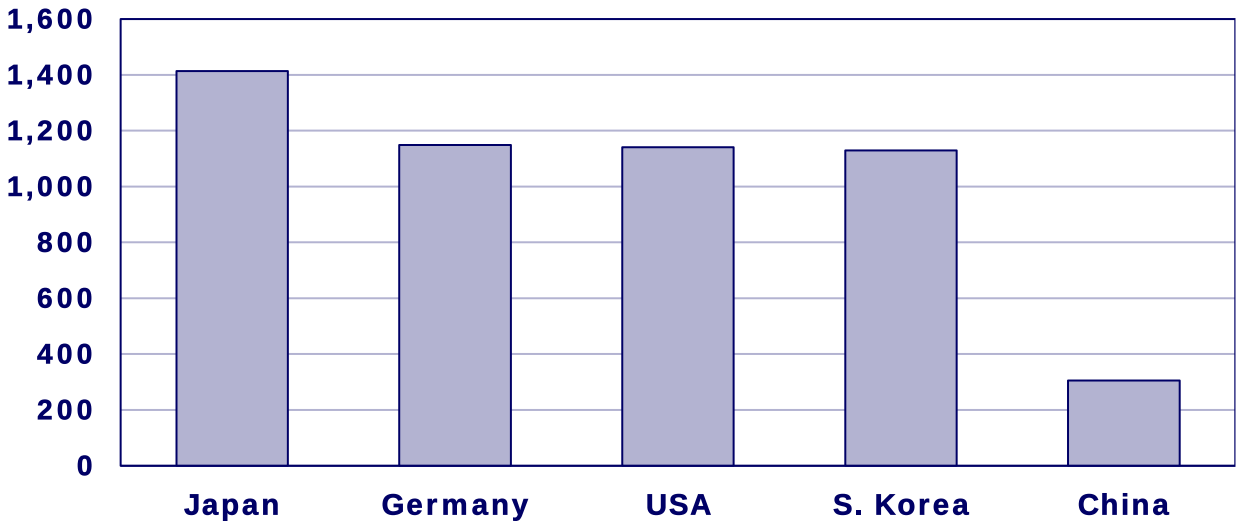


Figure 4: Number of robots in use per `10,000 workers in the automotive sector [WR 2015]

The adoption of robots in the automotive sector has primarily been to ensure consistent quality.

Foreign manufactured cars are typically twice as expensive as domestically manufactured cars in China. Today none of the cars manufactured in China are exported. In comparison BMW is the largest exporter of cars in USA.

A big driver in China has been increasing salaries that have required innovation to bring down / maintain production costs.

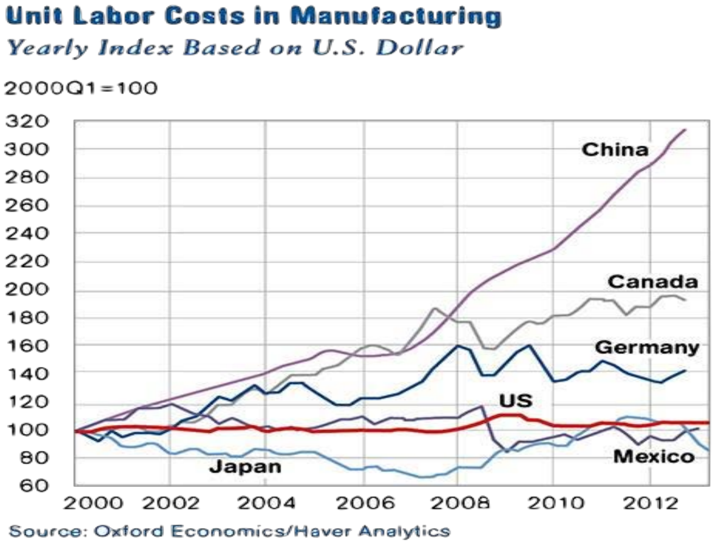


Figure 5 Changes in labor cost over time across several key nations.

3. The growth of a Chinese robot supply base

Today, the main robotics providers in China are FANUC, ABB, KUKA, and Yaskawa. These companies operate in China as joint venture subsidiaries. Already 2001 ABB chose to move their robotics R&D headquarter from Västerås, Sweden to Shanghai.

About 80% of all robots in China are provided by joint venture companies. In parallel several Chinese owned companies have emerged.

The biggest Chinese company is Siasun. The company is a spin-off from the Chinese Academy of Science. They were initially a systems integrator that purchased foreign manufacturing components and integrated them into complete systems. As they got more experience they have launched their own series of robots. Today about 20% of the robots sold in China are manufacturing by Chinese companies. The overall partition of the market is shown in Figure 6.

A challenge for Chinese companies have been access to high quality reduction / precision gears. These gears have almost exclusively been manufactured by the companies Nabtesco and Harmonic Drives in Japan. More recently, a Chinese company has emerged named Harmonious Drives and they produce gears that have a close resemblance to those made by Harmonic Drives.

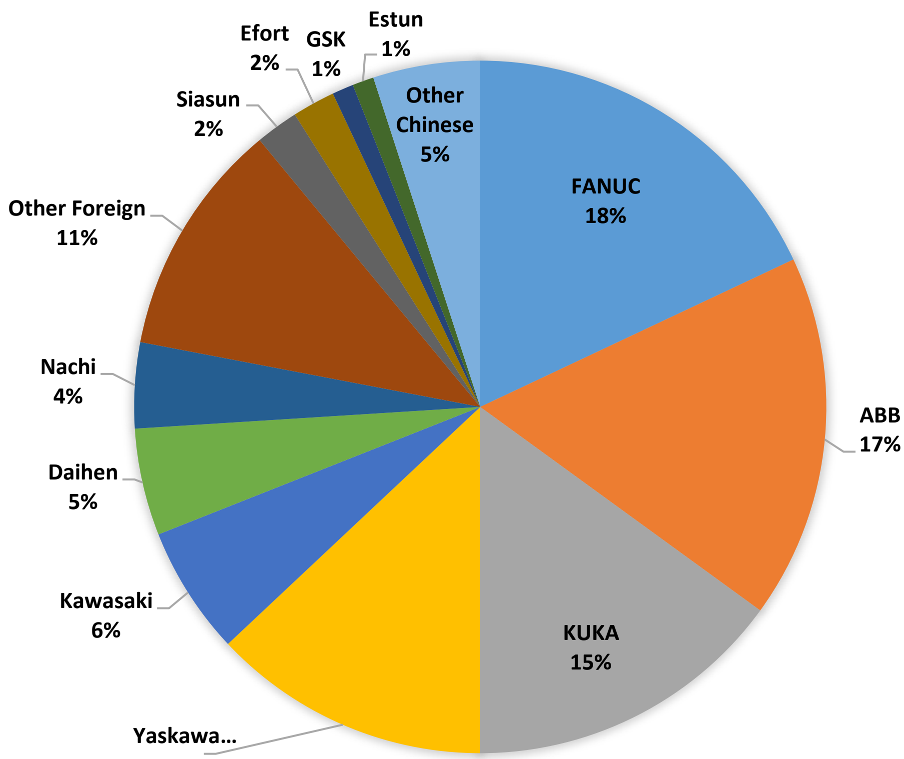


Figure 6: Division of sales across foreign and domestic companies in China for industrial robotics

The Chinese companies have had a reduced accuracy and repeatability compared to foreign manufactured products. A modern US / EU manufactured robot has a repeatability of 0.1 mm (~1/250") and an overall accuracy of about 0.3-0.8 mm. The average lifetime for an industrial robot is 10 years of operation. In comparison, a typical Chinese robot has a repeatability of 0.35mm and an accuracy of 1 mm (1/25") and the lifetime is 3 years.

An obvious question has been – how can China catch up? There are two obvious opportunities: i) accelerate R&D in China and/or international partnering or ii) acquire foreign owned IP and expertise. One such examples that took place during 2016 was the Chinese company Midea acquiring the 2nd largest robotics company KUKA AG (German) at a cost of $4.5B. The acquisition will be finalized during March 2017. No doubt more acquisitions will happen over the next few years.

4. A Chinese ambition for industrial robotics

China has a 3-stage strategy for robotics and manufacturing according to Mr. Wang Weiming, Vice Department Head of Industry Equipment Department of the Ministry of Industry and Information

Technology (MIIT): i) a short-term strategy, ii) a 2025 strategy and iii) a long-term 2049 strategy. The first decade 2006-2016 has been devoted to establishing China as a modern manufacturing nation. By 2025 the country wants to be a manufacturing world-power. By 2049 China wants to be the world leader in manufacturing. The overall ambition is outlined in the strategy document “Made in China 2025”. By 2025 China would like to have a penetration of robots corresponding to 150 robots / 10,000 workers. It is anticipated that by 2019 40% of the worldwide supply will be installed in China [World Robotics 2016]. To reach the target of 150 robots / 10,000 workers more than 600,000 new robots must be installed within the next 8 years. The worldwide supply during 2016 was 258,000 so it would require a major growth in manufacturing and installation of robots. Consequently, it is obvious why the big market for industrial robots today is China. The US market in comparison is only about 10% of the world supply and the growth rate is predicted to be around 15% per year.

5. The Chinese UAV industry

While most industrial robot manufacturing today is taking place outside of USA the same is not true for the Aerospace Sector where companies such as The Boeing Company, Northrup Grumman Corporation, General Dynamics, Lockheed Martin and General Atomics are significant providers of airplanes and unmanned aerial vehicles (UAVs). Traditionally Boeing and Airbus have been the big providers of commercial airplanes and only now is the Commercial Aircraft Corporation of China, Ltd. (Comac) introducing airplanes that are expected to compete with single aisle airplanes such as the Boeing 737.

In the area of unmanned aerial vehicles the military space has been dominated by companies such as General Atomics, Northrup Grumman and General Dynamics. For non-military applications companies such as DJI and 3D robotics have been market leaders. Today the biggest provider of drones for the commercial space is DJI. In the US 48% of the FAA registered UAVs are from DJI.

DJI has had a hard time convincing people to move to China to participate in their R&D and they have consequently setup research centers in USA and in Europe. This has been an effective strategy to have basic research carried out in USA and Europe while commercialization and manufacturing is taking place in China. The US company 3D robotics is moving away from the low-end commercial space and Chinese companies such as Ehang and Yuneec are quickly joining DJI to be the leaders in this space. The applications are abundant from infrastructure inspection over environmental monitoring to package delivery. Companies such as UPS and Amazon have announced that they are ready for short-range package delivery and both companies have reported early testing.

The UAV market is about to take off big time for assistance in the logistics space. The platforms will have numerous dual-use opportunities. Is this a space USA can afford to give away?

6. The long-term Chinese strategy

As mentioned earlier the “Made in China 2025” document outlines a clear ambition for robotics in China. The current investments are close to $10B / year. The portfolio of funding is across setup of strong research groups in China, transition of technology for production in China and acquisition of core IP from international companies.

China needs access to core technology to allow them to be the manufacturing leader not only in terms of mass manufacturing products such as cell phones, textile, but also for mass customized products such as cars and airplanes. To this end there is a need to build a strong industrial robotics industry anchored in China, but ideally connection to innovation centers worldwide.

For the defense industry and for unmanned aerial vehicles there is an opportunity for China to be the world-leader not only for low-cost commercial systems, but also for defense applications. Right now the backlog for delivery of commercial airplanes is 5-8 years. COMAC is testing an airplane that may be delivered significantly faster. The fastest growing market for air-traffic is in Asia. Boeing is now delivering 31% of their production to Asia and expect the numbers to grow to 29% by 2035. COMACs creation of a competitive single aisle airplane could challenge this economic growth. The same technologies are not only used for commercial airplanes but also for larger UAV systems as manufactured in the US by General Atomics, Northrup Grumman and General Dynamics. Clearly the commercial UAV industry will also provide core technologies for defense application. No doubt USA is the leader on large scale UAV technology today, but given that more than 50% of the commercial UAV industry is in China today this balance could change quickly.

7. Policy implications?

By far the biggest industrial robotics market today is China. Today market is already 240% larger than the US market and that number is expected to grow over the next decade. The investment in China is at least $10B / year. The corresponding number in the USA is likely around $2B. It is hard to accurately estimate these numbers as big commercial players such as Amazon, UPS, United Technologies, Google, Qualcomm are making major investments and the numbers are in most cases not public. For industrial robots non-US companies are today more likely to invest in China than in USA as the big growth opportunity is in South Eastern Asia. The US market is already relatively mature whereas the Chinese market is still emerging.

For industrial robotics the big companies FANUC, KUKA, ABB, and Yaskawa are already foreign. An emerging market for industrial robotics is collaborative systems, where the two market leaders ReThink Robotics and Universal Robots are controlled by USA investors, but their biggest markets are in Asia.

From a policy point of view there are some obvious opportunities

Investment into manufacturing robotics to make USA a competitive market for the future of manufacturing. Next generation manufacturing is in many cases focused on mass customized products rather than mass manufactured products. The single biggest market today is still in the United States. Ensuring that the US market is attractive for manufacturing opens new opportunities to also do the R&D and commercialization domestically.

Chinese companies are setting up R&D laboratories in USA as the movement of the best people to China still poses a challenge due to language and cultural barriers. There are regulations in place for Export Control and ITAR, but in many cases these regulations are too slowly adapting to limit broader dissemination of new technology. In addition, it is not clear that these mechanisms are particularly effective. Ensuring that technology is adopted and utilized in USA appears to be a more effective strategy

Today adoption of new legal frameworks for UAVs, driverless cars etc appears to be slower in USA than other nations. In addition, in some cases testing of new technology is faster / less restricted in other areas which encourages new research to be performed outside of USA.

Traditionally USA has been an innovation leader and attracted the smartest people to do R&D across academia, research laboratories and industry. To compete it will be essential to continue to promote USA as an innovation economy and the best place to innovate.

OPENING STATEMENT OF JONATHAN RAY
ASSOCIATE DEPUTY DIRECTOR, DEFENSE GROUP, INC.

MR. RAY: Thank you very much.

It's an honor to be here and discuss China's industrial and military robotics development. For today, I was asked, first, China's industrial and service robotics industries; second, China's military robotics and unmanned systems; third, the role of technology transfers for China's robotics development; and finally, how the United States can protect its economic and military advantages.

First, on industrial robotics, China is the world's largest market, as the previous speaker just stated. In 2015, China commanded 27 percent of the global market, and by 2019, that number could increase to 40 percent.

But while China's industrial robotics market is growing rapidly, it is still underdeveloped and faces numerous challenges. Consider that China's average robot density is less than half of that of the United States. The global leader, South Korea's robot density is over seven times as high. So there's room for growth especially as Chinese policies and rising labor costs drive greater automation across more industries.

But China is also continuing to face chronic challenges in its industrial robotics industry. A senior Chinese official stated that the industry is, quote, "plagued by low quality, overinvestment, and too much duplication."

Also China has been long dependent on imports for advanced components such as parts requiring high-precision engineering, data fusion, and integration and controller technologies.

To guide the industry and to address these challenges, the Chinese government has included industrial robotics in at least six state plans since 2006. The most ambitious of these is Made in China 2025. Instead of targeting one industry, it seeks to upgrade China's entire manufacturing sector, and industrial robots will play a key part in this.

The European Union, which is home to many of the world's leading companies for industrial robots, is concerned about this plan. The EU Chamber of Commerce in China recently described the policy tools for this plan's implementation as, quote, "highly problematic" and states that the support from central and local governments in the form of subsidies, funds, and other channels of support total hundreds of billions of euros in funding.

Now the Chamber is concerned that this policy will eventually lead to overcapacity in the market, greater pressure on international firms to hand over advanced technology in exchange for market access, and, in the long run, box out international competitors.

Changing gears to service robots, which assist people with tasks other than production and manufacturing, China's economy and demographics will likely drive more sustainable growth for the foreseeable future.

China's economy and investments in science and technology will sustain demand for professional service robots such as those that assist with infrastructure inspection, agriculture, and deep sea exploration.

China's aging population will drive demand for domestic service robots such as those supporting elderly care and medical rehabilitation.

And, finally, higher wages and more leisure time in the middle class will drive interests in other domestic service robotics, such as robotic vacuums, intelligent laundry machines, and smart toys that come out every year and sound really cool.

Changing gears again and looking to the military side, China's growing numbers of unmanned systems and the countermeasures enhance its anti-access/area denial capabilities and threaten the U.S. forces' freedom of operation in the Asia- Pacific region.

China's leaders and military strategists have written that they believe that the nature of warfare is fundamentally changing, and that future wars will have, quote, "unmanned, intangible and silent" characteristics.

Consequently, China is investing heavily in unmanned systems that improve key capabilities and can carry out an increasing variety of missions at air, land, and sea.

Among these domains, China's unmanned aerial vehicles, or UAVs, are certainly its more mature capability.

Now a direct comparison between Chinese and U.S. UAVs is difficult, but there are two trends that I would emphasize for today. First is that Chinese UAV manufacturers and their customers, both Chinese and abroad, appear to emphasize lower price points and quantity over increased capabilities. In other words, they'll go for "good enough" instead of the gold standard.

Second, the evidence strongly suggests that China lags behind the United States on technologies for propulsion, autonomous operation, advanced sensors and data links. This leaves systems like the Global Hawk as the global leader for these types of systems.

Now in a broader sense I would like to highlight three trends that I believe enhance China's A2 capabilities and can pose severe long-term threats to U.S. forces in the region.

First, the PLA's growing number of UAVs enhances its ISR and long-range precision strike capabilities. That can hold more U.S. assets at risk at greater distances. That's cause for concern.

Second, for unmanned underwater vehicles, there's a great deal of research into systems that could improve China's anti-submarine warfare capabilities and erode long-held U.S. advantages in undersea warfare.

Finally, the PLA considers the U.S. military to be increasingly dependent on unmanned systems and hence is developing countermeasures. China is actively researching hard and soft kill countermeasures to destroy or degrade U.S. systems. Even in peacetime, we have already seen these soft kill countermeasures in action. In 2015, a U.S. press report claimed that the PLA attempted to jam a Global Hawk UAV operating over the South China Sea.

I think we can expect to see these activities continue and escalate in the event of a crisis.

Next, on the role of technology transfers. China is actively acquiring components, technologies, and materials from abroad for its robotics industry and military unmanned systems. The three categories that I would use to describe these efforts are, first, illicit technology acquisitions. These include cyber intrusions that target defense contractors and intentional violations of U.S. export controls for sensitive components.

The second category is informal knowledge and technology transfers, such as China's massive open source collection efforts against U.S. military programs, the recruitment of foreign talent and Chinese experts living abroad, and international academic exchanges.

The third category is formal technology acquisitions and investments in which Chinese companies acquire or invest in foreign companies involved in robotics or enabling technologies like artificial intelligence.

Finally, for recommendations, there's a longer list in my written statement and the report that we prepared last year for the Commission, but my bottom line is that the United States has to keep ahead in advantages of innovation and quality and take steps to protect those advantages.

For the industrial and service robotics industries, U.S. initiatives such as Manufacturing USA and the National Robotics Initiative help the United States stay ahead by innovating new applications for robotics, innovating new components and enabling technologies, and by helping U.S. companies adopt robots into different operations.

The Congress can continue to support these initiatives and ensure that the U.S. maintains those leads in innovation.

On the military side, defense planners should expect to see growing numbers of Chinese unmanned systems as well as more countermeasures against our own assets.

And finally, to preserve commercial and military advantage, I would urge greater vigilance against each of the technology acquisition strategies I've discussed, including cyber threats, informal transfers, and international investment and acquisition activities.

Thank you again for having me and I look forward to your questions.

PREPARED STATEMENT OF JONATHAN RAY
ASSOCIATE DEPUTY DIRECTOR, DEFENSE GROUP, INC.

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

Introduction

China's commercial and military robotics industries are growing rapidly as the country upgrades its manufacturing sector and military capabilities. In a 2014 speech on the importance of science and innovation to the "great rejuvenation of the Chinese nation," Chinese President Xi Jinping stated that around the world industrial robots are considered the "jewel in the crown of manufacturing."[1] China's military planners believe unmanned systems and other technologies are transforming warfare and giving it "unmanned, intangible, and silent" characteristics."[2] Consequently the People's Liberation Army (PLA) is developing and deploying increasingly capable unmanned systems as well as countermeasures to the U.S. military's unmanned systems.

These developments pose serious challenges for U.S economic and strategic interests. China's policies and investments in industrial robotics could erode U.S. advantages in robotics and manufacturing. Unmanned systems will increase the PLA's intelligence, surveillance, and reconnaissance (ISR), long-range strike, and anti-submarine warfare (ASW) capabilities, challenging U.S. power projection in the Asia-Pacific region. To address these issues more fully, this testimony is organized as follows:

I. China's industrial and service robotics industries
II. The PLA's military robotics and unmanned systems
III. China's acquisition of foreign robotics technology
IV. Recommendations to maintain U.S. economic and strategic advantages.

[1] "习近平：把关键技术掌握在自己手里" [Xi Jinping: Grasp Key Technologies in Our Own Hands], 新华网 Xinhua Net, June 9, 2014, accessed March 1, 2017, http://news.xinhuanet.com/politics/2014-06/09/c_126597413.htm.
[2] Shou Xiaosong 寿晓松, *战略学 (The Science of Military Strategy)* (Beijing: Academy of Military Science Press, 2013), 97-98.

I. China’s Industrial and Service Robotics Industries

China boasts the world’s largest market for industrial robots and has ambitious plans to become the leading supplier of them. While China’s industrial robotics market is growing rapidly, it is still underdeveloped as China’s automation rates remain well below the averages of other leading manufacturing countries. The industry has also faced chronic challenges with components requiring precision engineering that are essential to industrial robots. China’s policies for its industrial robotics industry threaten to skew the market and block international competitors. State plans, most notably Made in China 2025, provide generous subsidies to Chinese industrial robotics firms that are beginning to oversaturate the market. The same plans strongly encourage Chinese companies to choose domestic brands of industrial robots, boxing out international competitors.

China’s service robotics industry has also quickly matured as robots for professional service and domestic use have proliferated. Chinese startups such as DJI have successfully expanded and marketed their products abroad to capture international market share. Factors such as China’s growing middle class and aging demographics will likely continue to drive this market.

As China focuses more on quantity of robots and catching up in component technologies, the United States should focus on its advantages in quality and innovation. U.S. universities, start-ups, branches of multinational corporations, and domestic companies have innovated in the past and are doing so today. Support mechanisms such as the National Robotics Initiative will be instrumental for future breakthroughs in areas such as human-machine collaboration.

The Rapid Growth of China’s Industrial Robotics Market

In 2015, China commanded 27% of the world’s industrial robotics market, and the International Federation of Robotics (IFR) predicts that number will increase to 40% by 2019. For perspective, consider that in 2015, sales of industrial robots in China surpassed the total sales volume of industrial robots for all of Europe. Sales in China increased 20% from 2014 to reach 68,600, surpassing Europe’s total sales volume of 50,100 units. Chinese suppliers saw increases of 29% in sales to their domestic market, while foreign suppliers enjoyed 17% increases.[3]

Despite its rapid growth and high volume, China’s industrial robotics market is still underdeveloped compared to other countries. One useful measurement from the IFR is China’s average robot density, measured as the number of industrial robots in operation per 10,000 employees. At 69 units, China is well behind the United States (fifth highest density with 176 units) and the global leader Republic of Korea (531 units). This data strongly suggests ample room for growth in this market as more Chinese industries automate.[4]

---

[3] “World Robotics 2016,” International Federation of Robotics, http://www.ifr.org/index.php?id=59&df=Executive_Summary_WR_Industrial_Robots_2016.pdf, pp. 11-12.
[4] Ibid, pp. 15-16.

Table 1: Number of industrial robots installed per 10,000 employees in the manufacturing industry as of 2015. Source: International Federation of Robotics.[5]

Country	Robot Density
Republic of Korea	531
Singapore	398
Japan	305
Germany	301
United States	176
China	49
Global average	69

Trends in China's Adoption of Industrial Robots

Chinese and international experts highlight the following trends for China's industrial robotics industry:

1. The automobile industry has driven much of the market to date. – Since 2000, China's automobile industry has been a primary driver for the country's industrial robotics market, which is common for other countries.[6] It is telling that Miao Wei (苗圩), a leading voice for the Made in China 2025 initiative (discussed below), was an automobile executive before becoming the Minister of Industry and Information Technology.[7] The IFR assesses that ongoing modernization for China's automobile industry will continue to boost robot installations.[8]
2. Other industries are increasingly adopting industrial robots. – In line with international trends, other industries such as the "3c" industries (computers, communications, and consumer electronics) machinery, electrical and electronics industries, rubbers and plastics, food industries, logistics, and manufacturing are demanding more automation.[9][10]
3. Traditionally, wholly owned foreign-owned enterprises and foreign joint venture enterprises have been the primary customers for industrial robots. Foreign enterprises and joint ventures in China have traditionally been more adept at adopting robots compared to their domestic competitors, who have

[5] Ibid.
[6] Rui Gongye 睿工业 and Liu Peng 柳鹏, "我国工业机器人发展及趋势" [Development and Trends of China's Industrial Robotics], *Robot Technique and Application* 机器人技术与应用, no. 5 (2012): 20; Shen Xuming 沈绪明 and Dong Peng 董鹏, "我国机器人发展现状、需求及产业化探讨" [An Investigation of China's Robotics Development Situation, Requirements, and Industrialization], *Logistics Technology (Equipment)* 物流技术 (装备版), no. 22 (2012): 69-70.
[7] "工业和信息化部部长、党组书记 苗圩" [MIIT Minister and Party Secretary Miao Wei], Ministry of Industry and Information Technology 工业和信息化部, accessed March 7, 2017, http://www.miit.gov.cn/n1146285/n1146347/n1147601/index.html.
[8] World Robotics 2016, p. 15.
[9] Zhao Jie 赵杰, "我国工业机器人发展现状与面临的挑战" (Development and Challenge of Chinese Industrial Robot), *Aeronautical Manufacturing Technology* 航空制造技术, no. 12 (2012): 26.
[10] "Industrial Robot Statistics," International Federation of Robotics.

had inflexible production models.[11] This trend may be changing as labor costs and state plans push greater automation across more industries.

4. Rising labor costs are a major reason for China's adoption of industrial robots in various industries. As in other countries (including the United States), China's labor costs are rising and encouraging industries, especially labor-intensive ones, to adopt industrial robots.[12]
5. The world's leading robot manufacturers are very active in China through sales and production in country, including Germany's KUKA, Japan's Yaskawa, and Swedish-Swiss multinational corporation ABB.

National Plans and Support Mechanisms for China's Industrial Robotics Industry

The Chinese government's support for its robotics industry is massive, and risks both overcapacity in China's domestic industry and boxing out international competition. From 2006 to 2012, China included robotics as part of broader science and technology, manufacturing, and state level Five-Year Plans (FYPs) and guidelines.[13] By 2013, as China became the world's largest market for industrial robots, the state plans became more specific in their goals.

- In 2013, MIIT announced its "Guideline on Promoting the Development of the Industrial Robot Industry" (关于推进工业机器人产业发展的指导意见) to address weaknesses in China's industrial robotics industry (including its dependence on foreign suppliers for high-precision components), to promote the adoption of industrial robots, and to develop national champions to manufacture these systems.[14]
- The Thirteenth Five Year National Economic and Social Development Plan (2016–2020) (国民经济和社会发展第十三个五年规划纲要) calls for numerous developments related to robotics, and includes "robotics equipment" (机器人装备). It was the first FYP to include the term artificial intelligence (AI).[15][16]
- In April 2016, China's MIIT, Ministry of Finance, and the National Development and Reform Commission jointly released the Robotics Industry Development Plan (2016-2020) (机器人产业发展规划（2016-2020年）), calling for advances in China's industrial and service robotics

[11] Shen and Dong, "An Investigation of China's Robotics Development Situation, Requirements, and Industrialization," 69-70.
[12] Ibid.
[13] National plans that included robotics from 2006 to 2012 include the National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020) (国家中长期科学和技术发展规划纲要 (2006—2020 年)) and the Twelfth Five Year Plan for Intelligent Manufacturing (智能制造科技发展"十二五"专项规划).
[14] "工业和信息化部关于推进工业机器人产业发展的指导意见" [Guiding Suggestions from MIIT on Promoting the Development of the Industrial Robotics Industry], Ministry of Industry and Information Technology 工业和信息, as posted at Sina 新浪, December 30, 2013, accessed March 7, 2017, http://finance.sina.com.cn/stock/y/20131230/170417797233.shtml.
[15] "中华人民共和国国民经济和社会发展第十三个五年规划纲要" (The Thirteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China), Xinhua Net 新华网, March 17, 2016, accessed March 7, 2016, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm.
[16] Qu Ting 屈婷, Liu Wei 刘伟, and Yang Dingmiao 杨丁淼, "'十三五'：中国开启人工智能商用新纪元" [The Thirteenth FYP: China Starts a New Era of Commercial Use for Artificial Intelligence], Xinhua Net新华网, March 8, 2016, accessed March 7, 2017, http://news.xinhuanet.com/fortune/2016-03/08/c_1118271033.htm.

> industries. The plan reiterates the same goals of breaking China's dependence on foreign suppliers for advanced components, increasing the adoption of industrial robots across industries, and increasing the production and sales of China's domestic models.[17]

Made in China 2025 (中国制造2025) is one of China's most ambitious programs to date. Instead of targeting a specific industry, this program aims to improve the entire Chinese manufacturing sector's competitiveness, innovation, technology, quality, reliability, and "green-ness."[18] While these goals have merit, the European Union Chamber of Commerce in China describes the policy tools for its implementation as "highly problematic." According to the Chamber, this support from central and local governments constitutes "hundreds of billions of euros of funding in the form of subsidies, funds, and other channels of support." This support is "contributing to overcapacity in the low- and mid-tiers of China's market." Furthermore, international firms are facing pressure to hand over advanced technologies for market access. In the long term, the program "amounts, in large part, to an import substitution plan."[19] In addition to skewing the playing field against international competition, this program is arguably a "shopping list" for China's foreign investment targets to acquire key technologies and licenses, as discussed in the technology transfer section below.[20]

Challenges to China's Industrial Robotics Industry and Reliance on Imports

While China's industrial robotics industry is growing rapidly, problems persist that hamper the development of Chinese manufacturers and leave them dependent upon foreign suppliers for key technologies. At a broader level, some analysts worry that Chinese companies are struggling to find niches, and that overinvestment is leading to blind competition. At a more technical level, while China is proficient in the general construction and design of robotics systems, it lags behind on complicated components and controls, as well as parts requiring precision engineering.

Xin Guobin, Vice Minister of the MIIT, commented in June 2016 that despite the growth of China's demand for industrial robots, the industry is "plagued by low quality, overinvestment and too much duplication."[21] Chinese industry analysts agree, stating that Chinese manufacturers tend to imitate leading brands rather than innovate, have trouble converting prototypes into marketplace products, and lack qualified personnel.[22] Additionally some commentators consider China to be overinvesting in its robotics

---

[17] He Huifeng, "China's Five-Year Plan to Transform Its Robotics Industry," *South China Morning Post,* April 6, 2016, accessed March 7, 2017, http://www.scmp.com/news/china/policies-politics/article/1934071/chinas-five-year-plan-transform-its-robotics-industry.

[18] "国务院关于印发《中国制造2025》的通知" [State Council Releases "Made in China 2025" Announcement], May 8, 2015, accessed March 7, 2017, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

[19] "China Manufacturing 2025: Putting Industrial Policy Ahead of Market Forces," European Union Chamber of Commerce in China, 2017, www.europeanchamber.com.cn.

[20] Sebastian Heilmann, "Europe Needs Tougher Response to China's State Led Investments," post at *Financial Times,* June 9, 2016, accessed March 7, 2017, http://blogs.ft.com/beyond-brics/2016/06/09/europe-needs-tougher-response-to-chinas-state-led-investments/.

[21] Mandy Zuo, "China's Robot Industry 'Plagued by Low Quality, Overinvestment and Too Much Duplication'," *South China Morning Post*, March 7, 2017, accessed August 29, 2016, http://www.scmp.com/news/china/economy/article/1976825/chinas-robot-industry-plagued-low-quality-overinvestment-and-too; "工信部副部长辛国斌：机器人已有投资过剩隐忧" [MIIT Vice Minister Xin Guobin: Worries that Robotics Already Has Surplus Investment], Sina 新浪 , June 16, 2016, accessed March 7, 2017, http://finance.sina.com.cn/china/gncj/2016-06-16/doc-ifxtfrrc3709815.shtml.

[22] Cai Zixing 蔡自兴, "中国机器人学40年" (Robotics in China Daring [sic] the Past 40 Years), *Science & Technology Review* 科技导报 , no. 21 (2015):

companies. According to the CRIA, China has built or started construction on 40 new robot industrial parks since 2014.[23] For some Chinese observers, the problem with too much competition too quickly is that companies do not define a niche in the market and blindly compete.[24] The EU Chamber of Commerce in Beijing, as noted above, considers this overinvestment to be oversaturating the market.

At a more granular level, China is proficient at general robotics, but continues to struggle with advanced components, complicated controls, and integration of data and sensors. It continues to struggle with high-precision reduction drives, servo (small electric motor) electrical machinery, controllers, and other components that require precision engineering. Additionally, China remains behind international standards in programmable logic controller (PLC) and changing frequency controls products, multiple sensor information fusion control technology, remote control plus local autonomous system remote control robots, and intelligent assembly robots. [25]

As China grapples with problems of quality and defining competition, international brands have reputations for quality, defined market niches, and declining prices (at least over the past decade). As of 2012, Chinese analysts wrote that automobile industry executives preferred foreign brands for these very reasons.[26] As Made in China 2025 progresses, a key indicator of progress will whether these attitudes change and Chinese robotics manufacturers come mature and offer better quality products, defined niches, and competitive prices.

Opportunities and Implications for the U.S. Industrial Robotics Industry

The U.S. industrial and service robotics industries have tremendous potential to compete and innovate. The key for stakeholders is to recognize the structure of the U.S. industry and define realistic goals for success. The majority of leading industrial robotics firms are based in Japan and Europe and have operations here in the United States. Major foreign suppliers with U.S. plants and subsidiaries include Japanese firms Fanuc, Kawasaki, and Yaskawa-Motoman; the German company Kuka; and Switzerland's ABB and Stäubli. Instead of completed robots, half of the value of U.S. industrial robotics exports and a quarter of U.S. imports of industrial robots are parts.[27] In short, the U.S. and Chinese industrial robotics industries are very different.

While China rapidly expands production numbers and catches up on component technologies, the guiding principles for the U.S. robotics industry should be quality and innovation. The United States have

26.

[23] Mandy Zuo, "China's Robot Industry 'Plagued by Low Quality, Overinvestment and Too Much Duplication'," *South China Morning Post*, June 17, 2016, accessed March 7, 2017, http://www.scmp.com/news/china/economy/article/1976825/chinas-robot-industry-plagued-low-quality-overinvestment-and-too.

[24] Ibid.,"工信部副部长辛国斌：机器人已有投资过剩隐忧" [MIIT Vice Minister Xin Guobin: Worries that Robotics Already Has Surplus Investment], *Sina* 新浪, June 16, 2016, accessed March 7, 2017, http://finance.sina.com.cn/china/gncj/2016-06-16/doc-ifxtfrrc3709815.shtml.

[25] Rui and Liu, "Development and Trends of China's Industrial Robotics," 21; Cai Zixing 蔡自兴and Guo Fan 郭璠, "中国工业机器人发展的若干问题" [Development and Basic Problems of China's Industrial Robotics Development], *Robot Technique and Application* 机器人技术与应用, no. 3 (2013): 10-11.

[26] Cai, "Robotics in China Daring [sic] the Past 40 Years," 26; Zhao, "Development and Challenge of Chinese Industrial Robot," 28; and Sun, Wang, and Zhang, "On the Development Status and Tendency of Industrial Robots," 62.

[27] Michael Stanton-Geddes and Dennis Fravel, "U.S. Manufacturing Companies Are Global Leaders in Industrial Robot Consumption," USITC Executive Briefing on Trade, May 2014.

advantages to leverage in the robotics industry, including highly trained personnel, leading R&D institutions, and dynamic companies that innovate robotics technologies. For personnel, Chinese experts are openly envious of U.S. universities and the quality of their programs. Continuing to support university research and attracting leading students from around the world ensures this advantage. For R&D, the United States should continue to support universities and companies with grants and R&D tax incentives that help fund research into new applications and enabling technologies. The National Robotics Initiative (NRI, now NRI 2.0) is an excellent model of making funding available to research that fundamentally changes robotics, in this case by focusing on human-machine collaboration.

U.S. companies are already leaders in innovation for industrial and service robots. For example, SoftWear Automation Inc., an Atlanta-based robotics startup, has developed robots that can sew garments, the first of their kind.[28] Rethink Robotics, whose founder helped produce the iconic Roomba at iRobot, introduced Baxter in 2012 to create a new category of automation called collaborative robotics.[29] While European and Asian manufacturers are established leaders and were the first to commercialize traditional industrial robots, U.S. innovations may be the first of their kind and generate interest in international markets, including China.

In addition to supporting U.S. robotics R&D and manufacturing, the U.S. Government should voice the same concerns over Made in China 2025 raised by the European Union Chamber of Commerce in China. Barriers to market access, pressure on companies for intellectual property in exchange for market access, generous subsidies to Chinese companies, and import substitution policies skew the playing field against U.S. companies.

Service Robotics Industry

China's service robotics industry has grown rapidly over the past decade, and Chinese official expect the industry to become more prominent within the overall robotics industry in the future. Service robots are partially- or wholly-autonomous robotic devices that assist people with tasks other than production and manufacturing, and are generally divided further into professional service and domestic use categories.[30] Professional service robots include nuclear power plant inspection robots, unmanned aerial vehicles (UAVs) for agriculture or infrastructure maintenance, deep sea and space exploration robots, and search and rescue robots. Domestic service robots assist people with tasks related to life and home management. Examples include elder and handicapped caretaker robots, medical rehabilitation robots, cleaning robots, nursing robots, surgery robots, and entertainment and education interactive robots.[31]

---

[28] James Hagerty, "Meet the New Generation of Robots for Manufacturing," *The Wall Street Journal*, June 2, 2015.
[29] "About," Rethink Robotics, accessed March 7, 2017, http://www.rethinkrobotics.com/about/.
[30] In most taxonomies, military robots and unmanned autonomous vehicles are considered a subset of service robots, given they engage in activities other than manufacturing.
[31] "《服务机器人科技发展"十二五"专项规划》解读" [Explanation of Service Robot Technology Development Twelfth Five Year Plan Special Program], China Robot Industry Alliance Web 中国机器人产业联盟网, May 7, 2012, accessed March 7, 2017, http://cria.mei.net.cn/news.asp?vid=1550.

A number of factors drive demand for service robots in China, including:

- Rising living standards are increasing demand for service robots, which offer comparatively inexpensive domestic services and serve as a status symbol for members of the growing middle class.[32] Higher wages and more leisure time are increasing interest in service robot technologies that can make life more comfortable or entertaining such as robotic vacuum cleaners, intelligent laundry machines, and smart toys.[33]
- China's aging population encourages the domestic service robot industry today, and can drive strong growth for the future. The CRIA notes that as of 2016 China has over 221.82 million citizens aged 60 years old or older, amounting to 16.15 percent of the total population.[34]
- As of 2016, China has approximately 60 million handicapped citizens who are limited in their capabilities or require nursing care, affecting almost one in ten Chinese households.[35]
- New service robot applications are also driven by technology "push" factors, such as the advent of improved AI and cloud computing technologies that greatly enhance service robot sophistication and their ability to act independently. Smart autonomous vehicles, logistics systems, and medical service robots are expected to continue to improve due to these advances.

China's government has provided industry guidance to the service robotics industry. Services robots were the focus of a special development program by China's Ministry of Science and Technology (MOST) during the Twelfth FYP period (2011 through 2015). The program built off previous Chinese advancements in service robots related to public security robots, bio-mimetic robots, and medical and rehabilitation robots.[36] In December 2015, CRIA, China's main government-sponsored robotics industry association, formally established a service robot expert committee (服务机器人专业委员会) in order to oversee and promote the healthy development of the service robot sector.[37]

Chinese manufacturers are at or near international standards for industrial, commercial, and recreational consumer UAV systems. Dai-Jiang Innovation Technology Company (DJI) was a startup in 2011, and today corners 70% of the market for commercial and recreational UAVs. The leading U.S. competitor was 3D Robotics, until missteps with its flagship UAV and ill-advised market projections led to its collapse. DJI outmaneuvered the company with consistent performance from basic models, introduction of newer

---

[32] Melanie Ehrenkranz, "This Rich Chinese Guy Traveling with 8 Robot Maids is Redefining Luxury," *Tech.Mic*, April 20, 2016, accessed March 7, 2017, https://mic.com/articles/141369/this-rich-chinese-guy-traveling-with-8-robot-maids-is-redefining-luxury.

[33] "三大国内服务机器人需求分析" [Analysis of Three Major Domestic Service Robot Needs], China Robot Industry Alliance Web 中国机器人产业联盟网, March 1, 2016, accessed March 7, 2017, http://cria.mei.net.cn/news.asp?vid=3282.

[34] "质疑和虚火 中国服务机器人不需要" [Doubts and False Fire – Chinese Service Robots Not Needed), China Robot Industry Alliance Web 中国机器人产业联盟网, April 27, 2016, accessed March 7, 2017, http://cria.mei.net.cn/news.asp?vid=3369.

[35] Ibid.

[36] "《服务机器人科技发展"十二五"专项规划》解读" [Explanation of Service Robot Technology Development Twelfth Five Year Plan Special Program], Ministry of Science and Technology of the PRC, accessed March 7, 2017, http://www.most.gov.cn/kjzc/zdkjzcjd/201205/t20120504_94140.htm.

[37] "中国机器人产业联盟成立服务机器人专业委员会筹备小组" [China Robot Industry Alliance Sets Up Small Group for Service Robot Expert Committee], China Robot Industry Alliance Web 中国机器人产业联盟网, December 10, 2015, accessed March 7, 2017, http://cria.mei.net.cn/news.asp?vid=3107.

models more quickly, and price cuts.[38] It appears difficult U.S. newcomers to compete in this industry, though newer companies like XCraft are innovating designs to break through the market.[39]

One advantage that U.S. firms have in the services robotics industry, including in China, is their brand recognition as the original pioneers of products and applications. For example, iRobot receives substantial attention from Chinese media as an innovator for service robots because of its broad scope of products, the use of their products in disasters that garner media attention, and their original applications for these systems. Examples include the global popularity of the Roomba vacuum cleaning robot, U.S. researchers' use of iRobot's unmanned underwater vehicle (UUV) Seaglider to assess the Deep Horizon Oil Spill in 2010, and Japanese rescue workers' deployment of PackBot robots during the Fukushima nuclear disaster in 2011.[40]

II. The PLA's Military Robotics and Unmanned Systems

China's leaders and military strategists believe the nature of warfare is changing and increasingly relies on unmanned and robotic systems. These weapons are appearing in the air, land, and sea domains, and necessitate that China develop its own systems and countermeasures. Consequently China is providing generous support to the R&D and production of unmanned systems, and is fielding increasingly capable systems. These unmanned systems and countermeasures against unmanned systems present challenges to the U.S. military operating in the Asia-Pacific region, particularly as U.S. defense planners implement the Third Offset strategy.

The Changing Nature of Warfare Necessitates Unmanned Systems

China's defense planners consider many new technologies such as unmanned systems to be maturing rapidly and changing the nature of warfare. For example, the most recent edition of *Science of Military Strategy*,[41] an authoritative Chinese text on military affairs, states that "…intelligent technology, unmanned technology, stealth technology, and other types of new concept technology are integrating together, and will perhaps give future warfare "unmanned, intangible, and silent" characteristics."[42] In 2015, senior analysts at China's National University of Defense Technology (NUDT) wrote that unmanned systems are as revolutionary as steam engines, tanks, airplanes, missiles, and the Internet.[43]

---

[38] Ryan Mac, "Behind The Crash Of 3D Robotics, North America's Most Promising Drone Company," *Forbes*, October 5, 2016, accessed March 7, 2017, https://www.forbes.com/sites/ryanmac/2016/10/05/3d-robotics-solo-crash-chris-anderson/#65e7c4473ff5.

[39] XCraft, accessed March 7, 2017, Ben Russell, "XCraft After Shark Tank – Recent Updates for 2017," June 19, 2016, accessed March 7, 2017, http://xcraft.io/; http://gazettereview.com/2016/06/xcraft-after-shark-tank-update/.

[40] "给力高交会开启机器人家居新时代" [The Awesomeness of iRobot Will Start a New Era for Robotic Households], China Finance 中国财经, March 7, 2017, accessed September 29, 2016, http://finance.china.com.cn/roll/20111118/262674.shtml.

[41] The *Science of Military Strategy* is produced by the staff of the Academy of Military Science, the PLA's highest-level research and education institute. It represents officially endorsed (or at least sanctioned) views of military affairs, other national security topics, and developments in sciences and technologies with defense applications.

[42] Shou *The Science of Military Strategy*, 97-98.

[43] Zhu Qichao 朱启超, Liu Jifeng 刘戟锋, and Zhang Huang 张煌, "科技革命视野中的军事战略创新" (Military Strategic Innovations from the

China's 2015 Defense White Paper on the "National Security Situation" endorses these views, claiming that the "…world revolution in military affairs (RMA) is proceeding to a new stage. Long-range, precise, smart, stealthy and unmanned weapons and equipment are becoming increasingly sophisticated."[44]

Chinese defense analysts consider these trends to be global and necessitate the PLA's own development of such systems and countermeasures. An article from the *PLA Daily* estimates that 70 countries have military robotics plans, and over 4,000 types of UAVs are available on the global market.[45] In addition to the United States, analysts follow developments in unmanned systems, particularly UAVs, in Russia, Israel, the United Kingdom, India, and others. Among these countries, unmanned systems are increasingly able to operate autonomously, fuse different intelligence and data, participate in joint manned and unmanned operations, and conduct operations with multiple unmanned systems.[46]

Trends in PLA's Development and Deployment of Unmanned Systems

China is investing heavily in unmanned systems that improve key capabilities and can carry out an increasing variety of missions at land, air, and sea. Among these domains, China's UAVs are the most mature, and contribute to the PLA's long-range ISR and strike operations that could pose challenges to the U.S. military. While UUV capabilities appear to be more nascent, their development could advance China's anti-submarine warfare (ASW) capabilities and erode long-held U.S. advantages. To date, Chinese media has covered PLA drills or deployments of unmanned systems for various missions including counterterrorism,[47] ISR (including in the South China Sea),[48] various military exercises,[49]

Perspective of Scientific and Technological Revolution), *China Military Science* 中国军事科学 3, no. 135 (2014): 75-81, 92.

[44] "National Security Situation," Ministry of National Defense of the People's Republic of China, accessed March 7, 2017, http://eng.mod.gov.cn/Database/WhitePapers/2015-05/26/content_4586688.htm.

[45] Pang Hongliang 庞宏亮, "智能化军事革命曙光初现——从美'第三次抵消战略'解读军事技术发展轨迹" [The Smart Military Revolution Is Dawning–Interpreting the Track of Military Technology Development from the U.S. "Third Offset Strategy"], *PLA Daily* 解放军报, January 28, 2016, accessed March 7, 2017, http://www.mod.gov.cn/wqzb/2016-01/28/content_4637961.htm.

[46] Tao Chuanhui 陶传辉, "各国军队竞相发展无人作战平台 已渗入陆海空等空间" [Every Country's Military Competing in Development of Unmanned Combat Platforms Has Already Entered Land, Air, and Sea Spaces], *National Defense Reference* 国防参考, May 27, 2014, accessed March 7, 2017, http://www.mod.gov.cn/wqzb/2014-05/27/content_4512254_2.htm; "深度：印度无人机差点飞中国 传回图像让印军不敢信" [Depth: India's UAV Short of Flying to China, Returning Images Cause India's Military to Not Dare], Sina 新浪军事, May 10, 2016, accessed March 7, 2017, http://mil.news.sina.com.cn/jssd/2016-05-10/doc-ifxryhhh1873725.shtml.

[47] "China Unveils Most Advanced Drone at 2014 Peace Mission Drill," *CCTV English* 央视网, August 27, 2014, accessed March 7, 2017, http://english.cntv.cn/2014/08/27/VIDE1409091365559432.shtml.

[48] Ankit Panda, "South China Sea: China's Surveillance Drones Make it to Woody Island" *The Diplomat*, June 1, 2016, accessed March 7, 2017, http://thediplomat.com/2016/06/south-china-sea-chinas-surveillance-drones-make-it-to-woody-island/; Imogen Calderwood, "Satellite Image Reveals China Has Begun Using Drones with Stealth Capabilities in the South China Sea," *Daily Mail Online*, May 27, 2016, accessed March 7, 2017, http://www.dailymail.co.uk/news/article-3613173/Satellite-image-reveals-China-begun-using-drones-stealth-capabilities-South-China-Sea.html.

[49] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2016," (Washington, DC: U.S. Department of Defense, 2016), 5.

border patrol,[50][51] explosive ordnance disposal,[52] humanitarian assistance/disaster relief,[53] and combat support[54] (such as smaller UAVs for special forces).

A direct comparison between Chinese and U.S. unmanned systems is difficult, as both countries closely guard technical and performance parameters, but two trends are noteworthy. First, Chinese UAV manufacturers and their customers (both domestic and abroad) appear to emphasize lower price points and quantity over increased capabilities. Second, Chinese scientists and Department of Justice (DOJ) reporting on espionage cases strongly suggest that China lags behind the United States on technologies for propulsion, autonomous operation, advanced sensors, and data links.

Unmanned Aerial Vehicles (UAVs)

China has invested considerable resources into the research, development, and deployment of UAV capabilities. Though no official estimates of the PRC's spending on UAVs was found, one report from 2014 predicts that from 2013 to 2022, Chinese demand for military UAVs will grow 15 percent annually on average, increasing from USD 570 million in 2013 to USD 2 billion in 2022.[55] The PLA's demand for UAVs stems from their ability to enhance numerous capabilities and support a wide range of missions.

According to the 2013 *SMS*, both the PLA Air Force (PLAAF) and PLA Navy (PLAN) should prioritize improving surveillance, early warning, and command and control capabilities.[56] Additionally, the PLAAF should prioritize medium and long-range precision strike systems that extend PLA strike capabilities to the second island chain.[57] UAVs are ideal for all these missions. Russian media and at least one Chinese commercial analyst believe the "Soar Dragon" High Altitude Long Endurance (HALE) UAV could be used for guidance for the DF-21D anti-ship ballistic missile (ASBM), a threat to U.S. aircraft carriers operating in the region.[58]

---

[50] Guo Fahai 郭发海, Xiong Zhenxiang 熊振翔, Sun Liwei 孙力为 (Ed.), "'无人机'飞进边关哨所助力边防管控" ["UAV" Flies at Border Station Post and Assists in Border Defense Control], Ministry of Defense Online 国防部网, February 29, 2016, accessed March 7, 2017, http://www.mod.gov.cn/hdpic/2016-02/29/content_4645198.htm.

[51] "解放军单兵机器人亮相中朝边境 射击弹无虚发" [PLA Single Soldier Robot Makes Appearance at China-Korea Border, Fires Munitions without False Fire], Sina 新浪军事, October 30, 2016.

[52] "解放军机器人中越边境执行任务:越南乐开花" [PLA Robot Conducts Mission on China-Vietnam Border: Vietnam is Happy], Sohu搜狐, April 25, 2016, accessed March 7, 2017, http://m.sohu.com/n/446034214/?wscrid=32576_2.

[53] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2016," (Washington, DC: U.S. Department of Defense, 2016), pp. 62-63.

[54] "解放军特种部队单兵无人机曝光" [PLA Special Forces Single Soldier UAV Exposed], *Global Times Online* 环球网, October 22, 2015, accessed March 7, 2017, http://mil.huanqiu.com/photo_china/2015-10/2806047.html.

[55] Feng Fuzhang [The UAV Industry Is Entering a Period of Rapid Development], China Securities¸ September 15, 2014, 14.

[56] Shou, *Science of Military Strategy*, 223-224; and Zhang Yueliang张岳良, Wu Qirong伍其荣, and Zhu Dan朱丹, "An Analysis of the 'All-Domain Access' Concept of the US Navy" [美国海军"全域进入"概念探析], *China Military Science* 中国军事科学, no. 4 (2015): 135-142.

[57] Shou, *Science of Military Strategy*, 223-224.

[58] Feng Fuzhang 冯福章, "无人机行业进入快速发展期" [The UAV Industry Is Entering a Period of Rapid Development], 证券研究报告 · 行业深度 [Securities Research Report · Industry in Depth], China Securities 中信建设证券¸ September 15, 2014, 14; "俄媒称"翔龙"无人机可引导DF-21D反舰弹道导弹" [Russian Media Claims the "Soar Dragon" UAV Could Guide the DF-21D Anti-ship Ballistic Missile], UAV Network全球无人机网, July 5, 2011, accessed March 7, 2017, http://www.81uav.cn/uav-news/201107/05/904.html.

Looking ahead, Chinese defense companies have demonstrated unmanned combat aerial vehicles (UCAVs), but their status remains unclear. UCAVs are ideal systems for high-risk missions such as suppression of enemy air defenses (SEAD). China's UCAVs seen to date include Lijian (利剑 / Sharp Sword), which completed taxi tests in May 2013; the Anjian (暗剑 / Dark Sword), which is reported to be capable of supersonic speeds and carry air-to-air weapons; and the Zhanying (战鹰 / Warrior Eagle), designed for SEAD missions.[59]

Unmanned Underwater Vehicles (UUVs)

China has made drastic progress on UUV technologies, as evidenced by increases in the numbers of teams working on the relevant technologies at major research institutes and universities, increased funding (mainly from the PLA), and recent technological breakthroughs.[60] UUVs, deep sea submergence vehicles (DSVs), and other underwater robotics systems are useful for commercial activities such as laying and repairing undersea cables and exploring natural resources. In 2016, Chinese UUVs carried out exploration missions in the southwest Indian Ocean searching for sulfide deposits and precious metals.[61] These vehicles can also, however, wiretap, disrupt, or sever undersea cables, as well as support ASW operations.

The Zhishui series of autonomous underwater vehicles (AUVs) may currently be in service with the PLA Navy.[62] According to a military enthusiast website, the Zhishui-III entered service with the PLAN in 2000, and is a large 2,000 kg UUV with twin propellers and two cross-tunnel thrusters for maneuvering.[63] According to authors with Harbin Engineering University (HEU), in 2003 the university's Underwater Intelligence Robot Technology Laboratory (水下智能机器人技术实验室) completed the "Zhishui-IV" underwater robot. The design incorporated a large number of more advanced sensors, including ones for depth, elevation, GPS, compasses, velocity, collision avoidance sonar, 3D imaging sonar, and TV.[64]

China is actively exploring newer concepts for UUV designs and technologies. In 2014, Tianjin University and the National Ocean Technology Center in Tianjin completed a sea trial for the Haiyan (海燕) AUV in the northern area of the South China Sea.[65] This AUV is an underwater glider, which uses small changes

[59] Kimberly Hsu, Craig Murray, and Jeremy Cook, "China's Military Unmanned Aerial Vehicle Industry," U.S.-China Economic and Security Review Commission, June 13, 2013.

[60] Michael S. Chase, Kristen A. Gunness, Lyle J.Morris, Samuel K. Berkowitz, and Benjamin S. Purser III, "Emerging Trends in China's Development of Unmanned Systems," (Arlington, VA: RAND Corporation, 2015), 3.

[61] "Chinese Submersible Explores Indian Ocean for Precious Metals," *Economic Times*, March 24, 2016, accessed March 7, 2017, http://economictimes.indiatimes.com/news/international/world-news/chinese-submersible-explores-indian-ocean-for-precious-metals/articleshow/51542348.cms; "China may build seabed 'space station' to help hunt for minerals in South China Sea," *Japan Times*, June 8, 2016, accessed March 7, 2017, http://www.japantimes.co.jp/news/2016/06/08/asia-pacific/china-may-build-seabed-space-station-help-hunt-minerals-south-china-sea/.

[62] Zhishui is likely a shortened version of 智慧 (*zhihui*, intelligent) and 水下机器人 (*shuixia jiqiren*, underwater robot).

[63] "Zhishui," NavalDrones, accessed March 7, 2017, http://www.navaldrones.com/Zhishui.html.

[64] Zhao Jiamin 赵加敏, Xu Yuru徐玉如, and Lei Lei雷磊, "用于水下机器人智能路径规划的仿真器的建立" (A Simulator for the Test of Intelligent Path Planning of AUV), *Journal of System Simulation* 系统方针学报16, no. 11 (November 2004): 2448-2450.

[65] "天津大学研发水下滑翔机技术创多项国内纪录" [Tianjin University Developed Underwater Glider Technology and Created Multiple Units in Domestic Record], CERNET China Education and Research Network 中国教育和科研计算机网, May 26, 2014, accessed March 7, 2017, http://www.edu.cn/cheng_guo_zhan_shi_1085/20140526/t20140526_1119599.shtml.

in buoyancy and its wings to convert vertical motion into horizontal motion. This system is slower but more energy efficient, enabling longer surveillance and exploration missions.

Unmanned Surface Vehicles (USVs)

China has made advancements in this field, most notably with its Jinghai (精海) series. In July 2016 Xinhua reported on the progress of Jinghai-series models, developed under the leadership of Shanghai University's Unmanned Vessel Engineering Institute (上海大学无人艇工程研究院).[66] These activities included the following:[67]

- In 2013 the Jinghai-1 USV accompanied a Chinese coast guard vessel around the Paracel and Spratly Islands in the South China Sea, completing topographical and hydrological surveys.
- In 2014 the Jinghai-2 accompanied the "Snow Dragon" (雪龙) on China's 31st expedition to the South Pole, conducting topography surveys.
- The Jinghai-3 uses a highly modularized design and the most advanced "intelligent obstacle avoidance guidance systems."

Unmanned Ground Vehicles (UGVs)

China's deployment of unmanned ground systems (UGVs) to date appears limited. UGVs encompass numerous vehicles that operate on land with a human operator or autonomously. They can execute military missions including combat, ordnance disposal, and transport. U.S. forces in Iraq and Afghanistan used UGVs such as TALON and Warrior "…to detect and defeat roadside bombs, gain situational awareness, detect chemical and radiological agents, and increase the standoff distance between Soldiers and potentially dangerous situations."[68]

Numerous Chinese civilian and defense companies, universities, and research institutes are developing UGVs and other unmanned ground systems. R&D on intelligent guidance for unmanned ground platforms received support from China's 973 and 863 programs for high-technology development, as well as the Twelfth FYP of the former General Armament Department (GAD).[69]

To spur these systems' development, in September 2016 the PLA hosted the "2016 Leap Over Treacherous Paths" (跨越险阻2016) contest. The contest featured five competitions to simulate battle operations

---

[66] "无人艇：在江河湖海中展露身手" [Unmanned Vessel: Showing Skill in All Waters], Xinhua 新华社, July 7, 2016, accessed March 7, 2017, http://news.xinhuanet.com/2016-07/07/c_1119182583.htm.
[67] Ibid; "Unmanned ships deemed helpful in survey and patrol of South China Sea," *Global Times* 环球网, July 8, 2016, accessed March 7, 2017, http://www.globaltimes.cn/content/993071.shtml.
[68] Robert Karlsen and Bob Van Enkenvoort, "Heftier Unmanned Ground Vehicle Offers More Lifting, Hauling Strength," U.S. Army news item, June 4, 2013, accessed March 7, 2017, https://www.army.mil/article/104710. For more on TALON and other UGVs, see Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*, (New York: Penguin, 2009), 26-30.
[69] "北理工杨毅老师被授予第八届海淀区"十大杰出青年"称号" [Beijing Institute of Technology Professor Yang Yi Awarded the Eighth Haidian District "Ten Outstanding Youth" Title], Beijing Institute of Technology, accessed March 7, 2017, http://www.bit.edu.cn/xww/mtlg/105218.htm.

including rough terrain battlefield reconnaissance, rough terrain battlefield marching in formation, urban battlefield reconnaissance and search, transport in mountainous regions by bionic unmanned platforms, and transport in mountainous regions by non-bionic unmanned platforms.[70]

"Military-Civilian Fusion" in China's Robotics Industries

Across many industries, China is pursuing its strategy of "military-civilian fusion" (军民融合), in which military, commercial, and academic entities are encouraged to jointly develop and share breakthroughs in technologies.[71] Robotics and related technologies such as artificial intelligence are ideal for this "fusion" as commercial companies outpace their military counterparts. This close integration of military and civilian institutes poses diversion risks for U.S. entities as cooperation agreements, academic exchanges, and investments can inadvertently support PLA end-users. One example is the Chinese Association for Artificial Intelligence (CAAI), which leads international academic exchanges for AI, but also has leaders and member institutions with military affiliations. Another potential example is Chinese investment in Neurala, a Boston-based company for AI software for UAVs and other unmanned systems that has potential military applications. These cases and other technology transfer risks are discussed in more detail in the section below on China's acquisition of foreign robotics technology.

Challenges for China's Unmanned Systems

China is proficient in unmanned system designs and manufacturing, but lags behind the United States on advanced components. In a 2013 interview with a Chinese UAV designer, challenges included capabilities, engines, data links, and airborne electronics as challenges for China's systems.[72] According to the designer, China's data links and airborne electronics in particular lag behind U.S. standards, making systems such as the RQ-4 Global Hawk and the X-47B the global standard. China also has traditionally struggled with advanced materials such as high-grade carbon fiber, and acquired it through illicit means.[73][74]

For UUVs, China has sought advanced components from the United States. The technology transfer discussion below includes the case of Yu Amin, AKA Amy Yu. In June 2016 Yu pleaded guilty to acting

[70] "跨越险阻-2016"地面无人系统挑战赛等你来战！" [The 2016 Leap over Treacherous Paths Ground Unmanned Systems Competition Welcomes You to Come Compete!], *China Military Network* 中国军网, June 14, 2016, accessed March 7, 2017, http://www.81.cn/jmywyl/2015-02/27/content_6372686_5.htm.
[71] For more on "military-civilian fusion" and China's civil-military integration policies, see Daniel Alderman, Lisa Crawford, Brian Lafferty, and Aaron Shraberg, "The Rise of Chinese Civil-Military Integration" in Tai Ming Cheung (ed.), *Forging China's Military Might: A New Framework for Assessing Innovation* (Baltimore, MD: Johns Hopkins University Press, 2014), 109-135.
[72] Zhao Lei, "Foreign Buyers Eye Chinese Drones," *China Daily USA*, June 20, 2013.
[73] Chen Shaojie 陈绍杰, "Composite Materials and UAVs" [复合材料与无人飞机], *Hi-tech Fiber & Application* 高科技纤维与应用, no. 2 (2003); and Chen Shaojie 陈绍杰, "Brief Discussion of Shaping Technologies for Composite Structures" [浅谈复合材料整体成形技术], *Aeronautical Manufacturing Technology* 航空制造技术, no. 9 (2005).
[74] Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases (January 2010 to the present: updated June 27, 2016)," June 2016, p. 7, https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download

in the United States as an illegal agent of a foreign government and obtaining systems and components from U.S. companies for marine submersible vehicles, likely including UUVs.[75]

The PLA Seeks to Exploit the U.S. Military's Dependence on Unmanned Systems

The PLA considers the U.S. military to be increasingly dependent upon unmanned systems, and actively researches countermeasures to such systems. The Third Offset strategy's emphasis on unmanned systems and human-machine collaboration confirmed what China perceived to be the growing importance of unmanned systems in the U.S. military. One analyst writes that robots and unmanned systems will outnumber people in the U.S. military by 2040.[76] With this assessment that the U.S. military is heavily invested in unmanned systems, the PLA has demonstrated and funded research into soft- and hard-kill countermeasures.

Chinese analysts consider the United States to be a pioneer in the development of unmanned systems, and have closely followed their deployment. Writing on the history of military UAVs, a PLAAF senior colonel follows the U.S. deployment of UAVs from the first Gulf War to the War on Terrorism.[77] The 2013 *SMS* discusses the U.S. military's use of UAVs for precision strikes in Afghanistan, Pakistan, and Libya.[78] Analysts also consider the United States to be a leader in the development and application of UGVs, citing systems such as the Scorpion Small UGV, SWORDS armed system, Packbot, and Big Dog.[79]

Among the military services, Chinese analysts consider the U.S. Navy to be the most dependent upon unmanned systems. They are following the Navy's plans to develop large-scale long-deployment autonomous unmanned submersibles, the X-47B, and ship-launched unmanned aerial surveillance and attack systems, and estimate the Navy will have a fleet of 1,000 unmanned submersibles by 2020.[80] One program receiving special interest is the ASW Continuous Trail Unmanned Vessel (ACTUV) program funded by the U.S. Defense Advanced Research Projects Agency (DARPA),[81] which is a "vessel

---

[75] Ibid., p. 4.

[76] Hu Yiming 胡一鸣, "剑指未来，"白头鹰"再掀革新风暴" [Sword of the Future, "Bald Eagle" Raising a Storm of Innovation Again], *PLA Daily* 解放军报, February 27, 2016, accessed March 7, 2017, http://www.mod.gov.cn/wqzb/2016-02/27/content_4645032.htm.

[77] Chen Guichen 陈贵春 (Ed.), Min Zengfu 闵增富, and He Yuesheng 何月生 (Asst. Eds.), *军用无人机* [Military Unmanned Vehicles] (Beijing: PLA Publishing House, 2008), 202-205.

[78] Shou, *Science of Military Strategy*, 97-98.

[79] Lu Tiange 陆天歌, Hu Yajun 胡亚军, Wu Meng 武萌, "军用机器人迎来发展机遇期" [Military-Use Robots Forging Ahead in a Period of Favorable Development], *Liberation Army Daily* 解放军报, December 2, 2015, accessed March 7, 2017, http://news.mod.gov.cn/tech/2015-12/02/content_4631281.htm; Tao Chuanhui [Every Country's Military Competing in Development of Unmanned Combat Platforms Has Already Entered Land, Air, and Sea Spaces], May 27, 2014.

[80] Li Daguang 李大光, "A Strategic Analysis of US Future Defense Orientation" [美国未来防务走向战略分析], *China Military Science* 中国军事科学, no. 5, 2012, 142; and Qiang Dong 钱东, Tang Xianping唐献平, and Zhao Jiang 赵江, "UUV 技术发展与系统设计综述" (Overview of Technology Development and System Design of UUVs), *Torpedo Technology* 鱼雷技术22, no. 6 (December 2014): 401-414.

[81] The Defense Advanced Research Projects Agency (DARPA) is a DOD agency responsible for developing emerging technologies for use by warfighters. The agency has sponsored projects that made technological breakthroughs in unmanned system technologies, battlefield robotics, computer networking, and artificial intelligence among many others.

optimized to robustly track quiet diesel electric submarines."[82] Chinese research and military institutes track the system and assume it is targeting China's diesel attack submarines.[83]

Chinese analysts perceive the United States to be dependent on unmanned systems for financial and technological reasons, a view confirmed by the Third Offset. Following the U.S. budget debates in 2012 and sequestration cuts of 2013, Chinese analyst concluded that financial constraints will make the U.S. military even more dependent upon technological advantages like unmanned systems.[84] The Third Offset strategy's objective to leverage technological advantages such as human-machine collaboration confirms these analysts' views, and convinces them that the strategy and emphasis on unmanned systems are aimed at China.

With this in mind, it is not surprise that China is investing heavily in countermeasures against unmanned systems. The 2013 *SMS* calls for innovating countermeasures against UAVs in particular, and military research institutes routinely use U.S. systems as examples and targets in their research.[85] The most illustrative example of such research is an article titled "Analysis of X-47B UCAS and Electronic Counter Measures" that appeared in *Aerospace Electronic Warfare*, China's leading journal on electronic warfare.[86] The authors assess that this system has advantages in stealth, flexibility for different operations, and the ability to carry out long-range precision strikes. In the authors' assessment, the critical weakness of the X-47B is that if it loses contact with controllers or is confused, the system defaults to returning to base. Hence they propose countermeasures such as electronic interference to negate information collection capabilities and better camouflage for targets to force the system to return to base. Kinetic countermeasures include air-based intercepts, obstacles (such as balloons), early warning fighter intercepts, and even preemptive strikes on the launch platform (such as an aircraft carrier).[87]

Some of these non-kinetic countermeasures appear to already be in operation. In 2015 a U.S. press report claimed the PLA attempted to jam a Global Hawk UAV operating over the South China Sea, and Chinese authors followed Iran's downing of the RQ-170 UAV in 2011 by interfering with its navigation system.[88] These non-kinetic countermeasures likely are attractive to the PLA because they can be used for

---

[82] Scott Littlefield, "Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV)," Defense Advanced Research Projects Agency, accessed March 7, 2017, http://webcache.googleusercontent.com/search?q=cache:23zPJFueENwJ:www.darpa.mil/program/anti-submarine-warfare-continuous-trail-unmanned-vessel+&cd=1&hl=en&ct=clnk&gl=us.
"人艇作战使用分析" [Analysis of U.S. Anti-Submarine Unmanned Surface Vehicles Operations and Uses], *Ship Electronic Engineering* 舰船电子工程, no. 8 (2012).
[83] Wang Chuan 汪川, "DARPA: 美军战略优势的技术创新支柱" (DARPA: The Technological Innovation Backbone of the U.S. Military's Strategic Advantages), *Military Digest*军事文摘 (June 2015): 51-54; Tian Jun田军, She Yajun余亚军, and Cai Long 蔡龙, "针对持续性跟踪无人艇的探测技术" (Research on Detection Technology on ACTUV), *Ship Science and Technology*舰船科学技术35, no. 4 (2013).
[84] Li Daguang, "A Strategic Analysis of US Future Defense Orientation," p. 142.
[85] Shou, *Science of Military Strategy*, 101.
[86] Wu Xiaofang 吴晓芳, Tian Zhongcheng 田中成, and Liang Jingxiu 梁景修, "X-47B无人空战系统及其对抗途径分析" (Analysis of X-47B UCAS and Electronic Counter Measures), *Aerospace Electronic Warfare*航天电子对抗, vol. 29, no. 5 (2013): 11-13.
[87] Ibid.
[88] Gertz, Bill. "Chinese Military Using Jamming Against U.S. Drones–Global Hawk Targeted Over Disputed South China Sea Islands," *Washington Free Beacon*, May 22, 2015; and Wang Haoyu王灏宇, Fan Hongshen范宏深, and Zhao Guowei赵国伟, "The Function Demand of Spacecraft by the Integration of the Net Electric for Space Warfare" (空间作战融合网电力量对航天器的功能需求), *Aerospace Electronic Warfare 航天电子对抗*, no. 5 (2014): 24-27.

interference in peacetime, and in a crisis are less escalatory than a kinetic kill. These options pose challenges for the U.S. military power projection in the Asia-Pacific region as unmanned systems become increasingly integral to ISR and other capabilities.

III. China's Acquisition of Foreign Robotics Technology

China actively acquires components, technologies, and materials from abroad for its robotics industry and military unmanned systems. From a commercial standpoint, technology transfers can greatly improve the quality of Chinese robotics systems, particularly for higher end components that have been a chronic weakness of the industry. From a security standpoint, intelligence on U.S. unmanned systems can improve China's own military assets and provide insights into countermeasures. This section breaks down China's acquisition and technology transfer efforts by the following categories:

- **Illicit technology acquisitions** include the illegal means through which China acquires key technologies from abroad, such as cyber intrusions and export control violations.
- **Informal knowledge and technology transfers** refer to China's acquisition of foreign technologies via open source collection, talent recruitment, and academic exchanges.
- **Formal technology acquisitions and investments** involve Chinese companies acquiring or investing in foreign robotics companies or other entities to acquire targeted technologies.

Illicit Technology Acquisition

China actively seeks U.S. technologies for unmanned systems through illicit means including cyber intrusions into sensitive U.S. defense contractors and state entity-directed efforts to circumvent U.S. export controls.

China's vast cyber espionage campaign has directly contributed to its unmanned systems, including UAVs and UGVs. In 2013 a U.S. cybersecurity company reported on a massive two-year operation dubbed Operation Beebus by Chinese hackers to steal U.S. designs and relevant technologies for UAVs.[89] Of the 261 attacks uncovered, 123 of them are reported to have targeted U.S. UAV companies.[90] According to a manager of the investigation, "We believe the attack was largely successful."[91] Other cyber targets include companies such as QinetiQ North America, a major supplier of UAVs, satellites, helicopters, military robotics, and other systems for the U.S. military.[92] According to news reports, the hackers first targeted

[89] Edward Wong, "Hacking U.S. Secrets, China Pushes for Drones," *The New York Times*, September 20, 2013.
[90] Alex Pasternack, "Hackers Are Helping China Build Cheap Clones of America's Drones," Motherboard, September 23, 2013, accessed July 6, 2016, https://motherboard.vice.com/blog/hackers-are-helping-china-build-cheap-clones-of-americas-drones.
[91] Dunn, John, "Chinese malware targeted US drone secrets, security firm alleges," *TechWorld*, February 4, 2013.
[92] Riley, Michael and Elgin, Ben, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg, May 1, 2013.

QinetiQ's UAV and robotics technologies. Then in April 2012, the PLA displayed a bomb disposal robot similar to QinetiQ's Dragon Runner, likely reflecting the use of this stolen data.[93]

According to the DOJ and the Bureau of Industry Security (BIS) at the U.S. Department of Commerce, numerous individuals in the United States have attempted to illegally export unmanned systems and their relevant components and materials to China. Since 2010, DOJ reporting includes six cases in which China has sought to acquire U.S. unmanned systems and their technologies.[94] BIS reports that between 2007 and 2008, a couple in the United States illegally exported miniature UAV autopilots to Xi'an Xiangyu Aviation Technical Group in China.[95]

On June 10, 2016, Amin Yu, AKA Amy Yu, pleaded guilty to acting in the United States as an illegal agent of a foreign government without prior notification to the Attorney General.[96] According to the plea agreement, Yu obtained systems and components from U.S. companies for marine submersible vehicles (such as UUVs).[97] She then illegally exported the components to the PRC. She acted at the direction of co-conspirators working for Harbin Engineering University, a leading Chinese institute for commercial and military UUV research.[98]

Informal Knowledge and Technology Transfers

China actively acquires U.S. technology through informal means that are extralegal, or not clearly defined and regulated by current U.S. legislation. These means include leveraging a vast open source intelligence apparatus, recruitment of leading talents from around the world, and academic exchanges. These means are not properly defined and regulated by existing U.S. legislation, but as one analysis states, "There is a thin line between stealing secrets and informal technology transfer, and China pursues the latter to the limit."[99]

China leverages a vast open source collection and exploitation system to spot, study, and acquire data concerning foreign technologies that China has not yet been able to develop on its own.[100] This system features institutions that monitor foreign technical developments, disseminate information to relevant Chinese institutions, and model foreign R&D for domestic programs. In the field of UAVs, a leading

---

[93] Ibid.
[94] Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases."
[95] U.S. Department of Commerce, "Don't Let This Happen to You: Actual Investigations of Export Control and Antiboycott Violations," Bureau of Industry and Security, Export Enforcement, July 2015 Edition, 45-46.
[96] Ibid.
[97] According to the indictment, Yu exported the following components: underwater acoustic locator devices; underwater cables and connectors, including AWQ/XSL and MSSK/MINL Marine Cables; PC104 computer processing units for mission, motion and video guidance computers; 907 Multiplexers for digital signal transmission through fiber optics; underwater pressor [sic] sensor, conductivity and temperature sensor; and control sticks and button strips.

[98] United States of America v Amin Yu, Case No. 6:16-cr-23-Orl-37GJK, (FL, United States District Court, Middle District of Florida, Orlando Division March 26, 2016), accessed on July 6, 2016, https://www.justice.gov/usao-mdfl/file/843506/download.
[99] William C. Hanas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (London: Routledge, 2013), 2.
[100] Ibid., 18-49.

collection institute is the 310th research institute (RI) under the China Aerospace Science and Industry Corporation (CASIC). The 310th RI closely follows UAVs, aircraft, and missiles of foreign countries, and publishes the *Aerodynamic Missile Journal* (飞航导弹), which "introduces intelligence on relevant foreign flying missiles, and advances the rapid development of China's flying missile industry." [101]

Other Chinese researchers utilize publicly available images and data on U.S. programs, likely to advance their own research and to develop countermeasures. For UCAVs, Chinese researchers have modeled the X-47A prototype's slot-shaped inlet,[102] discussed the designs in context of decreased infrared signatures,[103] and simulated configurations and drag effects of what appears to be the X-45A's weapons bays.[104] For the X-47B system that will enter deployment, in 2013 researchers published "Analysis of X-47B UCAS and Electronic Counter Measures," an assessment of the X-47B's advantages and potential weak points for Chinese countermeasures.[105]

The Chinese government actively recruits Chinese and foreign experts living abroad to work in China and boost domestic R&D in critical technologies. The central government organizes and guides this effort with active participation at lower levels. The leading program is the Thousand Talents Program (千人计划).[106] Many of China's top-level experts on robotics and related technologies are Thousand Talent professors at Chinese research institutes, laboratories, and centers with concurrent affiliations outside of China. In the case of robotics, many of these Thousand Talent recruits have educational and work experience outside of China in top-tier research institutions in Germany, Japan, and the United States.

Chinese research institutes and universities actively participate in and host international conferences on technologies such as robotics and artificial intelligence. Although most of China's participation is likely benign in nature, some attendees participate on behalf of Chinese defense firms and military research institutes. For example, Chinese Association for Artificial Intelligence (CAAI) is China's leader in promoting academic exchange, publication, education, and research exhibition for artificial intelligence.[107] CAAI participants, however, include the PLA General Staff Department, National University of Defense Technology, and National Defense University. [108] Furthermore, CAAI's leader is

[101] "飞航导弹" (Aerodynamic Missile Journal), Wanfang Data Periodical Profile, accessed May 11, 2016, http://c.wanfangdata.com.cn/PeriodicalProfile-fhdd.aspx.
[102] Zhang Hang 张航, Tan Huijun 谭慧俊, and Li Xiangping 李湘萍, "类X-47狭缝式进气道的流动特征与工作性能" [Flow Structure and Performance Characteristics of X-47-like Slot-shaped Inlet], *Acta Aeronautica et Astronautica Sinica*航空学报 (December 2009), 2243-2249.
[103] Xu Xingguo 徐顶国, Sang Jianghua桑建华, and Luo Mingdong 罗明东, "Research on Application of UAVS' Infrared Stealth Technology" [红外隐身技术在无人机上的应用研究], *Infrared and Laser Engineering* 红外与激光工程 (December 2012).
[104] Feng Qiang冯强and Cui Xiaochun崔晓春, "Study on Integrated Flow Control for Weapons Bay of Flying Wing Configuration Aircraft" [飞翼布局飞机弹舱综合流动控制技术研究], *Acta Aeronautica et Astronautica Sinica* 航空学报 (May 2012).
[105] Wu, Tian, and Liang, "(Analysis of X-47B UCAS and Electronic Counter Measures)," pp. 11-13.
[106] "千人计划介绍" [The Recruitment Program of Global Experts], accessed March 7, 2017, http://www.1000plan.org/qrjh/section/2?m=rcrd#.
[107] "中国人工智能学会简介" [Chinese Association for Artificial Intelligence Introduction], Chinese Association for Artificial Intelligence 中国人工智能学会, accessed March 7, 2017, http://new.caai.cn/index.php?s=/Home/Article/index/id/2.html.
[108] "中国人工智能学会第七届理事会负责人名单" [Chinese Association for Artificial Intelligence Seventh Board Member Leadership Name List], Chinese Association for Artificial Intelligence 中国人工智能学会, accessed March 7, 2017,

Li Deyi (李德毅), whom English-language sources describe as an academic and professor, but Chinese-language credentials openly state is a major general in the PLA.[109] Li has worked on national defense electronics key engineering development projects, is deputy director of the All-Army Informatization Work Office (全军信息化工作办公室), and has served as a member of the former General Armament Department's Science and Technology Committee (总装备部科技委).[110]

Formal Technology Acquisition and Investments

Chinese state-owned conglomerates, companies, and venture capital (VC) firms are actively acquiring or investing in foreign AI and robotics companies. According to one U.S. financial advisory firm, Chinese investors are "poised to target artificial intelligence deals in [the] U.S.,"[111] While China's AI investments are more recent, its robotics investments trend are accelerating, as there has been a drastic increase of Chinese companies and VC firms trying to acquire or invest in European robotics companies. A benign explanation is that Chinese companies are investing capital abroad to acquire good investments. With Made in China 2025 and other state plans emphasizing robotics, however, these investments appear more targeted. One observer characterizes the plans as a "shopping list" for foreign investment targets that could help China acquire key technologies and licenses to improve its own industries.[112]

Recent AI and robotics deals since 2015 include the following:

- Haiyin Capital's investment in Boston-based Neurala - In June 2016, Haiyin Capital invested $1.2 million in Neurala, a maker of AI software that will soon be integrated into UAVs, self-driving cars, and toys.[113] The software is capable of navigation as well as identifying, classifying, tracking, and avoiding obstacles. This software could benefit military end-users as the AI software in military UAVs must accomplish all these functions. As of 2014 Neurala had contracts with NASA and the U.S. Air Force to develop smart learning systems, which may support collision avoidance systems for UAVs and autonomous navigation systems for robots on Mars.[114] In October 2015, NASA awarded Neurala a $250,000 grant to commercialize autonomous navigation, object

---

http://new.caai.cn/index.php?s=/Home/Article/detail/id/85.html; "中国人工智能学会2016副秘书长名单" [Chinese Association for Artificial Intelligence 2016 Vice-Secretary Name List], Chinese Association for Artificial Intelligence 中国人工智能学会, accessed March 7, 2017, http://new.caai.cn/index.php?s=/Home/Article/detail/id/114.html; "公司概况" [Company Summary], Horizon Robotics, accessed March 7, 2017, http://www.horizon-robotics.com/company_cn.html.

[109] Li Deren, Li Deiyi, and Wang Shuliang, *Spatial Data Mining: Theory and Application*, Springer-Verlag Berlin Heidelberg (2015): xxvi; Li Deyi and Du Yi, *Artificial Intelligence with Uncertainty*, Chapman & Hall/CRC, 2008; "Plenary Speech," 3rd CIS & RAM on Cybernetics and Intelligent Systems Robotics, Automation, and Mechatronics, an IEEE conference, September 21-24, 2008, accessed March 7, 2017, http://www.cis-ram.org/2008/ple-spe.html.

[110] Ibid; "专家介绍——李德毅" [Expert Introduction—Li Deyi], Chinese Association for Artificial Intelligence 中国人工智能学会, accessed June 9, 2016, http://caai.cn/contents/108/1711.html (webpage inactive as of March 7, 2017).

[111] "Chinese Investors Poised to Target Artificial Intelligence Deals in U.S.," blog post by Vasari Capital, January 30, 2016, accessed March 7, 2017, http://www.vasaricapital.com/chinese-investors-poised-to-target-artificial-intelligence-deals-in-u-s/.

[112] Sebastian Heilmann, "Europe Needs Tougher Response to China's State Led Investments."

[113] Sara Castallanos, "Chinese Investors Bet on Boston AI Tech for Drones, Toys, Self-Driving Cars," *Boston Business Journal*, June 2, 2016, accessed March 7, 2017, http://www.bizjournals.com/boston/blog/startups/2016/06/chinese-investors-bet-on-boston-ai-tech-for-drones.html.

[114] Dennis Keohane, "Tim Draper Backs Boston Robot Software Company Neurala," *The Boston Globe*, December 10, 2014, accessed March 7, 2017, http://www.betaboston.com/news/2014/12/10/tim-draper-backs-boston-robot-software-company-neurala/.

recognition, and obstacle avoidance technology in UGVs and UAVs.[115] Chinese investment in Neurala potentially poses at least two risks for the United States. One is that Chinese access to source code and underlying technologies behind Neurala software could benefit PLA end-users. Another is that it is unclear if China's access to Neurala will prevent U.S. end-users from taking advantage of the company's technology, effectively wasting previous U.S. contracts and grant money.

- Midea Group's investment in KUKA – In February 2016, Midea Group, a major Chinese producer of home appliances, began increasing its shares in the leading German robot manufacturer Kuka AG, and by July 7th held a majority stake in the company.[116] KUKA has been a leading supplier of industrial robotics for Chinese companies for a long time.[117] According to one analysis, this acquisition raises questions on technology transfers, because KUKA is a supplier for the European defense industry, including robots used in the construction of the Eurofighter.[118] Leading German officials, including Chancellor Angela Merkel herself, were skeptical or opposed the deal, arguing that KUKA should remain an independently German brand, and that China must "level the playing field" for foreign investors in China.[119] KUKA also maintains U.S. operations, leading to a review of the Midea deal by the Committee on Foreign Investment in the United States (CFIUS) and the Directorate of Defense Trade Controls (DDTC). To comply with the security-relevant requirements, in December 2016 KUKA sold KUKA Systems Aerospace North America to the U.S. company Advanced Integration Technology Inc.[120]
- AGIC Capital – In 2015 Henry Cai, who is regarded as the "godfather of the China capital markets," cofounded Asia-Germany Industrial Promotion Capital (AGIC). The purpose of this private equity firm is to invest in European companies and facilitate greater sales to China of advanced technologies including robotics, high-end systems and components, and advanced materials and technologies.[121] In June 2016 AGIC announced it would acquire a majority stake in Gimatic, a leading Italian supplier of end-of-arm tools for industrial automation and robotic applications.[122] The deal is reported to be worth USD 113 million.[123] These tools are ideal for

[115] "Neurala Receives $250,000 NASA Grant to Bring Autonomous Software to Self-Driving Cars, Home Robots and Drones," Neurala press release, October 23, 2015, accessed March 7, 2017, http://www.neurala.com/nasa-phase-iie/.
[116] "Midea, Kuka and the Rise of China's Robots," *The Economist*, July 12, 2016.
[117] Cai and Guo, "Development and Basic Problems of China's Industrial Robotics Development," 10-11.
[118] Sebastian Heilmann, "Europe Needs Tougher Response to China's State Led Investments."
[119] Arne Delfs and Patrick Donahue, "Merkel Confronts China Ambitions in Clash Over Robot Maker Kuka," *Bloomberg Technology*, June 10, 2016, accessed March 7, 2017, https://www.bloomberg.com/news/articles/2016-06-10/merkel-confronts-china-ambitions-in-clash-over-robot-maker-kuka; and Amie Tsang, "Midea of China Moves a Step Closer to Takeover of Kuka of Germany," *The New York Times*, July 4, 2016.
[120] "KUKA Sells Systems U.S. Aviation Section to Advanced Integration Technology Inc." press release for KUKA, December 15, 2016, accessed March 7, 2017, https://www.kuka.com/en-us/press/news/2016/12/kuka-sells-systems-us-aviation-section.
[121] "About Us," AGIC, accessed March 7, 2017, http://www.agic-group.com/about-us/; "EY Strategic Growth Forum China Speakers," Ernst & Young Global Limited, accessed March 7, 2017, https://webforms.ey.com/CN/en/Services/Strategic-Growth-Markets/EY-strategic-growth-forum-china-2016-speaker-henry-cai.
[122] "AGIC Capital Announces Acquisition of Gimatic Srl," press release by AGIC, June 13, 2016, accessed March 7, 2017, http://www.agic-group.com/agic-capital-announces-acquisition-of-gimatic-srl/.
[123] Eugene Demaitre, "China Continues to Invest in European Industrial Automation," Robotics Business Review, June 13, 2016, accessed March 7, 2017, https://www.roboticsbusinessreview.com/china-continues-invest-european-industrial-automation/.

industrial robots in the automotive, plastics, electronics, food, and pharmaceuticals industries, among others.

IV. Recommendations to Maintain U.S. Economic and Strategic Advantages

As China surges ahead with production and deployment of industrial, service, and military robotics systems, it is essential for the United States to define and protect its advantages and interests. For industrial and service robots, the United States should focus on the advantages of quality and innovation, and support both U.S. entities developing new technologies for robotics and U.S. businesses trying to compete in the Chinese market. For military systems, the United States holds technological advantages that must be protected from cyber intrusions and other illicit activities, and take into account China's rapid development of countermeasures against these systems.

Below are more detailed recommendations for Congressional and Executive action to maintain and increase U.S. economic and strategic advantages.

1. The Congress should continue to support initiatives that advance U.S. manufacturing and innovation in the industrial and service robotics industries, such as Manufacturing USA and the National Robotics Initiative, and monitor Chinese plans like Made in China 2025 to ensure it does not exclude U.S. companies from Chinese markets.

2. U.S. defense planners should monitor and account for Chinese advances in unmanned systems and electronic countermeasures that may improve anti-access/area denial (A2/AD) capabilities such as long-range precision strike and anti-submarine warfare.

3. The U.S. Government should increase awareness among federal agencies, defense contractors, and research universities that Chinese research institutes actively collect their published materials, designs, specifications, and graphics to assess U.S. military systems and guide Chinese research.

4. The U.S. Government should fully implement the Cybersecurity National Action Plan (CNAP) and incorporate input from companies and research institutes that develop unmanned systems, robots, and their relevant technologies.

5. To help counter Chinese espionage against unmanned systems and other sensitive technologies, the U.S. Government should better exploit China's state plans, procurement practices, defense plans, and other Chinese language materials. Such sources identify technologies that the Chinese government is seeking to acquire and would provide advance warning to U.S. law enforcement.

6. The U.S. Government, in particular the Committee on Foreign Investment in the United States (CFIUS), should monitor and when necessary investigate China's growing foreign investments in

robotics companies, and consider the security implications of transactions and acquisitions involving emerging technologies such as artificial intelligence and nanorobotics.

OPENING STATEMENT OF PATRICK J. SINKO
ASSOCIATE VICE PRESIDENT FOR RESEARCH AND DISTINGUISHED PROFESSOR OF PHARMACEUTICS AND DRUG DELIVERY, RUTGERS UNIVERSITY

DR. SINKO: Members of the Commission, good morning and thank you for the opportunity to testify today.

This testimony represents my personal views and does not reflect the view of Rutgers, The State University of New Jersey.

The United States and China are two of the world leaders in nanotechnology R&D. To answer the question of how Chinese activities in nanotechnology compare to those of the United States and how they impact U.S. interests, this testimony will briefly describe the status of nanotechnology R&D in the U.S. and China, and then I will summarize and make some recommendations.

The National Nanotechnology Initiative, or NNI, coordinates the federal nanotechnology-related R&D activities and it has invested about $24 billion in nanotechnology R&D since 2001. The NNI has already made significant scientific and commercial impacts because of the R&D activities of about 1,200 companies, universities, and government labs that have introduced nanotechnology into about 750 products.

Since its peak in FY2010, NNI funding has gradually decreased, and in FY2018, it's projected to be the lowest since 2004.

Government funding, technical support, and regulation of nanotechnology in China comes primarily from the Ministry of Science and Technology, the Chinese Academy of Sciences, and the National Natural Science Foundation of China.

The Ministry of Science and Technology administers two key programs for disbursing R&D funding: the 86-3 program and the 97-3 program. The 86-3 program focuses on industrialization, while the 97-3 program focuses on basic science. This is an important distinction because most R&D disciplines are funded by one of these programs but not both, and nanotechnology is actually funded by both very uniquely in China.

The goal of China's major industrial science and technology R&D policy, the MLP, or Medium-to-Long-Term Plan, is to make China an innovation-oriented society by 2020. Nanotechnology with its promise of vast commercialization potential was among the megaprojects identified by the MLP to elevate the core competitiveness of China on the world stage.

Among the MLP's science mega-programs, only nanotechnology is supported by both the 86-3 and 97-3 programs, demonstrating the daunting breadth and complexity of inventing and commercializing nanotechnology products.

China has already met the MLP goal of moving itself into the top five countries with respect to the number of patents issued domestically and the number of international citations on their publications of scientific papers. It is on target to meet its second goal of increasing China's gross expenditures on R&D to at least 2.5 percent by the year 2020.

However, they are lagging significantly behind on their third goal, to strengthen China's innovative capacity and reduce their dependence on foreign technology. By its own analysis, China ranked 18th in the world in 2015 in innovative capacity, whereas the U.S. ranked first.

Formidable barriers exist between the R&D ecosystem and private industry in China, and as a result, they struggle with an immature venture funding market that discourages risk taking, a lack of firm intellectual property protection, and a deficiency of skillful and knowledgeable managers who understand not only technology but also the financial, legal, and other aspects of the tech transfer process. All this has led to an insufficient nanotechnology product pipeline and poor commercialization performance.

In summary, nanotechnology is a discipline that requires a strong parallel commitment to funding both basic research and commercial development. The U.S. dominance of the nanotechnology field since 2001 can be attributed directly to the firm federal commitment to NNI agencies and their R&D funding appropriations.

The U.S. must remain committed to supporting basic nanotechnology research. Otherwise new opportunities will not be discovered and commercial pipelines will dry up. Furthermore, an industry focused on tight development timelines and a short horizon for achieving acceptable return on investment will not likely have the patience for commercial nanotechnology product development and investment may suffer.

As a result, there's an urgent need for the federal government to reverse the trend of reducing its support of nanotechnology R&D. Further funding reductions coupled with China's continued increases in investment threaten the position of the U.S. as a world leader in nanotechnology.

It is important to note that nanotechnology is considered a dual-use technology, one that can be reasonably anticipated to provide knowledge, products or technologies that could be directly misapplied by others to pose a threat to public health, agriculture, plants, animals, the environment, and materiel.

Therefore, reductions in nano funding would not only lead to reduced global competitiveness in areas such as healthcare, science and technology, and other industries, but also could have serious implications on national defense as more than 60 countries have national nanotechnology development programs with their eye on dual-use technologies.

Therefore, I make the following recommendations:

First, the appropriations to NNI agencies should be restored to maintain the position of the United States as the global leader in nanotechnology R&D. Specifically, funding should be appropriated and priority given to basic nanotechnology research science programs. These programs require federal support since they're considered to be too early for industry, and also I recommend that the fractional allocation of the Small Business Innovation Research and Small Business Technology Transfer programs should be increased to further promote early stage commercialization and partnerships between academia and industry.

Second, I recommend that federally-funded programs to support university intellectual property development and technology transfer be established. The U.S. research universities do not have an adequate commitment to or sufficient funding for developing and protecting IP. In addition, the quality of most university-based technology transfer programs is lacking. In other words, the U.S. is leaving a lot on the table when it comes to IP.

Third, Chinese intellectual property activities and progress on IP enforcement should be closely monitored, and the Chinese patent organization, SIPO, activity, should be actively engaged and encouraged to comply with WTO standards to keep the playing field level.

Finally, the development of public-private partnerships should be expanded to the establishment of nanotechnology accelerator hubs across the country. Developing nanotechnology ecosystems with a critical mass of resources and distinct locations will not only spur R&D but will also ensure the retention of high-paying jobs in these centers across the United States.

Thank you.

PREPARED STATEMENT OF PATRICK J. SINKO
ASSOCIATE VICE PRESIDENT FOR RESEARCH AND DISTINGUISHED PROFESSOR OF PHARMACEUTICS AND DRUG DELIVERY, RUTGERS UNIVERSITY

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

This testimony was prepared by Patrick J. Sinko in his personal capacity. The opinions expressed are the author's own and do not reflect the view of Rutgers, The State University of New Jersey.

Nanotechnology is a transformative technology revolutionizing many areas including energy, defense, information technology, agriculture, environmental protection and healthcare. While there are more than 60 countries that have launched national nanotechnology programs, the United States and China are the two leading countries engaged in nanotechnology research and development (R&D). It is important to understand the current status, drivers of R&D and commercialization, and market opportunities for nanotechnology development in the United States and China. Nanobiotechnology, nanorobotics and nanoinformatics, three nanotechnology subsectors that range in maturity status from near commercialization to emerging, will have an important impact on advancements in the field. A comparison of publications, granted patents, ecosystems, government and company investment, policies and regulations, technology transfer and commercialization, and industrial enterprise growth in nanotechnology-related fields reveals some marked asymmetries between the United States and China.

In order to address these issues, the testimony will be organized as follows:

1. Status of nanotechnology R&D in the United States.
2. China's major industrial policies supporting the development of the nanotechnology sector.
3. China's investment in nanotechnology R&D.
4. China's successes and challenges in nanotechnology R&D.
5. Summary of key points and recommendations for congressional action.

1: Status of Nanotechnology R&D in the United States.

Typically any discussion regarding nanotechnology starts with defining a size range (1 to 100 nm), however, the importance and potential impact of nanotechnology relates to the distinctive material properties that begin to express themselves when bulk scale material is nanosized. Other physical properties such as shape, porosity and smoothness strongly influence the behavior of nanoscale materials. In addition to physical properties, the composition of the material and material properties also significantly impact behavior at the nanoscale. While nanotechnology Research and Development (R&D) focuses on developing novel products based on Engineered Nano Materials (ENMs) in areas such as diagnostics, therapeutics or even military/defense applications, the unique properties of nanotechnology-based products have introduced unexpected environmental and health and safety issues that will require consideration by scientists and regulators alike.

The National Nanotechnology Initiative (NNI) is a multi-agency program established in 2000 that coordinates federal nanotechnology-related Research and Development (R&D) activities and related budget and planning processes to advance the field of nanotechnology across the United States. The NNI, the world's first national nanotechnology program, is comprised of 20 federal departments and independent agencies and commissions that invest in nanotechnology R&D and provide oversight. The NNI is coordinated within the White House through the National Science and Technology Council (NSTC), a Cabinet-level council under the Office of Science and Technology Policy. The Nanoscale Science, Engineering, and Technology (NSET) subcommittee of the NSTC, which is composed of representatives from participating agencies, coordinates planning, budgeting, implementation and review.

The vision of the NNI is "a future in which the ability to understand and control matter at the nanoscale leads to a revolution in technology and industry that benefits society."[1] To realize its vision, the NNI has established four goals:

- advance a world-class nanotechnology R&D program;
- foster the transfer of new technologies into products for commercial and public benefit;
- develop and sustain educational resources, a skilled workforce, and a dynamic infrastructure and toolset to advance nanotechnology; and
- support responsible development of nanotechnology.[1]

The NNI does not have centralized funding; rather, funding is provided directly through collaborative efforts by NNI member agencies that include the National Science Foundation (NSF), National Institute of Health (DHHS/NIH), Department of Energy (DOE), Department of Defense (DOD), and National Institute of Standards and Technology (NIST). Each agency allocates its nanotechnology R&D budget into categories of investment called Program Component Areas (PCAs) based on its needs and interests.

[1] Subcommittee on Nanoscale Science, Engineering, and Technology, National Science and Technology Council Committee on Technology. National Nanotechnology Initiative Strategic Plan. (2016).

The five PCAs are: (1) nanotechnology signature initiatives (NSIs); (2) foundational research; (3) nanotechnology-enabled applications, devices, and systems; (4) research infrastructure and instrumentation; and (5) environment, health, and safety. The NSIs are designed to focus on areas of national priority through interagency coordination and collaboration to facilitate faster translation from basic research activities to commercial applications. Current NSI priority areas include sustainable nanomanufacturing, nanoelectronics, nanotechnology knowledge infrastructure (NKI); sensors, and water sustainability.

The NNI has invested approximately $24 billion in nanotechnology R&D since 2001. Plotted in **Figure 1** is the inflation-adjusted total funding appropriation to the NNI since its inception. NNI funding by Congress gradually increased from FY2001 and reached its peak of $1.9 billion in FY2010. However, after the Department of Defense drastically reduced their investment (by $256 million) in FY2013, total NNI funding has not exceeded $1.5 billion. For FY2017, the Federal budget provides approximately $1.443 billion for nanotechnology R&D, which is 25% less than NNI funding for FY2010.[2] Under President Trump's FY2018 budget proposal, the spending on basic science would shrink by an additional 10.5%.[3] If a 10.5% reduction occurs, the inflation-adjusted NNI appropriation would be the lowest since 2004.

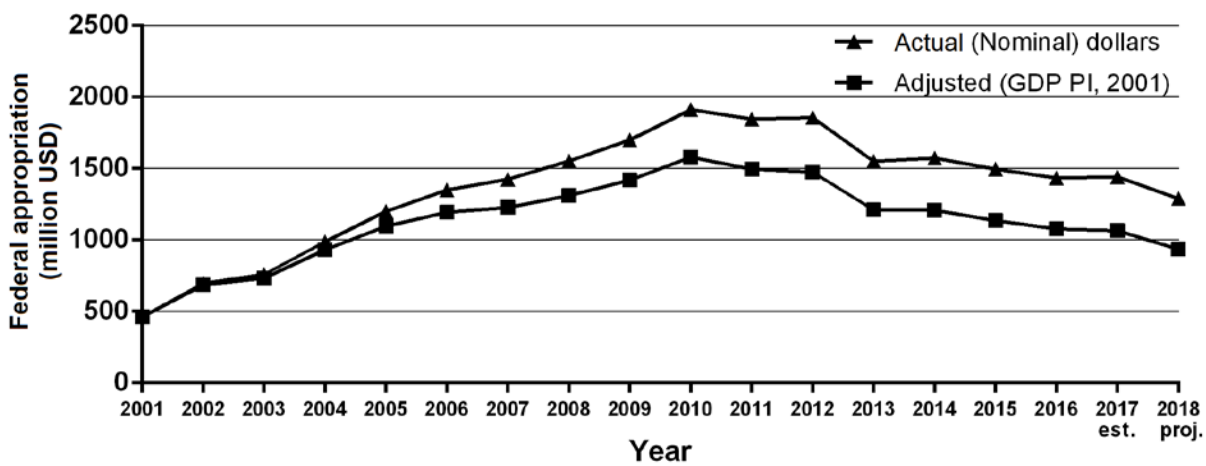


Figure 1. NNI funding, FY2001-18. Appropriations were inflation-adjusted to 2001 dollars to demonstrate real purchasing power. The GDP price index was used to make the adjustment. 2009 figures do not include American

The NNI has already made significant scientific and commercial impact thanks to the R&D activities of ~1200 companies, universities and government laboratories that have introduced nanotechnology into

[2] Subcommittee on Nanoscale Science, Engineering, and Technology, National Science and Technology Council Committee on Technology. The National Nanotechnology Initiative Supplement to the President's Budget for Fiscal Year 2017. (2016).
[3] Malakoff, D. *Trump's 2018 budget will squeeze civilian science agencies*, <http://www.sciencemag.org/news/2017/02/trump-s-2018-budget-will-squeeze-civilian-science-agencies> (2017).

about 750 products. For example, scientists funded by the DOE's Office of Energy Efficiency and Renewable Energy Vehicle Technologies Program invented a new lithium-ion battery technology that incorporates integrated electrode structures at the nanoscale, thereby improving battery energy and efficiency.[4] Single-cell biology was a new area when the NNI was launched, but now it is "one of the most rapidly evolving assay biotechnologies."[5] Development of nanoscale sensors will also enable healthcare providers to detect and treat diseases at the molecular level. The NNI provides public access to the long list of achievements in nanotechnology online.[6]

Moving forward, the NNI has expanded its focus from investments in fundamental research to technology transfer that can promote the commercialization of nanotechnology-enabled products. For foundational research, the NNI continues to invest in the five NSIs. In 2016, a new NSI, *Water Sustainability through Nanotechnology: Nanoscale Solutions for a Global-Scale Challenge*, was launched to ensure water quality and supply.[1] To encourage the transfer of nanotechnology inventions from the laboratory to the commercial marketplace, NNI agencies sponsor a number of programs to drive the process. In 2016, the Nano Startup Challenge in Cancer (NSC^2) was introduced. The NSC^2 is a partnership among multiple government institutes and companies that used crowdsourcing to recruit talent across the country and around the world to foster the commercialization of cancer nanotechnology inventions.[7] Another example of public-private partnership is the Nano-Bio Manufacturing Consortium (NBMC) supported by the Air Force Research Laboratory. The NBMC has the goal of creating an industrial nano-bio ecosystem of suppliers, integrators, and end-users.[1]

The merging of multiple technologies into more complex systems has led to a variety of nanotechnology subfields. Three important areas of US nanotechnology development, nanobiotechnology, nanorobotics and nanoinformatics, where the US is the world leader will be highlighted to illustrate the convergence of technologies with nanotechnology and their implications. On the one hand, nanobiotechnology is the most mature of the three subfields that will be highlighted and, as such, there is an increased emphasis on translation and commercialization. Nanoinformatics, on the other hand, is an emerging field of great importance that will play a critical future role in nanotechnology opportunity and threat assessment.

Nanobiotechnology

---

[4] National Nanotechnology Initiative. *Improving Our Energy Resources for Today and Tomorrow: Nanotechnology-Enabled Energy Solutions*, <https://www.nano.gov/node/1497>

[5] Heath, J. R. Nanotechnologies for biomedical science and translational medicine. *Proc Natl Acad Sci U S A* **112**, 14436-14443, doi:10.1073/pnas.1515202112 (2015).

[6] National Nanotechnology Initiative. *What are National Nanotechnology Initiative accomplishments?*, <https://www.nano.gov/node/1497>

[7] Truman, R. & Locke, C. J. Gazelles, unicorns, and dragons battle cancer through the Nanotechnology Startup Challenge. *Cancer Nanotechnol* **7**, 4, doi:10.1186/s12645-016-0017-6 (2016).

In his book, Ehud Gazit defines nanobiotechnology as the “applications of nanotechnology techniques for the development and improvement of biotechnological process and products.”[8] The convergence of two different fields—biotechnology and nanotechnology—has inspired many investigators due to its potential for innovation and as a result, this fairly new field has expanded rapidly over the past two decades. Nanobiotechnology includes many scientific disciplines such as biopharmaceuticals, drug delivery, diagnostics and certain areas of specialty instrumentation. One area in which nanobiotechnology has the greatest potential for changing current paradigms is therapeutics, especially precision medicine. “Precision Medicine refers to the tailoring of medical treatment to the individual characteristics of each patient. It does not literally mean the creation of drugs or medical devices that are unique to a patient, but rather the ability to classify individuals into subpopulations that differ in their susceptibility to a particular disease, in the biology and/or prognosis of those diseases they may develop, or in their response to a specific treatment. Preventive or therapeutic interventions can then be concentrated on those who will benefit, sparing expense and side effects for those who will not.”[9] Rather than a “one-size-fits-all” approach, nanobiotechnology will allow the use of nanoscale techniques to develop more accurate diagnoses and more precise targeting, leading to effective treatments tailored to subpopulations of patients.

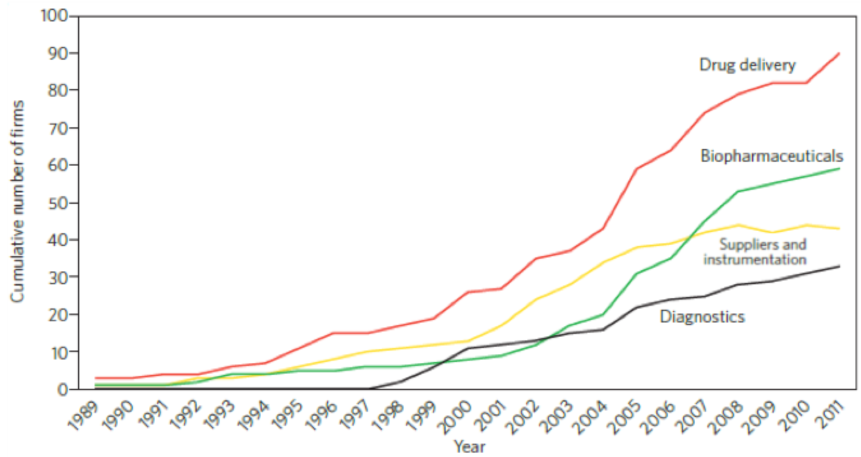


Figure 2. Cumulative number of companies in the US developing products in the four primary nanobiotechnology subsectors. (Reproduced from reference 10)

Nanobiotechnology is one of the more well-established nanotechnology subfields as a result of years of laboratory research and investment in universities and research institutes and by companies. Doxil®, one of the first successfully translated nano products that was approved by the FDA in 1995, encouraged the growth of new companies entering the bionanotechnology sector (**Figure 2**). Even though the suppliers and instrumentation subsector reached a plateau after years of rapid growth, the other subfields continued to increase, with the growth in the number of drug delivery startups being impressive. Interestingly, the plateau in the suppliers and instrumentation subsector was attributed to the emergence of a “dominant design”— in other words, a standard set of product features or technological attributes

[8] Gazit, E. *Plenty Of Room For Biology At The Bottom: An Introduction To Bionanotechnology*. (Imperial College Press, 2007).
[9] National Research Council (US) Committee on A Framework for Developing a New Taxonomy of Disease. *Toward Precision Medicine: Building a Knowledge Network for Biomedical Research and a New Taxonomy of Disease*. (National Academies Press (US), 2011).

that becomes expected by the marketplace (for example, processes for nanoparticle synthesis)—resulting in a consolidation of firms in the industry.[10] At this stage of maturity, firms will refine their process attributes, such as cost reduction, and the market will start adopting the technology. Unfortunately, the translation of laboratory research in the nanobiotechnology sector to commercial products has been lackluster. As noted by numerous commentaries and articles, the timeframe for nanotechnology R&D has been much longer than originally expected reflecting two important nuances about nanobionanotechnology R&D. First, the research component has a much longer time horizon due to a general lack of a scientific foundation at the molecular scale. In addition, many unexpected phenomena have highlighted numerous potential environmental and health and safety issues. These potential issues have attracted significant attention by regulators, which further slows the introduction of nanobiotechnology products to market. While it is clear that the US is the world leader in nanobiotechnology R&D with approximately 60% of the companies[10] and the largest investment of any country in this sector[11], it is also clear that sustained investment in research is still required.

Nanorobotics

Micro/nanorobotics represent the next logical step forward after nanobiotechnology and is the result of the convergence of traditional robotics and nanotechnology. These small-scale robots function much like larger robots of today. Micro/nanorobots have been designed for targeted drug delivery, precision surgery, sensing, and detoxification.[12,13,14,15,16] They can move (locomotion), require an energy source for the "motor", have moving parts that can assist in surgery or take biopsy samples, etc. However, the challenges of miniaturization are numerous. For example, in order to move through blood vessels the robots can't be larger than a red blood cell (RBC), which moves freely through vessels. A RBC is about 6-8 microns in size. However, to move into tissues or tumors, the robot will likely have to be in the nanometer size range. At this size, regular molecular motions that occur (e.g., Brownian motion) will have a major influence on the locomotion of the nanorobot. As one paper recently concluded "Moving nanorobots from test tubes to living organisms would require significant future efforts. ... Operating these tiny devices in human tissues and organs that impose larger barriers to motion [than blood] requires careful examination."[12] From the perspective of the energy required for motion and the penetration into tissues it is clear that "smaller is better" and this is where the role of nanotechnology becomes clear. As such, significant technological developments will be required in the fields of nanotechnology and materials science. Although interest in micro/nanorobotics has grown significantly over the past decade the field is still in its infancy. Numerous significant challenges exist and translate

[10] Maine, E., Thomas, V. J., Bliemel, M., Murira, A. & Utterback, J. The emergence of the nanobiotechnology industry. *Nat Nanotechnol* **9**, 2-5, doi:10.1038/nnano.2013.288 (2014).
[11] OECD website. (2017).
[12] Li, J., Esteban-Fernández de Ávila, B., Gao, W., Zhang, L. & Wang, J. Micro/nanorobots for biomedicine: Delivery, surgery, sensing, and detoxification. *Science Robotics* **2** (2017).
[13] Chin, S. Y. *et al.* Additive manufacturing of hydrogel-based materials for next-generation implantable medical devices. *Science Robotics* **2** (2017).
[14] Kagan, D. *et al.* Functionalized Micromachines for Selective and Rapid Isolation of Nucleic Acid Targets from Complex Samples. *Nano Letters* **11**, 2083-2087, doi:10.1021/nl2005687 (2011).
[15] Hu, C.-M. J., Fang, R. H., Copp, J., Luk, B. T. & Zhang, L. A biomimetic nanosponge that absorbs pore-forming toxins. *Nature nanotechnology* **8**, 336-340, doi:10.1038/nnano.2013.54 (2013).
[16] Saadeh, Y. & Vyas, D. Nanorobotic Applications in Medicine: Current Proposals and Designs. *Am J Robot Surg* **1**, 4-11, doi:10.1166/ajrs.2014.1010 (2014).

into limited short-term potential for addressing healthcare issues. However, given the potential significance of micro/nanorobotics it is expected to become a vigorous area of research in nanotechnology in the future.

Nanoinformatics: Big Data, Artificial Intelligence and High Performance Computing.
"As multiple technology domains converge into more sophisticated systems, they link not only the benefits of those disparate technologies but also their risks."[17] Big Data, artificial intelligence and high performance computing are three emerging technologies that will play an important role in assessing potential opportunities and threats of nanotechnology products. Big Data generally refers to the handling and processing of large and/or complex data sets while artificial intelligence uses the data as well as pattern recognition and computational learning to generate new knowledge. High performance computing is required to accomplish these complex analyses. In fields like biotechnology, these approaches have already allowed "for leveraging research investments across multiple initiatives, facilitating trans-disciplinary translation of information, accelerating scientific discovery, and enabling faster risk assessment and commercialization of new technologies."[18] Similarly, large and complex data sets are inherent to the field of nanotechnology due to the wide variety of potential physicochemical properties as well as methods for fabricating, characterizing and evaluating nanomaterials. "This has led to diverse and rapidly emerging data in terms of materials, their interactions in environments, and across a broad spectrum of potentially relevant biological interactions."[18] For example, nanomaterials and their properties can be radically transformed upon release to the environment or exposure to the body. In other words, nanomaterials are highly dynamic in nature and there is an urgent need to understand, predict and control these changes. These profound and dynamic changes have significant implications on the potential efficacy, safety and toxicity of nanotechnology derived products in biomedical applications, environmental health and safety as well on national security and defense applications. To better understand nanomaterial behavior, the Nanoinformatics 2020 Roadmap was proposed and recently expanded: **"**Nanoinformatics is the science and practice of determining which information is relevant to meeting the objectives of the nanoscale science and engineering community, and then developing and implementing effective mechanisms for collecting, validating, storing, sharing, analyzing, modeling, and applying the information, and then confirming that appropriate decisions were made and that desired mission outcomes were achieved[…]."[18] In the future, nanoinformatics will be the primary tool for assessing the risks of applying nanotechnology as well as its potential benefits as well.

2: China's Major Industrial Policies Supporting the Development of the Nanotechnology Sector

In 1956, China established the Science Planning Commission consisting of more than 600 science and technology (S&T) experts to develop the first National Science and Technology Long-Term Plan (1956-1967) (the 12-year plan). The 12-year plan is credited with establishing the foundation for modern

[17] Hull, M. National Security and the Nano Factor. *HDIAC Journal*, 16-21 (2017).
[18] Hendren, C. O., Powers, C. M., Hoover, M. D. & Harper, S. L. The Nanomaterial Data Curation Initiative: A collaborative approach to assessing, evaluating, and advancing the state of the field. *Beilstein J Nanotechnol* **6**, 1752-1762, doi:10.3762/bjnano.6.179 (2015).

science and technology in China and had notable achievements including the development of China's nuclear weapons and space programs.[19] In the 12-year plan, the central government identified priority projects and provided resources to fund programs in those project areas.

In 2000, the National Steering Committee for Nanotechnology Development was established, which formally organized nanotechnology efforts at the national level. They were responsible for planning, coordination and providing advice on nanotechnology development. The committee was composed of scientists from universities, institutes and industry as well as administrators from the Chinese Academy of Sciences (CAS), Ministry of Science and Technology (MOST) and other government organizations.

Medium- to Long-Term Plan for the Development of Science and Technology (2006-2020) (MLP)
Modeled after the 12-year plan, China initiated the MLP in 2006. It became "increasingly obvious to [Chinese leaders] that those who own the intellectual property, and who control technical standards, enjoy privileged positions in, and profit most from, international production networks."[19] Therefore, the objective of the MLP was to make China an innovation oriented society by 2020. The MLP identified eleven priority S&T areas relating to national needs such as national defense and manufacturing. The MLP also identified eight areas of enabling technologies (referred to as "Frontier Technologies") and a series of priority projects in each area. Some examples of Frontier Technology areas included advanced manufacturing, biotechnology and new materials. The MLP calls for an expansion of basic research (i.e., developing new interdisciplinary areas as well as new disciplines) and identified 17 national megaprojects. The megaprojects are considered critical S&T project areas for elevating the core competitiveness of China on the world stage. They have involved substantial government investments and incentives for key technology and engineering projects with commercial applications.[20] Thirteen engineering megaprojects including prevention and treatment of major diseases such as HIV/AIDS and drug innovation and development and four science megaprojects including the development of nanotechnology were identified. Priority areas in nanoscience included research focused on nanotechnology in the fields of energy, the environment, information, and medicine.

As discussed in detail by Cao et al, the MLP addressed four critical problems in China's S&T development: (1) its record of innovation in commercial technology was weak, (2) the state of its technological capabilities failed to meet the nation's social needs, (3) its overall capability for defense-related technological innovation was less than impressive and (4) the state of science in China did not live up to expectations given the investments that were made.[19] Specific objectives of the MLP were to:

- Increase China's gross expenditures on R&D (GERD) to 2.5% or above of the gross domestic product (GDP);
- Strengthen domestic innovative capacity and reduce the dependence on foreign technology (to 30% or less); and

---

[19] Cao, C., Suttmeier, R. P. & Simon, D. F. China's 15 year science and technology plan. *Physics Today* **59**, 38-43 (2006).
[20] Springut, M., Schlaikjer, S. & Chen, D. China's Program for Science and Technology Modernization: Implications for American Competitiveness. (2011).

- Move China into the top five countries with respect to the number of patents issued annually to Chinese nationals and number of international citations of scientific papers.

Chinese government funding, technical support and regulation of nanotechnology comes primarily from the Ministry of Science and Technology, Chinese Academy of Sciences and the National Natural Science Foundation of China.

The Ministry of Science and Technology (MOST) - The Ministry of Science and Technology is responsible for determining China's science and technology (S&T) development priorities, establishing strategies, administering S&T programs, developing regulations and managing international relationships. In 2013, much of the expenditures were S&T program related with funded projects receiving about $4.5 billion USD.[21] "MOST funds approximately 15% of [China's] national S&T expenditures."[21] The two primary programs for disbursing R&D funding are the 863 and 973 programs.

The National High-Technology Research and Development Program (the 863 program)
The 863 program focused on industrialization. The goals of the 863 program were to boost China's high tech development, R&D capacity, socio-economic development, and national security. The 863 program can fund academic institutions, research institutes and domestic companies.

The National Key Basic Research and Development Program (the 973 program)
The 973 program focuses on basic science. Among the goals of the 973 program are to strengthen and support research on many major scientific issues concerning national socio-economic development including nanotechnology. Other important aspects of the 973 program deal with attracting, cultivating, and retaining highly qualified scientists, promoting international exchange and cooperation, and attracting high caliber individuals from overseas. The 973 program utilizes a 2/3 funding model whereby a decision is made for continued funding or to adjust priorities and funding level after the second year of a project is completed.

Among the MLP's science mega-programs, only the nanotechnology mega-program is supported by the funding mechanisms of both the 863 and 973 programs, further demonstrating the daunting breadth and complexity of inventing and commercializing nanotechnology-based products.

The National Natural Science Foundation of China (NSFC)
The NSFC is responsible for providing funding for fundamental basic research using the Chinese National S&T Guiding Principles. Applied research projects can also be funded especially if the project originates from a funded basic research project. Since the implementation of the MLP, the central government allocation to the NSFC has increased about 20% per year for the past ten years. Unlike other programs, the NSFC funds investigator-initiated (i.e., bottom-up) projects as well as strategy-driven (i.e., top-down) projects that emerge from established national priorities and needs.[21] About 45%

[21] McCuaig-Johnston, M. & Zhang, M. China embarks on major changes in science and technology. (University of Ottawa, 2015).

of NSFC funding was in life sciences and health projects in 2013.[22] As a funding agency, the NSFC, which directly reports to the State Council, has broader reach since it also funds scientists who are not competitive for the 863 or 973 programs. The success rate of NSFC grant applications is about 25%, which is higher than the US National Institutes of Health average rate (18.3%) across all institutes and centers in FY2015.[23]

Chinese Academy of Sciences (CAS)

The CAS has played a key role in Chinese research since 1949. "CAS is headquartered in Beijing and comprises 104 research institutes, 12 branch academies, two universities and 11 supporting organizations in 23 provincial-level areas throughout the country. It both funds and performs research. [The CAS employs] 60,000 people across all of its institutes and universities, and [it had] a budget of $6.8 billion [USD in 2013]."[21] The CAS provides experts for the selection committees of the 863 and 973 programs.

Recruiting Leading Academics and Overseas Talent

China recognized early on that there was a significant problem with the state of science in their country especially due to "brain drain."[19] To make up for this deficiency and revitalize the state of science in China, it made active efforts in training and recruiting back highly qualified human resources. Two of its most important efforts in this area are the Hundred Talents Program and the Thousand Talents Program. The Hundred Talents Program began in 1994 with the goal of attracting 100 outstanding scholars from within and outside of China by the year 2000. Over the years, the program recruited and cultivated over 2000 outstanding scientists.[21] In 2015, the program was redefined to support the recruitment of three specific categories of talents: academic director, engineering director, and young talents.[24] The Thousand Talents Program started in 2008 to attract overseas Chinese and top university talent from globally ranked universities. To date the program has attracted over 4200 people.

3: Current Status of China's Investment in Nanotechnology R&D.

Financial Support Provided to Chinese Companies, Institutes and Universities

R&D Intensity (RDI), a commonly used indicator of an economy's relative degree of investment in generating new knowledge, is calculated from R&D expenditures as a percentage of GDP according to the Organisation for Economic Co-operation and Development (OECD). From 1998 to 2005 China's RDI nearly doubled to 1.34%.[19] In 2015, China's RDI was 2.07%.[11] By comparison, the United States' RDI was 2.79% in 2015. An important aspect of the MLP is its reliance on the business sector. To reach the 2.5% target China will rely heavily on private industry R&D investing since government expenditures represent only 21.6% of overall R&D expenditures.[21] Projecting the current trend in China's investment in Gross Domestic Spending on R&D through 2020 (**Figure 3**) it appears that China may reach their RDI goal of exceeding 2.5% per year by 2020. However, many challenges remain that

[22] NSFC. 2013 Annual Report, Part V: Statistics of NSFC's financial allocations and funding in 2013. (2013).
[23] NIH.
[24] University of Science and Technology of China. *Hundred Talents Program of Chinese Academy of Science - Young Talents,* <http://employment.ustc.edu.cn/cn/enindexnews.aspx?infoID=665597895156250032>

could impede the growth of the business sector investment such as the barriers between the R&D system and industry created by the less than optimal Intellectual Property Right (IPR) system and the inefficiencies of an immature technology transfer infrastructure remain. In addition, high technology research areas like nanotechnology that rely heavily on developments in the basic sciences may lag behind. This is a result of "China's emphasis on applied and product-development research[, which] means that funding for basic science remains low: only 5% of the country's total R&D [in 2014] is devoted to this, compared with 15–20% in other major OECD nations."[25]

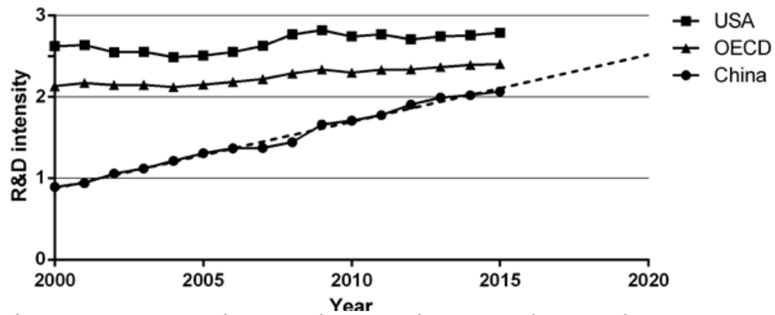


Figure 3. R&D intensity % (gross domestic spending on R&D as a % of GDP) for China, the United States, and OECD average, 2000-2015.

In general, financial support for nanotechnology R&D in China comes from a variety of sources including the Central, provincial and local/city governments as well private industry and venture funds. In addition, companies benefit from incubators/accelerators, which in some cases are massive operations with all of the elements required for a nanotechnology ecosystem. This is particularly needed in China today as challenges with technology transfer and translation have been noted. For Universities and Research Institutes, nanotechnology funding for research is available from all of the programs and agencies previously described (i.e., MLP, MOST, 973, 863, NSFC and CAS). Funding for nanotechnology research in the US has been at or greater than $1 billion USD since 2004. Recent trends (i.e., since 2010) have demonstrated a steady and significant decline in US government funding of nanotechnology-related research funding (**Figure 1**). China, on the other hand, has seen dramatic increases in NSFC nanotechnology funding from $90 million USD in 2004 to about $600 million in 2014.[26] In 2012, US total spending (i.e., corporate and government) totaled approximately $2.2 billion USD whereas China's total was ~$1.3 billion USD.[26,27]

China's Innovative Capacity

The Chinese National Innovation index was developed by China in 2006 to track its progress in innovation by comparing itself to the top 40 countries that represent 98% of total global expenditures on R&D. The innovation index uses data from several sources among them the MOST, OECD, World Bank, World Intellectual Property Organization, World Economic Forum and others. The index is comprised of 30 qualitative and quantitative indicators in five groups (innovation resources, knowledge

[25] Van Noorden, R. China tops Europe in R&D intensity. *Nature* **505**, 144-145, doi:10.1038/505144a (2014).
[26] Gao, Y. *et al.* China and the United States--Global partners, competitors and collaborators in nanotechnology development. *Nanomedicine* **12**, 13-19, doi:10.1016/j.nano.2015.09.007 (2016).
[27] Strange, K. L. & Baucher, M. A. in *OECD/NNI International Symposium on Assessing the Economic Impact of Nanotechnology* (Washington, DC, USA, 2012).

creation, enterprise innovation, innovation performance and innovation environment). The National Innovation Index Report 2015 was issued by the Chinese Academy of Science and Technology for Development (CASTED) on 29 June 2016. The top 10 in the ranking of the year were the US, Japan, Switzerland, South Korea, Denmark, Germany, Sweden, the UK, the Netherlands, and Singapore. China was ranked 18th in 2015, moving up one place from the previous year. In terms of the five main indicators that contributed to the overall ranking, China saw improvement from the previous year in innovation resources, knowledge creation, and enterprise innovation, whereas its innovation performance remained steady and innovation environment slipped compared with the previous year. According to the report, the weaker performance in the innovation environment reflected the need to improve the accessibility of venture capital for enterprise innovation and IP protection relative to the increased demand for both because of the growing recognition of the importance of IP in China. In 2015, the State Council formally recognized innovation and entrepreneurship as critical for achieving economic development. In addition China intends to relax rules applying to foreigners with technical talent seeking permanent residency or even citizenship in China, allow Chinese researchers to participate in projects outside of China, implement stronger IP protections, and increase market competition to boost innovation.[21] China's entrepreneurship base has a solid foundation in the 115 university science parks and 1,600 technology incubators/accelerators. Leveraging these infrastructure investments and resources are critical to China's advances in entrepreneurship. However, other issues such as the ability of companies in the market to truly compete independent of the influence of the State and partner with foreign companies in fair IP arrangements will have a great influence on their success.

4: China's Successes and Challenges in Nanotechnology R&D

China has made considerable investments in nanotechnology R&D since 2000. Substantial successes were achieved during this period in the number of patents issued to Chinese inventors, the number of publications and related citations and the creation of dedicated nanotechnology science parks.[28] These successes help to build a foundation for innovation. However, China has had difficulties in translating innovation into commercialization. In the sections that follow, China's successes and challenges in nanotechnology R&D are discussed.

Successes:
<u>*Patents issued*</u>

[28] Cao, C., Appelbaum, R. P. & Parker, R. "Research is high and the market is far away": Commercialization of nanotechnology in China. *Technology in Society* **35**, 55-64, doi:10.1016/j.techsoc.2013.03.004 (2013).

An important metric of innovation identified in the MLP was the number of Chinese patents issued to Chinese nationals annually. In 2008, 64% percent of nanotechnology patent applications to the US Patent and Trademark Office (PTO) were from American inventors.[26] However, Chinese innovators have been prolific in applying for and receiving domestic patents (i.e., in China). While overall applications to the State Intellectual Property Office (SIPO) of China were slightly less than applications to the US PTO in 2008 (18,438 versus 19,665), Chinese inventors represented ~89% of the applicants. US inventors ranked second with 4.4% of the total applicants to SIPO. In fact, in 2012 Chinese domestic resident patents accounted for 22.3% of the total number of patents submitted worldwide, which was second only to Japan.[21] The trend is similar even when the scope of the search is narrowed to micro- and nanotechnology patents. From 2011 to 2015, China ranked first in patent grants with 23.3% of the total patents granted worldwide.[29] Only 4% of 3460 patents were granted from patent offices outside China, whereas more than 57% of US patents were granted abroad (**Figure 4**). Most nanotechnology patent applications in the US are from the industrial sector whereas in China the clear majority is from academia.[26] The focus of China's patents strategy is clearly domestically focused with only ~5% filed with patent offices outside of China.[21] This is low when compared to the US where over 50% of domestic patent applications are filed internationally. The large number of patent applications as well as issued patents in China raises questions about patent strategy and breadth of coverage. As a result, it has been suggested that many of those patents are not used (i.e., licensed), which potentially limits their value and impact on China's economy.[25]

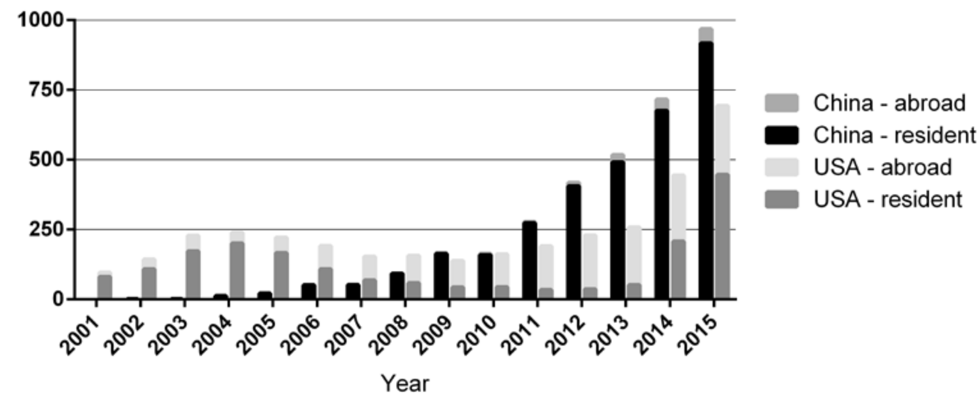


Figure 4. Resident and abroad counts of patent grants in micro- and nanotechnology in China and the United States, 2001-15 (Source: reference 29)

International citations of scientific papers

Between 2004 and 2014, China ranked second in the world in total number of science and technology publications and fourth in the rate of citations.[21] In addition, from 2001 to 2011 the increase in publication rate was steady at ~15% annually. While the increase in total publications has been impressive, gains in the citation rate for S&T papers have also been impressive. From 2004 to 2013 China produced 5.2% of the world's highly cited papers ranking fourth according to the Chinese National Innovation Index (2013).[21] The Chinese NII defines "highly cited" as papers that are in the top

[29] WIPO. (2017).

1% of their fields with respect to citations. The US ranked first with nearly 40% of the highly-cited papers.[21] The NSF reported that the fraction of highly cited papers by China, as of 2012, was 37% lower than expected given their productivity.[21] In terms of nanotechnology papers, similar trends were observed. The annual publication totals during the period of 2001 to 2014 were collected using the Thomson Science Citation Index's (SCI) Web of Science database using the search term "nano* NOT nanomolar" to show the recent publication patterns of the two countries.[26] Both China and the US demonstrated steady growth in nanotechnology publications over the 14-year period that was analyzed. While China lagged behind the US from 2001 to 2009, it surpassed the US in 2011. In terms of bionanotechnology papers relating to cancer, China surpassed the US in 2013. However, as we noted in our analysis "there is a severe mismatch between China's high publication productivity and low citation numbers."[26,30] Like the analysis of patent trends, the recent higher Chinese publication rate (i.e., quantity) did not correlate linearly with citation rate (i.e., a measure of quality). It is also interesting to note that while China generally is much weaker than the US in nano-bio, in cancer bionanotechnology (a relatively small field) the countries are closer to parity depending on the metric used for evaluation. This is likely the result of cooperativity agreements between China and US. The application of nanotechnology to cancer research has proven to be an interesting case study and promising area for China–USA collaboration.[31] Joint support for cancer nanotechnology research by the NIH and NSFC started in 2010 and continues today. There is a solid trend of co-authorship between US and China authors in this area demonstrating the complementary interests and opportunities for cooperation in otherwise competitive research areas. The US–China Symposium on Nanobiology and Nanomedicine has been held every two years since 2008 and provides a unique opportunity for experienced scientists to exchange ideas and establish new collaborations. It helps to increase US–China cancer bionanotechnology partnerships including promoting new programs for reciprocal training and exchange, co-sponsoring workshops focused on specific cancer bionanotechnology topics of high priority to both countries, and joint financial assistance of collaborative research projects by Chinese and US funders.

Creation of dedicated nanotechnology science parks: Ecosystems for Nanotech Development

The government has played a central role in the development of nanotechnology in China. They've created policies, provided funding for R&D, infrastructure development and capacity building and importantly, they are a key source of venture funding.[28] Local (i.e., city) governments also have a history of supporting the field by building and supporting nanotechnology development centers in China. Included in these cities are Shanghai (Shanghai Nanotechnology Promotion Center), Tianjin (Nanotechnology Industrial Base of China), and Suzhou (China International Nanotech Innovation Cluster or CHINANO). Suzhou stands out among these centers because of its outstanding track record in manufacturing, its strong support of innovation and the funding invested. For example, Suzhou Innovation Park (SIP) launched the Nanopolis Suzhou initiative and committed $1.6 billion (USD) over a five-year period. The goals of Nanopolis are to not only develop companies but also to provide a nanotech ecosystem. Nanopolis provides technology incubation, R&D, and pilot production. The

[30] Lenoir, T. & Herron, P. Tracking the current rise of chinese pharmaceutical bionanotechnology. *J Biomed Discov Collab* **4**, 8 (2009).
[31] Schneider, J. A., Grodzinski, P. & Liang, X. J. Cancer nanotechnology research in the United States and China: cooperation to promote innovation. *Wiley Interdiscip Rev Nanomed Nanobiotechnol* **3**, 441-448, doi:10.1002/wnan.149 (2011).

initiative is focused on nanotech commercialization with an emphasis on micro- and nano-manufacturing technologies, energy and green technologies and nanomedicine. The investment in nanomedicine is particularly noteworthy given the significant strength of the US in nanobio and the need not only for development but, importantly, research in this area. A combination of incentives and support is provided by the Suzhou government and SIP including housing and manpower subsidies and tax reductions. Nanopolis Suzhou has IP development and protection services as well. Over an approximate 20-year period, Suzhou has had over 20,000 national and multinational company sponsors, has over 170 startups and more than 150 investment companies in SIP. For nanotechnology specifically, there are more than 20 investment companies focusing on nanotech incubation. In addition to Nanopolis, SIP initiated the State University Science Park for Nanotech, which is focused on developing research institutes and joint education programs for tech transfer and commercialization. Finally, bioBay was established by SIP in 2007 to develop the emerging biological industry focusing on bio and bionanotechnology. bioBay offers numerous services including IP services free-of-charge to the companies that they incubate. These services include residential housing, business rental and manpower subsidies, access to the nanotech characterization and fabrication facilities and they are eligible for start-up funding. Funding for bioBay is provided by the city government (Suzhou), the provincial government (Jiangsu), the State (MOST) and a variety of venture funds. The Chinese Academy of Sciences selected bioBay as the site for its Suzhou Institute of Nano-Tech and Nano-Bionics (SINANO). SINANO is a joint venture between the CAS, Jiangsu, Suzhou and SIP. Entrepreneurs selected for the program receive as much as $1.5 million USD but half of it is public investment. The downside to this funding model is that the company loses its financial independence.

Challenges:

Cao et al[28] eloquently described the formidable barriers that exist in China between the R&D ecosystem and private industry that result in a translation/commercialization pathway that does not function well. These barriers include: "(1) An environment that lacks rigid intellectual property right (IPR) protection making technology transfer difficult, if not impossible; (2) an immature venture capital market that discourages risk taking; and (3) the dearth of skillful and knowledgeable managers who understand not only technology but also financial, legal and other aspects of the technology transfer process."[28] There are also nanotechnology specific commercialization issues as well including special considerations regarding the environment and safety and the enormous investment required and time horizon for successfully introducing a nanotechnology-based product to the market. The coordination between scientists and engineers (both on the academic and industrial sides of the equation) and entrepreneurs is of critical importance to successfully transferring technology in a way that promotes commercialization. Finally, the entire "nano" field has been the subject of considerable hype – not just in China but worldwide. This combined with the fact that transformative results are scarce has cast a shadow on investment flow from the private sector. Furthermore, government funding agencies struggle with awarding long-term grants and have instituted a proof-of-concept requirement in the early stages of a project. Given the very long-term commercial prospects and investment heavy requirements of nanotechnology development, it is unrealistic to push for absolute early stage proof-of-concept using a commercialization standard rather than a scientific standard.

Research specialization areas in nanotechnology

In a recent analysis on research diversification and its impact in nanotechnology, Herron at al[32] demonstrated that Chinese nanoscientists were predominantly focused (i.e., specialized) in the areas of thin films and nanoparticles/self-assembly. In the US and EU, the areas of specialization are bio (i.e., nanomedicine and nanobiotechnology) and electronics (i.e., nanoelectronics and nanoptoelectronics). The publishing trends are shown in **Figure 5**. The Revealed Literature Advantage (RLA) for the US in bio is extremely high, which shows a very significant focus in nanomedicine and nanobiotechnology. The authors concluded that while the US is opening up new frontiers in nanobio and electronics other countries such as China are following but with a considerable lag. They go on to state "we interpret this as a reflection of a process of scientific catch-up, with the Newcomers [such as China] attempting to diversify by making up ground in areas such as nanobio, and the US and EU attempting to maintain a competitive edge in nanobio and electronics—two areas in which their industries have been investing heavily".

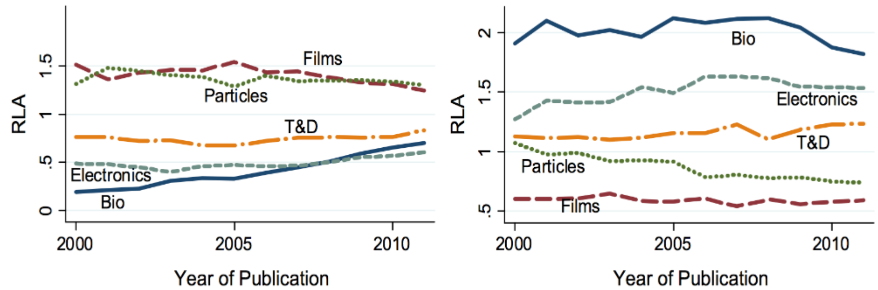


Figure 5. A plot of the Revealed Literature Advantage (RLA) versus year for China (left) and the US (right). The RLA is basically a ratio of a country's publications in a nanotechnology subfield to its total publications in nanotechnology. When the RLA is greater than 1, a country is considered to specialize in a subfield. From the data it can be seen that China is specializing in films and nanoparticles while the US is specializing in bio (nanomedicine and nanobiotechnology), electronics (nanoelectronics and nanoptoelectronics) and T&D (carbon nanotubes and quantum dots). (Reproduced from reference 32)

Intellectual Property Rights

China has been moving towards international standards and modern regulatory practices since about 2012. The commitment to IP protection may be pragmatic and a reflection of their ramped-up investment in S&T R&D. In other words, China wants to ensure that they protect their investment and the technologies that are created. Historically, China has not been IP friendly and there were serious problems with enforcement. Currently, there are more than 80 agencies involved with IP protection in China. Furthermore, three dedicated IP courts have been established in Beijing, Guangzhou and Shanghai.[21] However, it is fair to say that a fair degree of skepticism exists and only time will tell if IP enforcement is truly occurring and is effective. In the meantime, export control in the US especially as it relates to Universities and Research Institutes must continue to be vigilant in controlling the flow of materials, data and information to China.

[32] Herron, P., Mehta, A., Cao, C. & Lenoir, T. Research diversification and impact: the case of national nanoscience development. *Scientometrics* **109**, 629-659, doi:10.1007/s11192-016-2062-7 (2016).

Technology Transfer

Technology transfer is a widely recognized challenge in China. Promoting innovation and facilitating the translation of R&D projects into commercial products was a primary driver for China's heavy investment in science and technology parks and programs such as the Innovation Fund for Small Technology-based Firms (Innofund). Innofund provides funds to companies on a project-by-project basis in the form of grants, loans and subsidies. Despite the nearly $4.5 billion USD that was invested from 1999 to 2013 in all types of S&T projects by InnoFund, technology transfer and commercialization in China is lacking.[21] Currently, "imperfect university – industry links" are considered to be the major obstacle to technology transfer and commercialization in China since universities and research institutes are responsible for the vast majority of granted nanotechnology patents.[26] "The lack of interest in acquiring frontier knowledge in many industries and the lack of communication channels between academic institutions and industry hinder[s] the commercialization of nanotechnology-derived products [in China]".[26] As such, improving technology transfer and nanotechnology commercialization remains a priority for China. It is clear that the path forward needs to include continued improvements in intellectual property rights, the removal of barriers between academics and companies and the fostering of a venture funding market that is not risk averse and attracts investors from outside of the government and includes significant foreign investment.

5. Summary of Key Points and Recommendations for Congressional Action

A. **Nanotechnology in China** - China has had tangible successes in publishing, domestic patenting and the creation of ecosystems in the form of science and technology parks, which incubate/accelerate R&D. However, China still struggles with an immature venture funding market, intellectual property protection, technology transfer and commercialization. The vast majority of Chinese nanotechnology patents are produced by universities and research institutes rather than companies. Poorly developed mechanisms of technology transfer along with weak university-industry networks lead to an insufficient product pipeline and a lack of commercialization. The lack of firm intellectual property protection also negatively influences technology transfer and venture investment.

B. **The Duality of Nanotechnology R&D –** Nanotechnology is a unique discipline that, unlike others, requires strong commitment to parallel funding of both basic research and commercial development. The commercialization of nanotechnology requires an enormous investment of funding and time due to factors such as the complexity of design, unexpected behavior, scalability and environmental, health and safety concerns. An industry focused on tight development timelines and a short horizon for an acceptable return-on-investment is not likely to have the patience for commercial nanotechnology product development especially in the bio space. In addition, there is a critical need to maintain and even increase basic research activities in nano science and technology in order to foster further discovery and inventions that will eventually become development candidates and fill a commercial pipeline.

C. **Financial Support of Nanotechnology R&D in the United States –** The U.S. can maintain its strategic advantage in nanotechnology by maintaining and possibly increasing its investment in research, development and commercialization. The NNI is the world leader in organizing, setting priorities and providing funding for nanotechnology R&D activities. However, after peaking in 2010, FY2018 federal support for nanotechnology R&D is projected to be at its lowest level since 2004 while China continues to increase investment. Since U.S. Gross Domestic Spending on R&D, including on nanotechnology, has been relatively constant since 2010, companies' investment in R&D may be offsetting reductions in government support although it is likely that commercial development is emphasized over basic research especially in the bio-nano field. It is clear that overall U.S. dominance of the nanotechnology field since 2001 can be attributed to a firm government commitment to the NNI and substantial funding appropriations for R&D.

D. **Implications for the United States –** Reductions in nanotechnology R&D funding will have serious implications on the global competitiveness of U.S. business sectors such as information technology, healthcare and national security and defense. Nanotechnology is considered a dual use technology –one that can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health, agriculture, plants, animals, the environment, or materiel. Therefore, reductions in nano funding would not only lead to reduced global competitiveness in healthcare and science and technology but also it could have serious implications on national defense as more than 60 countries have national nanotechnology development programs with their eye on dual use technologies.

E. Recommendations –

a. At least restore the appropriation to the NNI in order to maintain the position of the United States as the global leader in nanotechnology R&D.
   i. Appropriate funding for basic nanotechnology research programs. These programs require federal support since they are too "early stage" for industry.
   ii. Increase the fractional allocation of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs to further promote early-stage technology commercialization and partnerships between academia and industry.[33]

b. Establish federally funded programs to support University intellectual property development and technology transfer programs. With the exception of a relatively few major U.S. universities, the vast majority of universities do not have an adequate commitment to developing and protecting IP. In addition, the quality of most university-based technology transfer programs is lacking.

c. Monitor Chinese intellectual property activities and progress on IP enforcement, actively engage the SIPO and encourage compliance with WTO standards.

d. Support the development of public-private partnerships to promote/expand the establishment of nanotechnology accelerator hubs. Developing nanotechnology ecosystems with a critical

[33] NIH Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs. *What are SBIR and STTR Programs?*, <https://sbir.nih.gov>

mass of resources in a single location will not only spur R&D but will also ensure the retention of high paying jobs in these centers in the United States.

PANEL II QUESTION AND ANSWER

HEARING CO-CHAIR SLANE: Thank you all for that great testimony.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for your testimony.

My wife criticizes me as being a glass is always empty type person because rather than half full or half empty, I always turn it upside down to see where it's made.

[Laughter.]

COMMISSIONER WESSEL: I'm all wet, she says, as well, which is often the case.

[Laughter.]

COMMISSIONER WESSEL: So with that prelude, you know, what each of you has said in your oral testimony as well as your written testimony concerns me in terms of the economic and national security interests of the U.S., and what are I think some significant gaps or lapses in how we're dealing with these issues.

Dr. Christensen, you talked about the need to look at export controls, ITAR, et cetera.

Dr. Sinko, I think it was in your testimony you raised both the Hundred and the Thousand Talents programs, which I think there are many in our security and IC community who see as a tremendous opportunity for China to advance, if not leapfrog, their capabilities because of the porosity, if you will, of our system.

And I think, Mr. Ray, you talked about the R&D centers, et cetera. Do you see the same threat profile that I do that here we have sectors that are of tremendous long-term competitive security economic interest to the U.S., but we're not doing all that we can to advance U.S. interests and may, in fact, be enabling China in some ways that may be adverse to our own long-term concerns?

Dr. Christensen, did you want to start?

DR. CHRISTENSEN: Sure. Thank you for the question.

So I think we are right now seeing that both in terms of IP and in terms of investments, it's going to southeastern Asia. It's not going in our direction, and I think it's both we have the innovation system here, we are not commercializing it, we're not protecting it, and right now I'm also seeing that we're in a world where we're starting a trend of not attracting necessarily all the best talent.

If you go and you become a researcher in China today, you can triple your salary tomorrow. So there is a huge trend there. And I'm not seeing us doing enough to make sure that we not only remain the innovation system, which we do--today, we do have the big R&D center for Baidu, the big R&D center for these Chinese companies, but also for Amazon, Google, Facebook, all of these, that are developing amazing technology in this area.

But we need to find a way to make sure that we also commercialize it and the monetary interests stay in the U.S. rather than move to southeastern Asia, which is what has been happening over largely the last ten years.

So we need to find a constructive way of addressing this rather than just--I don't believe in closing the fence and saying this is ours. So we need to find a constructive approach. The good news is that most of the investments today are happening in the private sector and not in the public sector. It is that area that's driving it. We're going to see tremendous progress in an area like self-driving cars, autonomous driving cars.

It's not clear it's going to get commercialized in the U.S. It's very realistic that that technology might come out of southeastern Asia in terms of commercialization. We need to figure out how can we control this in a reasonable way.

So we have talent, R&D, and the commercialization. I think we're winning on the first two, but at the same time, China today is investing five times more money in this sector than we are. So we're not going to continue to be the most interesting place to be.

COMMISSIONER WESSEL: Mr. Ray.

MR. RAY: My preface would be that my wife thinks I wear a tinfoil hat that's pretty big so--

[Laughter.]

COMMISSIONER WESSEL: I've met somebody who wears a tinfoil hat. We can talk later.

[Laughter.]

MR. RAY: So I empathize. And the threats that I would like to highlight are that we can't think of this--you know, China accuses of us having a Cold War mentality. Well, one area where I agree with them is that when we think of how to protect our commercial and military advantages, we think, oh, we just need to fix export controls, but today it's a totally different world.

Today we have such fusion in our academic sectors, and there is so much exchange between Chinese and U.S. institutions. In commercial, there's more exchange today than there ever was between the United States and the Soviet Union. So we're looking at totally different animals in terms of the problems that we face and the solutions that we have to arrive at, and that's why I think the technology acquisition and technology transfer section is so important.

When we look at informal technology acquisitions, you mentioned the Thousand Talents program. That is government directed technologies that they target and then fund for experts to come to China and help China leapfrog in its capabilities.

When we talk about commercial acquisitions, I can't fault the commercial companies for taking investments that are attractive. Where it comes down to the United States government where we have to figure out what we want to protect is the Committee on Foreign Investment in the United States and groups like it need to decide what are the strategic technologies, what are the emerging technologies that we need to protect? What kind of deals do we need to investigate further and set a threshold for before we will allow that company to be acquired by a Chinese company?

And finally these Chinese companies, where are they getting their money from? Because a lot of it is coming from venture capital firms that frankly I think they're government funded. They can launder the money how they want, but in the end, it's government money.

So those would be threats that I would highlight.

COMMISSIONER WESSEL: Thank you.

DR. SINKO: So I think the situation is a bit different in nanotechnology. I think that there are a few factors. First, the United States is I think far ahead of China, and the biggest threat there is that programs like the Talents programs are bringing back folks who have worked at the NCI and other places for many, many years, and it is--

COMMISSIONER WESSEL: I'm sorry. NCI, National Cancer Institute.

DR. SINKO: Sorry. The National Cancer Institute.

COMMISSIONER WESSEL: Yes, okay.

DR. SINKO: And organizations like that. And as they recruit back these talents, they're making some progress, but we are still far ahead.

The biggest threat in nanotechnology that I see is that they're going to catch up quickly between the investment and recruiting back the talents, and then eventually they'll exceed our innovative capacity in terms of nanotechnology.

The second thing, though, is that the Chinese are focused in nanotechnology more on how to make things and this is because of their history of manufacturing emphasis. And so while my colleagues in China are more interested in making the next nano device, me and my colleagues in the United States are planning and trying to do research on how to use those devices and to get into the complexities of biology.

So as a result, I think that the threat here with nanotechnology is that they will catch up quickly if we don't invest in the basic nanoscience and technology, and as a result, we won't be able to fill that pipeline and continue innovation.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR SLANE: Senator Dorgan.

COMMISSIONER DORGAN: Thank you very much.

It seems like in almost every area in the discussions we've had with witnesses, we conclude that we have the talent and we have the IP, but they have greater capability to decide they're going to commercialize, and as a result, we talk about these imbalances that will exist now or five years or ten years from now. Is that true in all three of the areas that we've discussed here?

MR. RAY: I can lead. In terms of commercialization in the industrial robotics industry, a lot of the Chinese experts, the work that we read for our report for the USCC last year, they actually complained that Chinese research institutes were really good at coming up with prototypes for different systems, but they really struggled to get those into production.

So my argument would be that based on what they are saying, they struggle with commercialization in terms of turning more advanced industrial robots into a commercial line or production. But I think you might have better insights too.

DR. CHRISTENSEN: Right. So I think if we look at industrial robotics, for the longest time China has had a performance that's been much worse than the western world. So in comparison, we would typically say that an industrial robot has a lifetime of ten years. A Chinese robot has a lifetime of three years. We would say for a good industrial robot, it has an accuracy of .1 millimeters. A Chinese robot's is somewhere around .3 to .5 millimeters. So they've been struggling to catch up. They've been what we would call fast followers, but they've not been able, and it's been lack of gearboxes. It's been lack of good enough control. It's been lack of good enough software.

And I think that's why they finally realized we need to acquire companies like KUKA, and basically that's the way you get access to the IP, trying to redevelop it and catch up. You need to skip a generation to basically catch up with us. And they've not been creative enough of coming up with new technology that could do this. So instead they have, as was mentioned, significant purses that allows them to go and acquire the IP on the open market.

So I think the fact that there's so much access to money right now to go and buy technology on the worldwide market rather than developing it domestically is their primary advantage. We're seeing the same thing if we go to the aerospace market in terms of composite technology, in terms of all of these areas where there's no doubt U.S. is the leader today. We build much better airplanes than they do in China.

Nonetheless, the new Chinese aerospace company is hard at work to try and see if they can come up with a single aisle aircraft that can compete with us. I think they're going to buy it. It's not clear they're going to buy it in the U.S., but they're going to buy somewhere else and catch up with us.

So I think they have bigger purses than we do, and that's probably the major advantage they have.

DR. SINKO: So in nanotechnology, actually in China, intellectual property is probably driven more, I mean way more by academia than in industry. And the real problem in China is that the tech transfer process between the groups in academia generating the IP and commercialization, the companies, let's say, it's very, very poor, and as a result, filling the pipeline based on Chinese IP in nanotechnology is very, very slow and very, very inefficient.

And one of the challenges that they face is how to get the funders, the companies, or the investors to actually believe that this is the next place to go, and the reason for that is because the Chinese are very good at looking at something and reproducing it, copying it and manufacturing it.

But in nanotechnology, they need the vision to see the future, and while academics in China are beginning to see the future, it's hard to convince a funding organization and companies who are used to just making something over and over again to see that vision, to see that future, and as a result, there's a terrible disconnect between the academics generating the IP and the companies who need to commercialize it.

COMMISSIONER DORGAN: Thank you.

HEARING CO-CHAIR SLANE: Commissioner Tobin.

HEARING CO-CHAIR TOBIN: Great. Thank you, gentlemen.

On this first round, I think I'll try to get out two questions for you, and the first one is for Dr. Christensen. You mentioned from a policy point of view that there are a number of opportunities, and one of them, I'm going to read from what you've written. I'd like you to expand on that further to help us better understand.

You said Chinese companies are setting up R&D laboratories in the United States as the movement of the best people to China is a challenge for them, and you went on to say that there are regulations for export control and ITAR, but in many cases, these regulations are too slowly adapting to new technology. In addition, it's not clear that the mechanisms are effective.

So what do we do about that? What should be done if we have them coming, setting up R&D labs, which you have all said that we have been providing, and then the innovationgoes directly over there? To me, it's a significant concern, and I'd like to hear your thoughts on that, and then I'll just raise an additional question later for you, Mr. Ray.

Dr. Christensen.

DR. CHRISTENSEN: Thank you.

So I think it's important to recognize that if we look at both ITAR and export control today, its very component based. So it's looking at what can we do with better gyros? What can we do with better? So it doesn't really consider today most of robotics is not about building sort of the best components. It's about integrating systems.

HEARING CO-CHAIR TOBIN: I see.

DR. CHRISTENSEN: And the fact that we are regulating components doesn't necessarily prohibit taking entire systems. So it's much more we need to figure out how can we make sure that the systems we're building are getting protected rather than the individual components.

And there is very little regulation on that today, which makes it much harder for us. I think we need to come up--and the other is that the export control is moving so slowly compared to how quickly innovation happens. So we've seen areas like collaborative robotics coming up over 18 months. There's nothing in export control about collaborative robotics.

So there's a number of areas where I think we need to go in and highlight and say these are the key innovation areas that's going to happen going forward, and I think we can very much predict it. We tried in the National Robotics Roadmap to predict where do we think we are five, ten, 15 years into the future in terms of manufacturing, service, health, space and defense, and I think the U.S. community has a very strong view on where are the innovation areas, and most of those are not protected by current. So we need to figure out how can we not only protect component technologies but also systems technology.

HEARING CO-CHAIR TOBIN: So systems thinking and very much forward-looking with speed.

DR. CHRISTENSEN: Exactly. Thank you.

HEARING CO-CHAIR TOBIN: Great. And that's a signal for the next part of my question; right? What was that?

HEARING CO-CHAIR SLANE: That's my dog.

[Laughter.]

HEARING CO-CHAIR TOBIN: Okay. The dog robot; right?

Mr. Ray, you spoke about, in your recommendations, the United States government should fully implement the Cyber Security National Action Plan and incorporate inputs from companies and research institutes that develop unmanned systems, robots and their relevant technologies.

It sounds like they have that partially implemented--am I right—but not fully implemented. So what would it take to have a stronger implementation?

MR. RAY: That's an excellent question, and just one thing I want to add really quickly to that point that Dr. Christensen just made. One thing to also look ahead in terms of ITAR and export controls is that with these emerging technologies like AI, it's not just military spinoff. There's a lot of spin on. We see advances into the commercial industries that are not protected and have applications that are military such as in artificial intelligence. I just wanted a quick side note.

Getting to your point about cybersecurity and how we can actually implement the plan, it's going to take more industry buy-in, and it's going to have to alleviate concerns about how much people are willing to share in terms of vulnerabilities, compromises, and there are a lot of good reasons not to tell your competitors your weaknesses and your strengths, and I sympathize with that.

The question becomes what kind of information sharing mechanisms can we set up in order to get people on board and in order to get people to take this problem as a collective effort instead of individually?

I think, in terms of U.S. government steps, if we can set up the information sharing protections correctly, then I think that would increase industry buy-in, and I think that defense contractors involved in unmanned systems would have a very interesting perspective on protecting information, and they would be the ones that I would want to be talking to and getting the buy-in the most because if you can get them on board, then I think you'll see greater progress across a lot more industries.

HEARING CO-CHAIR TOBIN: Okay. That's great. And Dr. Sinko, I'll wait till the next round and let others inquire.

HEARING CO-CHAIR SLANE: Commissioner Shea.

VICE CHAIRMAN SHEA: Thank you.

We've talked about self-driving cars, and that sounds great, but maybe not if you're a truck driver or a cab driver. We talked about industrial robotics. That sounds great, but may not be so great if you're a factory worker. We've talked about service robots, sounds wonderful, but may not be so good if you're a home health aide or work at a restaurant.

So we know that the Chinese want to be leaders in these areas for export, to be manufacturers of these products and export them, but what are their intentions to sell into their own domestic market and how are they considering the inevitable dislocations that will occur as a result of selling into their domestic market? Anyone? Dr. Christensen maybe?

DR. CHRISTENSEN: Okay. Thank you.

So I think it's a very important question. The entire jobs question is going to be very important. Right now, China, if you look at the automotive sector, they're not trying to sell at all outside of China. The demand is so large in China that it's purely for sales in China.

We will see that for every one robot, if we look at a very highly automated automotive manufacturing plant, there is one robot for every ten workers. So even if we bring back a plant, only about ten percent of the jobs will be taken by robots. 90 percent of them will be by regular factory workers. It's primarily because we are difficult customers. We all want personalized cars. If you look at an Audi A4, it's available in four million different configurations. There are 256 different steering wheels for an Audi A4.

VICE CHAIRMAN SHEA: Wow.

DR. CHRISTENSEN: Because we all want heating or automatic controls and want different audio systems. That makes it very hard for us to automate it. So it's still, if we brought back a lot of the automotive manufacturing to the U.S., it would bring back a significant number of jobs, not only robotics.

We are seeing areas where we will see like self-driving cars. There are jobs that would be replaced, and there I think again China has an advantage over us. If you go and look at China, the most important skills that you can give a child today is a solid education so it's very important for them that you invest in your children's education. They not only go to school, they have mentors after school to make sure they get the best possible education.

I would claim they have a better educational system than we have in the U.S. I used to live in Georgia where somewhere around 20 percent of a generation of young kids do not graduate high school. So we are in a very scary position in comparison because I think if you have an education, you can get retrained to other kinds of jobs. If you are unskilled labor, we are challenged.

VICE CHAIRMAN SHEA: Well, I agree. I mean I agree with you completely on education, but there's a phenomenon in China--the ant kids--the recent college graduates. They're overeducated.

DR. CHRISTENSEN: Right.

VICE CHAIRMAN SHEA: There's not enough jobs that meet their own qualifications. And so I'm just very curious about all the jobs because the number one priority in China is to maintain--

DR. CHRISTENSEN: Right.

VICE CHAIRMAN SHEA: --the CCP in power, and there's already huge economic inequality in the country, more so than in the United States, as I understand it.

DR. CHRISTENSEN: Oh, absolutely.

VICE CHAIRMAN SHEA: And with these autonomous robotics, you could have tremendous job dislocation. So others want to weigh in? Dr. Sinko says no way, I'm passing on this.

DR. SINKO: [Nods affirmatively.]

[Laughter.]

MR. RAY: Sure. You raise an interesting point because one of the things that we noticed last year in researching this topic more in-depth was that Chinese experts were pretty ambivalent about the jobs issue because you saw a lot of good arguments for, well, this robot can replace "x" number of workers and it's more reliable, and your turnover rates are just very prohibitive from just keeping a production line going for very long.

So there were arguments that way, but there were also arguments that like you articulated that this could lead to displacement, and if you're the CCP, that is of great concern.

So I think that the way that I would be thinking about it from their perspective and I think the way that I'd be thinking about it from the United States perspective is that industrial robots can provide an enduring advantage in sectors like manufacturing, and I think that's the way that China sees it.

When you go through these state plans and how they get put together and who's doing it, sometimes, you know, their eyes might be bigger than their stomachs. They look to 20 years and say we want to be the best or have the most of X, Y, Z. Well, they haven't thought through all the ramifications over the next five, ten years as those policies or programs come on line.

Shifting gears to the United States, the argument that I would make is that factories are going to go somewhere, and they should go in the United States. And if that means more factories with fewer employees but more robots, then I would take that deal.

VICE CHAIRMAN SHEA: Uh-huh.

MR. RAY: And I think that would be the paradigm shift that I would try to push or that's my own opinion. I'm incredibly attentive and sympathetic to the part of robots displacing American workers, but in the long term, the next few decades, I think that there are some unavoidable trends, and we can either get on board sooner rather than later and get those initiatives or we can stay behind.

And when you think about it from the perspective of if you have highly automated factories in the United States and China, it's going to make more sense for people to buy from U.S. factories here because they're closer, and the labor costs aren't as much of a concern.

If you look at materials and transportation that go into the factories, if it's domestic, then you save costs there too.

VICE CHAIRMAN SHEA: Right.

MR. RAY: So there are a lot of compelling arguments for increased automation in U.S. manufacturing, but I do agree that we need to figure out long term and short term what does that mean for jobs and displacement.

VICE CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR SLANE: Chairman Bartholomew.

CHAIRMAN BARTHOLOMEW: Thank you.

The vice chairman stole my question, but I'll throw one more dynamic in there which is sort of that bigger issue of what happens to these workers in the U.S. and China? You know there's a fair amount of discussion starting in some places about universal basic income, and I wondered if anybody's hearing anything like that? I mean, is the CCP concerned about what is going to happen with all of these workers who are now accustomed to a certain standard of living who all of a sudden don't have jobs?

MR. RAY: Short answer is yes. And that's partly what keeps me employed. So--

[Laughter.]

MR. RAY: --if the CCP is worried, then, you know, that means that there is a demand for China analysts like myself.

CHAIRMAN BARTHOLOMEW: Yeah.

MR. RAY: So that's good. But I do think that those are tough questions that I don't really have an answer for immediately, but I think that's where programs, whether it's training, vocational, any kind of programs that teach skill sets that are more technical, those are going to be invaluable going into the future because in today's economy, you don't necessarily need a college degree to get a good entry level position.

There are plenty of technical certifications and vocational schools that provide very tailored training for specific industries. So I think that those would be the options that I would be looking towards, and I think the United States is better geared to implement those programs than China. I think that China's still trying to catch up in a lot of ways including its educational system. What does it need to look like to provide the right types and numbers of workers for the modern and future economy?

CHAIRMAN BARTHOLOMEW: Mr. Ray, just one brief thing, and then I'm going to switch gears, and that is you mentioned the big impact on manufacturing. The people are just starting to focus on what is the impact going to be in rural America when freight trucks--you know, the first probably real commercialization of self-driven vehicles is going to be freight trucks. And the repercussions for what is left of the economy in rural America is pretty big.

But I want to switch gears and talk about some of the countermeasures that the PLA is working on, and the U.S. has just announced that it is going to be sending Gray Eagle drones, Hellfire missile carrying drones, to South Korea, and I wondered if we should be concerned about PLA countermeasures?

And do they have the ability, for example, to be able to reprogram what something might be targeting?

MR. RAY: I don't know. I would definitely be taking countermeasures into account, and the interesting thing, I differentiate between hard kill just knocking out of the sky, hitting it with a really fast missile, and soft kill, so being able to jam its receptors or confuse it. And the reason why soft kill countermeasures are so attractive is that you in some settings can have plausible deniability, but in that region, that's not going to happen.

But you can gradually escalate up that ladder much more gradually. So if China wants to be more assertive in its territorial claim or express its displeasure at the U.S. deployment of THAAD in South Korea, one way to do that would be have different soft kill countermeasures against any UAVs that we deploy.

So I will be curious to see in the coming months if that happens, if we do see countermeasures, whether that be different types of lasers, electronic jamming, any kind of intercepts, whatever it is.

That's one thing that I would be paying attention to in the coming months.

CHAIRMAN BARTHOLOMEW: Dr. Christensen, anything to add on that?

DR. CHRISTENSEN: No, I will--

CHAIRMAN BARTHOLOMEW: Okay. All right. Thank you.

HEARING CO-CHAIR SLANE: As you probably all know, the Chinese have stated that they intend to become the dominant advanced manufacturing power in the world by 2025 and then in all manufacturing by 2049.

And part of their strategy is to relocate critical industries to China. So, for example, they have wiped out our optoelectronics industry, and they're all now located in China, and they're in the process of relocating our semiconductor industry. And it just seems to me that if the U.S. government doesn't start to institute some sort of policy to at least incentivize our semiconductor industry to stay here, we just get further behind.

Can you talk about that? Starting with Dr. Christensen.

DR. CHRISTENSEN: Yeah. I think the thing we should be worried about is really our high-tech industries because the low-tech industries, I don't think it's going to go anywhere for various reasons. But I think for the high-tech industries, we need to figure out what are the high-tech industries we want to hold on to, and then I think it's not clear today that we have a national strategy. What are the key technologies that we are willing to fight for and make sure that we can incentivize the industries and the researchers to build an industry here so that we can dominate it?

I think Dr. Sinko's in terms of the nanotechnology is going to come up. If we don't own this now, it's never coming back, and then I think we have to fight for it now before they disappear because once they start leaving, it's very hard for us to bring it back like we've seen for the textile industries and for other areas because once the supply chain has left the country, we will not get it back.

So I think the semiconductor industry, clearly an area. I think optics is one of those areas as well. So very advanced optics. And I think the nano-bio industry are areas where we've traditionally been very strong. If we don't find ways of doing this, we are going to be in trouble.

At the same time, I think it's important for us to understand that some industries are changing rapidly so if you go and order a book from Amazon, there's a 50 percent chance that it's being printed in your local warehouse and getting delivered to you and never being put on a truck. So we're seeing more and more manufacturing being done locally for low-tech manufacturing where it wouldn't make sense for it to be made outside of the U.S. simply because we have now so advanced technologies that we can manufacture it very locally.

It might be on Chinese machines, but it would be manufactured locally. So I think we have to identify what are the high-tech industries we want to keep and what are the ones where it's okay.

MR. RAY: I would echo that recommendation wholeheartedly. I think that we need to think strategically in terms of what advantages we want to protect and which ones we're willing to see go the way of market forces, in this case heading towards China.

You mentioned semiconductors, and that is one area that our company is following very closely because we are concerned with different trends. The biggest one is that China is throwing a lot of money at this problem. They're acquiring and they're trying to incentivize different groups to set up shop in China, and those deals are incredibly attractive in terms of government financing, going in half and half, providing capital and infrastructure, and so it's a very bold strategy.

The one thing that I would point out is that when people say this is a surprise, I would disagree with that. They telegraph pretty openly what their intentions are and what their strategic industries are that they want to promote. So I think that we can also look at what they're targeting more effectively, and we can think, and we can talk about, or indeed have a discussion about, okay, which one of these things that they're going after poses a threat to U.S. interests?

In terms of how we go about responding to that, when we look at the mandate of CFIUS, the Committee for Foreign Investment in the United States, that tracks investment coming in. One thing that it does not look at is investment going out, and I think that that could be a problem, especially when it comes to China, because if you have China offering heavy incentives for U.S. companies to move out, then we don't have as many tools to prevent U.S. companies from doing so.

And I think that the way we need to think about this is that, sure, the ITAR list, as Dr. Christensen has said, it's very component-based, but we need to think, all right, what is below that threshold but still a strategic necessity to keep, and I think semiconductors are squarely in that camp, and we need to be monitoring U.S. companies moving out.

And in terms of mechanisms or incentives, a couple of year, two years ago now, we, DGI published a report on IBM's Open Power Initiative, and how a lot of different things are being spun off into China. Well, one of the direct consequences of that is that one of our missile defense systems had to change some of the components that it uses because those components are now Chinese.

So when we look at semiconductors that go into every major weapon system in the United States military, we need to be pretty careful about what we're allowing to move abroad. So I don't want to sound alarmist, but that would be my recommendation on how to think about this.

DR. SINKO: So I would just like to reemphasize something that Dr. Christensen said. I think the nanotechnology industry is one that we want to keep, and I tried to emphasize this in my written testimony, that we are far ahead. But if you look and reverse the role, you look at China trying to catch up to us, they're not in a very good position, and the one thing I would not like to see is that role reversal. So if we don't maintain our edge, we don't maintain that investment, we're going to be playing catch-up. In essence, we're going to be giving away major advancements in nanotechnology, and we're going to lose that industry.

HEARING CO-CHAIR SLANE: Commissioner Stivers.

COMMISSIONER STIVERS: Thank you.

Dr. Sinko, this is kind of a 101 question about nanotechnology. I remember studying this issue back in college, and when I was studying it, there were all sorts of concerns about the military and national security uses of this technology back then.

Should we be concerned about today about the misapplied uses of nanotechnology especially vis-a-vis China?

DR. SINKO: And so if you first think of all the beneficial things that you can do with nanotechnology, you know, you can deliver drugs better, more specifically for specific diseases in patients. Let's say, you know, that could be easily misapplied to delivering toxins, delivering chemical agents, and this would be a major concern.

Of course, we're far off from optimizing the delivery of nanotechnology, and so I think it's far in the future. But this remains I think a major concern from that perspective.

In terms of, you know, other types of nanotechnologies, I'm not as familiar with how they could be misapplied, but I think that our major focus should be on looking at advances in nanotechnology and looking at how these different technologies will converge, and the problem that we face is that as these technologies converge, you know, biotechnology, nanotechnology, there are factors that we are just not aware of, and as a result, you're going to see important areas, like big data and high-performance computing and artificial intelligence, being able to look at these threats and analyze these potential threats as well as the potential benefits of technology.

And so I think some of them are very obvious, like I said, taking agent delivery or drug delivery and misapplying them. But others we're going to need to use some of these high-performance computing related activities to be able to identify threats that we don't even know exist today.

COMMISSIONER STIVERS: Okay. Thank you.

HEARING CO-CHAIR SLANE: Commissioner Wessel.

COMMISSIONER WESSEL: Thank you.

Let me, Dr. Sinko, but for all the witnesses as well, to go back again on some of the porosity, if you will, of our market. For the Thousand Talents program, which I don't think has received enough attention here in terms of the let's call it a cherry-picking brain drain that's going on, what kind of limits, if any, do you think we should be putting on it?

So as far as I know, there are no limits on an individual working at a federal lab where we are expending federal resources and have invested in that individual for them to participate in the Thousand Talents program. Similarly, some of our major research institutions where there may be federal funding, whether it's, you know, NIH for nanotech as it relates to biotech, et cetera.

Again, I'm just getting into this. Tell me whether those concerns are correct. Is it something we should be looking at, almost, if you will, in sort of a deemed export type situation where the knowledge that they have acquired is a national asset that needs to be preserved?

DR. SINKO: Yes, so I think this is a major point of concern. As I, let's say, hosting even Chinese students in my laboratory, we are very careful about putting up firewalls because of the intentional or unintentional transfer of knowledge, especially as it comes from our federally-funded grants and research projects.

I think the challenge is going to be, if you look at these Talents programs, if you have Chinese nationals who can go back to China, we really can't prevent them going back to China, so then the real question becomes how do you put up firewalls?

COMMISSIONER WESSEL: But the Thousand Talents program is not just Chinese nationals. I mean it's--

DR. SINKO: Right.

COMMISSIONER WESSEL: Okay.

DR. SINKO: No, that's absolutely correct.

COMMISSIONER WESSEL: Right, right.

DR. SINKO: And, in fact, you know, I've been recruited to China as a high-end foreign expert, and I speak to groups there. I speak to government groups, and my association with Fuzhou University, and I'm very careful to what I would share or what I advise and give insight to.

But I'm not sure if that's universally done by others, and I think that the United States needs to take, especially with respect to not Chinese nationals, but with respect to Americans who go to China, there needs to be active programs because there are a lot of issues.

For example, when Americans sign contracts, you know, and I get them all the time as well, you have a Chinese version and an American version, or English version, of the contract, and there are known instances where the two contracts, the translation does not meet one-to-one and that certain either financial incentives or performance requirements are different in the Chinese versus the English version.

So this is really a major concern, and it's really hampered some of my interactions with the Chinese just personally because I think there's not just misinterpretation in the translation but maybe intentional misinterpretation in the translation.

And so I think that for Americans who go to China, there need to be some sort of procedures or rules whereby it's very clear that they know what their mission is and they know what their boundaries are, but in addition, somehow the Americans who are there need to understand those boundaries, and I think it's the role of the government to reach out because right now it's almost like a free-for-all.

I could interact with China and none of you would really know, and I think that's an issue. Now at Rutgers University, of course, we have an export control office, and for those who know, we communicate, but I can tell you there are many academics, for example, who don't know that.

COMMISSIONER WESSEL: But you do that because you know, not because there is a requirement that you consult, et cetera?

DR. SINKO: That's--

COMMISSIONER WESSEL: Okay.

DR. SINKO: That's exactly correct. And I think it needs to become a more formal requirement, and I think that's where the government could assist in giving guidance and establishing those rules.

COMMISSIONER WESSEL: Okay. Any of the other witnesses?

DR. CHRISTENSEN: So it's true there are regulations in place. Whenever you do foreign travel, you have to sort of sign off and do this. But I agree it would be very good to have more information to make sure that people are truly aware of this, to what they do, but I think if we look at something like the Thousand Talents program, I think it's equally important for us to figure out how can we make sure that it's attractive enough to stay in the U.S. because regulating it and saying you can't go is very counterproductive to this.

We need to figure out how do we do this, and then if we looked at other countries--so in Europe, for instance, they've launched a number of programs for future research leaders that are very, very attractive. We do have the CAREER program for young researchers in the U.S. but not so much for senior researchers. There are less opportunities here, whereas if you look in Sweden, have sort of the Strategic Research Foundation that are investing heavily and sort of say there are 50 people in Sweden, we will fund them to make sure that they don't leave Sweden.

We've seen similar things from the European Commission. We don't necessarily have similar program in the U.S. I think we should figure out how can we make it attractive enough. And then I agree, it should come with some conditions that if you accept a CAREER program or premier fellowship, you can't go to China next year and double up on this. So I think it's fair, there are ties to those, but I believe more in the carrot than the stick in terms of how we can do this.

And I think we can try and be strategic about who are the people we should hold on to to make sure they don't go elsewhere.

COMMISSIONER WESSEL: And potentially as a follow-up written response, if you're aware of anything with NSF, et cetera, any work they've done on the Thousand Talents program, and any exposures, things that we should see here to understand how this is being looked at in the scientific community, that would be helpful.

Thank you.

MR. RAY: Is there still time to?

COMMISSIONER WESSEL: Please.

MR. RAY: Sorry. Just--

HEARING CO-CHAIR SLANE: Oh, I'm sorry.

COMMISSIONER WESSEL: I'm sorry.

MR. RAY: We can move on if we need--okay. Just something I would add: we follow the Thousand Talents program. We're familiar with it. And I would say that the threat is more widespread than you are selling it. I think that informal technology transfer is a part that is very not well understood, and that's not just talent recruitment. That's academic exchanges where you have Chinese institutions.

In my written testimony, I talk about the Chinese Association for Artificial Intelligence. Well, in English literature, the head is just a researcher and, you know, an interesting guy. In Chinese literature, he's a major brigadier, he's a brigadier general in the PLA. So, you know, there's a little bit of disconnect there in terms of his biography.

And after we published that in our report last year for the USCC, pictures of him in military uniform started coming down from the sites that we used.

[Laughter.]

MR. RAY: So they were a little embarrassed by that. So when we talk about Thousand Talents, and my concern would be people working on federally-funded initiatives going to China. I agree more in carrots than sticks. Where I think that we need to start exploring better policies is what kind of conditions we can attach to federal funds. Example is that if you host an academic conference, then you need to bear greater scrutiny for the participants, to make sure that their Chinese resume matches up with their English resume.

And when we look at people going abroad, I would not accuse anybody of anything. My concern would be that these people are not trained. They don't have a CI briefing. They don't understand what they might encounter or how they might be prodded or poked for more information so I think that that's one thing that would be worth exploring in more detail.

COMMISSIONER WESSEL: I'm sorry if I understated the threat. I don't usually do that.

[Laughter.]

HEARING CO-CHAIR SLANE: Thank you.

Commissioner Tobin.

HEARING CO-CHAIR TOBIN: Great. Thank you all.

I like your phrase, Dr. Christensen, "we need to have a national strategy to fight for," a clear strategy, so let me now get back to you, Dr. Sinko.

If you were shaping policy--and I've read your testimony--but if you were thinking about our national strategy in terms of nanotechnology, both for defense purposes and for healthcare,what would you push for? What would the strategy be?

And if you want to make it even more concrete, assume that you're meeting with Secretary Mattis, who's thinking about defense and nanotechnology, and possibly Secretary Price, what would you be saying to them to fight for?

DR. SINKO: Sure. So, you know, I think in terms of nanotechnology, there has been I think recently a push towards commercialization, and I think that's important because research, you know, shouldn't be open-ended; right? There should be a point at which research is assessed, an evaluation is made, and then recommendations are made to shape the research program.

But also there's a point at which you need to commercialize the technology, and one of the things I see now, though, is that after the vast amounts of investment in nanotechnology, the push for commercialization, and that pressure may be somewhat premature because it's being made as a blanket recommendation, and as a result I think the research end is getting somewhat of a short shrift, and I think it's very important to emphasize that you need to have continuation of basic research, and that I think it's more difficult to say, like, for example, I'm in the healthcare sector, but on the other hand, I do work in chemical counterterrorism research. So I can look at both aspects, but in terms of military use, that's not my area of expertise.

And so I think besides emphasizing continued research funding and selective pushing of commercialization, I also think it's important to bring together the academics and private industry to have a collaboration of sorts so that people can understand advances in certain technology areas as you apply them to other technology areas, and I think that would help promote, let's say, for example, the transfer of technology know-how from, let's say, the healthcare sector to the military sector because I think as we get more and more sophisticated, we're going to need the merging of these fields, and that's where the opportunity is. Of course, the merging of all the different fields is where the threat is as well.

HEARING CO-CHAIR TOBIN: I see

DR. SINKO: I think that would be the message that I would send.

HEARING CO-CHAIR TOBIN: So synergy, and would you envision this being carried out by NSF or would you suggest another collaborative structure?

DR. SINKO: Yeah, so actually, I think that's a really, a really good question. You know, like I said, I'm in the healthcare sector, but I'm also involved in engineering programs, biomedical engineering and the like. And what I see is that there's a real crossover between, let's say, what the NSF is funding and what the NIH is funding, and they're merging.

If you look at the fields of biomedical engineering now, I mean today compared to ten years ago, you know, we're nearly identical to, let's say, pharmaceutical sciences, and so I think the programs in NSF and NIH from a practical pragmatic level are starting to merge, but from the funding level, from the programs, they're not yet talking to each other enough.

But I think they're really starting to merge, at least in the nanotechnology field, and in the future, it would probably be good to have more joint programs and commissions and committees that can coordinate efforts and make better use of funding and bring people together from the different fields.

HEARING CO-CHAIR TOBIN: Excellent. Do any of you have any comments on what Dr. Sinko just said? Thank you, all.

HEARING CO-CHAIR SLANE: Thank you.

Chairman Bartholomew.

CHAIRMAN BARTHOLOMEW: Thank you to all of you. This is really interesting.

And Dr. Sinko, of course, I mean when we think of nanotechnology, I have to say that I can tell a generational difference with my colleague who thought about it in college. I think when I was in college nobody even knew what nanotechnology was. So--

[Laughter.]

CHAIRMAN BARTHOLOMEW: It's just interesting to also hear about sort of the alignment--

HEARING CO-CHAIR SLANE: You're really old.

CHAIRMAN BARTHOLOMEW: I know. Really. Maybe just where I went to college. The alignment of technology and the pharmaceutical piece is just really interesting.

I think just listening to everybody when we talk about what do we do, one of the challenges, of course, is that the nature of science is the sharing of knowledge, and so it is a community generally I think that is sometimes resistant to any restrictions on it but sometimes it doesn't even think about it.

So I was particularly interested in this whole idea maybe of counterintelligence training. One of the things we recommended last year was actually making sure that there was training available to university students because they go and they just don't have any idea that they might be targets and what does that mean and what does it look like.

But, again, I have kind of a different question. This might actually be a distinction without a difference. Mr. Ray, you mentioned that one of the weaknesses in China's robotics program is that it lags behind on complicated components and controls as well as parts requiring precision engineering. Are these problems in the industry that is manufacturing Chinese robots or are those problems in the robots that they're manufacturing?

In other words, is it a limitation on what the robot itself can do or is it a limitation meaning that they can't manufacture to get to that point with the robots?

MR. RAY: So I have some thoughts, and then I'll default to Dr. Christensen because he spoke in more detail on this issue in his testimony.

But I think it's both. I think that when you look at domestic manufacturers in China, they have been dependent on those foreign components because they know that without them, the robots won't be up to snuff whether that's a degree of precision in margin of error or if that's durability for how long they operate.

They know that the German and the Japanese components are going to last a lot longer than anything they've done, but now that they're trying to indigenize and trying to rely more on domestic manufacturers, one thing that will be interesting to see with Made in China 2025 is they incentivize firms and they strongly encourage them to buy Chinese-made robots and to import less, which has been the tendency and the preference of companies, especially in automobile industry.

CHAIRMAN BARTHOLOMEW: Yeah.

MR. RAY: They prefer foreign robots because they just work better. Well, now if they're being squeezed to get domestic robots that aren't as good and don't last as long, then what does that mean?

So I think that the answer is yes to both the points that you made, and that's one thing that I'll be interested to see how that unfolds with Made in China looking to the next couple of years.

CHAIRMAN BARTHOLOMEW: Dr. Christensen.

DR. CHRISTENSEN: So I think it's true that there are some core components that the Chinese have not been able to make so it's in particular in what we call precision gears, to gearboxes with very high precision, and that market has been entirely dominated by Japan by two companies, Nabtesco and Harmonic Drives.

And now the Chinese have recently launched a company called Harmonious Drives, and I think we can guess what they're doing.

[Laughter.]

DR. CHRISTENSEN: So, they're trying to basically copy it, but so far they haven't been able to get to the same precision. So it's a core component that they can't manufacture yet. The bad news is that we are right now seeing a change in industrial robotics from sort of traditional industrial robots where you sort of do dumb control--there's really no intelligence--that do repetitive motion--they do it over and over again--to collaborative robots where we have robots that work directly with people and so they can do the heavy lifting of instrument panel, they can do all of it, and there we don't need the same precision.

The good news is that that market is today dominated by two U.S. companies, ReThink Robotics in Boston and Universal Robots, which is a Danish company, but they are owned by Teradyne in Boston. So both of these technologies are today dominated by a U.S. company.

They are starting to manufacture in China so I think you can expect that very soon we will see this technology also go to China. So I think old robots, the Chinese haven't figured out how to do yet. The new kind of robots you should see China being a very competitive player in that space.

CHAIRMAN BARTHOLOMEW: Wow. And every answer raises more questions. But I mean are the Japanese worried about losing their technological edge to China? Is there any way we can sort of work together to make sure that certain technologies aren't--again, I'm thinking military applications there--but to make sure that certain technologies aren't acquired?

DR. CHRISTENSEN: So I think if you go and look at industrial robotics, there are cultural barriers between China and Japan that make it very hard for them. So the biggest industrial robots company is FANUC. And they don't understand how to operate in China. They're just banging heads because they have very different ways of doing it, which has been good news for ABB and KUKA because they've sort of let their--

But I think if we go and look at technology, core technologies like building aerospace structures, so drilling and composite, that kind of automation, there are significant opportunities for us to make sure that we work with the Japanese and make sure that we maintain a technological advantage over what's happening in China, and that is an area where export control today actually works very effectively.

If we go to service applications, I'm not sure I'm seeing such a big opportunity, and then I think in nano, there are strong researchers, traditionally in Japan and here, and I think there's an opportunity for us to make sure that we leverage that to sort of have a counterbalance to what's happening in China.

CHAIRMAN BARTHOLOMEW: And do you think that that leveraging will be private sector driven or do we have government structures that can encourage or facilitate it?

DR. CHRISTENSEN: Personally I think it's going to be private sector driven much more than government driven. Also, a lot of the big research we're seeing in modern robotics today is being done by Amazon, Facebook, Google much more than government programs. They are investing significantly more than we are from government programs.

I think the government programs have to make sure that we invest in the basic research rather than the applied side of it.

CHAIRMAN BARTHOLOMEW: So we have to hope that consumers will see some of the advantages in cost reductions from the savings that these companies are getting by switching over to robotics. Yet to see if that's going to happen.

So thank you, all. Just one final observation, which is to thank you for raising again the importance of us being able to retain talent in this country because I heard recently, read recently, that there were people in India who were thrilled about the immigration restrictions that are taking place in the U.S. because they see it as a huge advantage for them to be able to strengthen and build their tech sector if people are not going to be able to come here and work. And that's not good for us.

DR. CHRISTENSEN: And for Europe.

CHAIRMAN BARTHOLOMEW: Yeah.

DR. CHRISTENSEN: And I travel to Europe regularly, and they're excited about this.

CHAIRMAN BARTHOLOMEW: Yeah.

DR. CHRISTENSEN: This year our application numbers for people going to graduate studies have gone down by 20 percent, and at the same time the numbers have gone up in Europe. So we need to figure out how we can do this. I think it's very important.

CHAIRMAN BARTHOLOMEW: Yeah. Thank you. Thank you all.

HEARING CO-CHAIR SLANE: Well, that concludes our hearing for this morning. And you guys have really been great, and we thank you so much for your testimony, and we will adjourn until 1:45.

[Whereupon, at 12:42 p.m., the hearing recessed, to reconvene at 1:46 p.m., this same day.]

PANEL III: BIOTECHNOLOGY

HEARING CO-CHAIR TOBIN: Good afternoon, everyone. And good afternoon, in particular, to those who are watching on our webcast, which will also be available going forward for you to view.

Welcome back. This is the third panel. I'd like to introduce our final panel which is focused on biotechnology. Wewill explore China's pursuit of biotechnology, particularly synthetic biology and genomics, and its implications for U.S. competitiveness and national security.

We will hear first from Ben Shobert. Mr. Shobert is the founder and managing director of Rubicon Strategy Group and a senior associate for international health at the National Bureau of Asian Research, where he advises the Bureau on aging and on healthcare reforms and the pharmaceutical industry in China and Southeast Asia.

His work has been featured at CNBC, China Business Review, Fortune Magazine (China), the Harvard Asia Quarterly, and Yale University's China Hands. He's also shared his expertise on a number of international TV programs, including CCTV, CNBC Asia, CNN, and ABC World News.

Next, we have Dr. Ken Oye. Dr. Oye comes to us from the Massachusetts Institute of Technology where he is a professor of political science, is affiliated with its Institute for Data, Systems and Society, and serves as director of the Program on Emerging Technologies for the Center for International Studies.

He also chairs the DARPA-Broad Institute Foundry Safety Committee and co-chairs the iGEM Safety Committee. Perhaps you can tell us about iGEM when we get going. In the last decade, Dr. Oye has worked on adaptive regulation of rapidly changing technologies, with emphasis on synthetic biology and pharmaceuticals.

Finally, we have Ed You. Mr. You is a Supervisory Special Agent in the FBI's Weapons of Mass Destruction Directorate, Biological Countermeasures Unit. He is responsible for creating programs and activities to coordinate and improve FBI and interagency efforts to identify, assess and respond to biological threats or incidents.

Mr. You is an active member of the National Security Council Interagency Policy Committee on Countering Biological Threats and ex officio member of the NIH National Science Advisory Board for Biosecurity. He also serves on two National Academies, their committees, one of which is the Institute of Medicine's Forum on Microbial Threats, and the second is the Committee on Science, Technology and Law's Forum on Synthetic Biology.

I would like to remind our witnesses to keep their remarks to seven minutes to ensure we have sufficient time for questions and answers.

Mr. Shobert, we'll begin with you.

OPENING STATEMENT OF BEN SHOBERT
FOUNDER AND MANAGING DIRECTOR, RUBICON STRATEGY GROUP AND SENIOR ASSOCIATE FOR INTERNATIONAL HEALTH, NATIONAL BUREAU OF ASIAN RESEARCH

MR. SHOBERT: Well, thank you for the kind introduction and for the opportunity to come back a second time and testify before the Commission.

While the questions that the Commission has today are certainly specific to biotechnology, they're not unique to this sector. In fact, as we've watched in the aftermath of the November election, many of the questions that are being asked by American workers, both blue collar and white collar, are captured in the challenges that are unique to the biotechnology sector.

And to the extent that we are in the midst of working through a reimagination of what the U.S.-China relationship is going to look like going forward, the biotechnology sector is actually a good opportunity to do that because much of the upside potential in China's biotech sector remains still to be found, and there are lessons that we can draw from other high-technology sectors that are relevant to the biotech community, specifically American multinationals' access to the China market.

It should be said that if China does prove to be successful, outcompeting America in a high-technology sector like biotechnology, it would represent another way in which many of the key assumptions that have guided globalization forward in its modern era have been proved to be either inadequate or simply empty rhetoric.

The mounting frustration that is felt by various workers in the American economy does have some capture, some purchase, in ways in which the Chinese economy does not immediately create the same sort of market access conditions as the American economy has created for Chinese companies coming here.

While we can understand China's pursuit of a biotechnology sector through the lens of other high technology industries, there are peculiar matters that are very specific to China's struggles around access, affordability and quality that are going to guide the Chinese policymaking community as it goes forward, and what we should say is that as we think about the Chinese biotechnology policies, what they're bringing together at the central government level, we can and should think about those as running along two tracks.

Track A is very much understood as a conventional national economic development goal, and this track has the Chinese government seeking out policies that will deliberately, intentionally and in a meaningful way try and create capacity in the Chinese environment where biotechnology R&D can take place.

The second track is much different. The second track has the Chinese government focused on how to make sure that the healthcare system in China can offer robust outcomes on par or at least with the aspirations to be on par with what you would see in the West, and China deserves a significant amount of credit for thus far not crossing some of the lines like India has done with questions around compulsory licensing, which have limited the willingness of many multinationals to invest in India to the same extent that they have with China.

What we know about the biotechnology sector is that it requires a very unique and somewhat fragile ecosystem. And that ecosystem is populated by a very peculiar interaction between governments funding for basic science, academic, venture capital, a very, very robust intellectual property system, that takes into account the unique gestation period of biotechnology innovations at scale.

The other thing that you need that China does not have so far is you need a reimbursement system, some combination of public and private that actually rewards risk takers through the reimbursement system. And to date that doesn't exist. And so there are reasons to believe that there are peculiar conditions that are required for the biotechnology community that do not yet exist in China and may very well never exist.

We could even go further and say that some other high-technology centers, like semiconductor manufacturing, like other IT areas, have probably been more vulnerable to Chinese central economic planning than biotechnology because they're not as reliant on this vulnerable ecosystem, and they could take advantage of what have been called first mover innovation advantages.

There are, however, risks that the Commission should be aware of and mindful of as it does its work and prepares its report for Congress. The first is that there needs to be additional transparency in China around the production of what are called APIs, or active pharmaceutical ingredients. Estimates on this vary, but somewhere north of 40 percent of the global supply chain for APIs originates in China, and the bulk, almost all, of the precursors that go into APIs originate in China. And there have continued to be challenges around FDA inspector access in China around these issues.

So from the point of view of inspector access of visa approvals for FDA inspectors, there's still significant improvement that can and should be done there.

Second, it is an ongoing effort to make sure that multinationals, American companies, European companies, in this sector, have immediate access to China or, to say that differently, that their access to China through innovative products is on a same time scale as what they would experience in other developed markets.

China has had and has made significant progress on this front, but has had what's called a "drug lag" that has prevented many of our companies from bringing their most innovative products to China.

And then, lastly, we do want to pay attention to specific areas like genomics where China has significant installed capacity, has demonstrated an ability to do very specific types of innovation at scale, that have the potential to be disruptive in positive and negative ways, but we want to continue to ensure that those, those advantages, do not purely accrue to the benefit of Chinese companies, and that American enterprise has the ability to access the China market, and in genomics, that has, as part of it, concerns over data privacy, where big data is domiciled, and the access to the proprietary data sets that come out of healthcare systems.

With that, I'll wrap up my testimony and look forward to the Q&A.

PREPARED STATEMENT OF BEN SHOBERT
FOUNDER AND MANAGING DIRECTOR, RUBICON STRATEGY GROUP AND SENIOR ASSOCIATE FOR INTERNATIONAL HEALTH, NATIONAL BUREAU OF ASIAN RESEARCH

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

The modern era of globalization was able to advance by putting forward several positive messages that are relevant to China's pursuit of a domestic biotechnology sector in particular. First, what has been euphemistically referred to as "rising tides lift all boats," or to say that in a more approachable way, that whatever short-term economic dislocations might be felt in developed economies, these would subside as new opportunities specifically related to globalization accrued to the benefit of consumers, workers and businesses in mature markets.

Second, that developed economies needed to divest themselves of low skilled industries, in particular manufacturing intensive sectors, and double down on higher technology manufacturing and disruptive service sector opportunities.

Third, that underdeveloped markets represented not only new opportunities to sell existing products and services into, but that in their own right these newly available markets held within themselves indigenous innovative capacity that, if properly directed, could lead to new technologies coming to market globally that would benefit everyone.

Each of these three positive messages has unique application to the biotechnology sector; however, to the extent today's US-China relationship is marked by a renewed sense of imbalance and the need to recalibrate expectations by both public (government) and private (business) sector players, the biotechnology sector presents an opportunity to address these concerns in a way that is mutually beneficial and indicative of what may need to be incorporated in other high technology sectors going forward.

Should China prove to be able to successfully outcompete America in a high technology sector like biotechnology, it would represent another way in which assumptions about how the American economy and its workforce would be able to compete in today's globalized world have been either overstated, or simply proven to be empty rhetoric. The mounting frustration as economic displacement felt by not only blue collar, vocationally trained workers, but also their white collar, college educated colleagues, has the potential to create additional unhelpful political pressures that would greatly complicate US-

China relations. Ensuring America can successfully compete in high technology sectors such as biotechnology is essential to ensure today's globalized world advances.

Critical Context

Properly framing a response to the Commission's questions around China's pursuit of a domestic biotechnology industry requires four initial critical pieces of context that are specific to China's biotechnology sector. First, the very unique intersection between matters of China's healthcare economy with China's industrial policy. While China's pursuit of a biotechnology sector can be partially understood through the same lens as other high technology industries, there are peculiar matters specific to healthcare access, affordability and quality that will be equally, if not more, animating features in what drives China's policy makers as they craft policies specific to biotechnology. It is helpful to think of China's pursuit of a biotechnology sector as running along parallel tracks where one track is focused on the country's desire to develop domestic high technology champions in areas that employ skilled labor, while the other track is focused on the development of a domestic biotechnology sector that ensures cost effective access to basic medicines and therapies. As is often the case with China's policy making agencies, the stated intentions at the central government level are subject to wide interpretations at the sub-national level, which in the case of biotechnology makes for particularly diverse operating environments where these two tracks are communicated to industry in ways that are at best confusing, and at worst work at cross purposes with one another.

What should be said is that China's healthcare access, affordability and quality challenges are of paramount concern to China's policy makers, and that the bulk of China's policy making and regulatory power will continue to be directed towards endeavors that help address these concerns. These two tracks have the potential to cross in situations where China chooses to emphasize a particular therapy as essential to the country's healthcare system, and develop a domestic player capable of delivering the therapy at a cost the Chinese healthcare economy can afford to pay, at the disadvantage of a foreign company. To date, concerns over this type of intentional policy making apparatus have not been born out as China has been careful to ensure that it avoids crossing the sort of line that India did with compulsory licensing, which has had negative impact on multinational biotechnology companies willingness to invest in R&D capabilities in India. What can be said is that the trade of volume for aggressive price reductions has become a clear policy making tool by the Chinese government that has tempered MNC's unbridled enthusiasm about their respective upside potential in China.

The second piece of critical context is that the biotechnology sector requires a very unique ecosystem in order to incubate innovation and scale it commercially. There are reasons to believe China may struggle to build out the various elements that are specific to biotechnology. There are at least six conditions required for a domestic biotechnology sector to take root: government incentives and funding for basic science, regulatory frameworks that address the long gestation periods for biotechnology to be developed and commercialized, talent in the form of both scientists and commercial specialists, a robust linkage between government, academia and the private sector, a vibrant venture capital space, and a national reimbursement system (whether public, private, or some combination of both) that rewards all of the stakeholders for innovation.[1] While China has made meaningful progress on each of these fronts, the country still suffers from very specific problems around regulatory systems that do not adequately facilitate innovation, a reimbursement environment that definitely does not reward risk taking, and a particularly poor linkage between academia and commercial sector players.[2] Much of what constitutes government biotechnology incentives in China remains focused on “digging holes and pouring concrete.” That is to say, Chinese policy making specific to biotechnology still elevates spending on new biotechnology industrial parks with the entire associated infrastructure, as opposed to levels of direct subsidization on core R&D activities – often referred to as “bench science” - that would compare to what the United States spends through the National Institute of Health (NIH). Biotechnology innovation is inherently reliant on early-stage, very high-risk R&D, which requires a mature ecosystem in order to scale and generate returns to both public and private sector stakeholders.

The third contextual element is that China’s pursuit of a domestic biotechnology sector may well indicate the limits of its particular centralized economic planning capability. Biotechnology does not easily line up with those other high technology sectors such as clean-technology and semiconductors where China has been able to become a globally disruptive force. A helpful way to think of high technology areas where China has been most successful is in those areas that had already transitioned from bench science to application engineering, and in areas where process innovation (doing more manufacturing faster and at greater scale than in developed markets), has been most impactful.[3] The seminal study of whether Asia’s national economic development model in general works specifically in biotechnology is Joseph Wong’s book Betting on Biotech: Innovation and the Limits of Asia’s Development State. Here he writes, “… in science-based industries such as biotech, where technological, economic, and temporal uncertainties are still so pronounced, it is difficult, if not impossible, to strategically pick winners.”[4] Wong’s analysis of attempts by other Asian nation states to emulate America’s success in biotechnology is that Asia’s economic development model does not map onto biotechnology particularly well: “… [the postwar developmental state in Asia] also benefited enormously from the advantages of late development. They were the beneficiaries of second-mover advantages, whereby the uncertainties of first-order technological innovations had been managed elsewhere. They were spared the uncertainty and the heavy lifting of creating, reaping at the other end the benefits of creatively copying.”[5] Advancements in biotechnology, broadly speaking, are a constant series of pure R&D activities that are very high risk in nature – what Wong calls “first order technological innovations.” While China is working to ensure it has similar biotechnology R&D infrastructure as its western peers, the ability to leverage pre-existing technology, manufacturing processes, and engineering principles is of more limited value in biotechnology as opposed to other high technology areas.

The fourth and final key contextual element is that where risks specific to China’s efforts to develop a

[1] Ajay Gautam, *Drugs, Politics and Innovation* (Singapore: Partridge Publishing, 2016), 2-3.
[2] Xiaoru Fei, Joseph Wong, “The Rise of Chinese Innovation in the Life Sciences,” The National Bureau of Asian Research, April 2016, 21.
[3] Dan Breznitz and Michael Murphree, *Run of the Red Queen: Government, Innovation, Globalization, and Economic Growth in China* (New Haven: Yale University Press, 2011), 162-163.
[4] Joseph Wong, *Betting on Biotech: Innovation and the Limits of Asia’s Development State* (Ithaca: Cornell University Press, 2011), 9.
[5] Ibid., 168.

domestic biotechnology sector do exist for American business and consumers they are relatively easy to define, and as such, policy makers should be able to address proactively. Three risks are most notable: first, transparency as to where Active Pharmaceutical Ingredients (APIs) are manufactured in China, and robust regulatory mechanisms in place that ensure quality, safety and efficacy standards are upheld. Second, ensuring American multinational biotechnology companies (MNCs) have fair and timely access to the Chinese market under conditions that do not require them – either implicitly or explicitly – to transfer IP to Chinese partners or to wait unreasonable periods of time to sell into China because of incompatibilities between western and Chinese drug approval processes.[6] Third, working to ensure that those limited areas such as genomics and personalized medicine where China does have installed capacity that greatly desires to become world class, Chinese companies do not develop advantages over their American counterparts because of American regulatory bottlenecks, or lack of meaningful public and private sector sponsorship at a time of perceived fiscal austerity from within the US government.

China's Major Industrial Biotechnology Policies

China's 13th Five Year Plan (5YP) calls for strategic investment in five industries, of which biotechnology is one. If successful, the 13th 5YP would result in a domestic biotechnology sector with revenue of RMB 4.5 trillion.[7] The primary areas the 13th 5YP emphasizes are vaccines (hepatitis A, malaria, TB, and AIDS specifically), oncology, central nervous system drugs (mental illness, Parkinson's and Alzheimer's specifically), monoclonal antibodies (mAbs), the most recent iteration of insulin (what is sometimes called "third generation insulin"), targeted efforts in CAR-T, and personalized medicine.[8] These efforts largely follow the decisions made in the 12th 5YP, as well as the 2008 New Drug Creation and Development program. What is notable is the more specific emphasis on diseases the Chinese government recognizes will be major drivers of cost to the Chinese healthcare economy over the next several decades.

China's public and private sector players spend the bulk of all biotechnology R&D monies in Asia ($160 billion in China out of $243 billion from all of Asia).[9] In real dollars, China now spends more on biotechnology R&D than Japan and, at current trends, China's combined annual public and private sector R&D investment will be greater than all of the biotechnology R&D spending from Europe.[10] Much like what has been done in western markets where risk sharing between the public and private sector has proven to be an essential element to accelerating biotechnology innovation, China has established a "Fund of Funds," of which Cdb Kai Yuan Capital" and its $10 billion allocation is the most well-known. Efforts like this have been essential to Chinese companies' pursuit of various PD-1, IDO mAb, IL-2 IO, EGFR lung cancer and HBV drugs.

The most common types of incentives offered to both domestic and foreign biotechnology companies by

---

[6] "Understanding the Dynamics of China's Medicine Regulatory Environment," Centre for Innovation in Regulatory Science, June 2015, 2.
[7] http://www.ndrc.gov.cn/zcfb/zcfbtz/201701/t20170112_834921.html
[8] James Shen, "China Issues 13th Five Year Plan for Biotech Sector Development," WiCON Pharma China, February 2017.
[9] Xuefei Mao, "Entering China's Emerging Life Sciences Markets," MaRS Market Insights, 2014, 5.
[10] Ibid., 12.

the Chinese provincial governments is subsidized space, usually free office, laboratory and small scale production space within a biotech park for up to 6 months, and after that rental of manufacturing space, at scale, for free anywhere up to 5 years. In addition, tax incentives the Chinese government has developed for other high technology sectors such as semiconductors have benefit to biotechnology. These include up to a 15% reduction in corporate income taxes, and a 150% pretax “super deduction” on specific types of R&D activity in China.[11] Beyond these opportunities, China has rolled out what is called the “1,000 Talent Plan” that, if the person in question is selected, allows them to move to China from abroad and have the government make up the difference between what they were personally earning in a foreign market and what they would make in China at an equivalent job, as well as provide some start-up capital assuming the idea they want to pursue meets the government’s objectives.[12] Biotechnology has been one of the government’s specific points of emphasis for this program. McKinsey, who has developed a proprietary index that measures and monitors the public and private sector investment environment for biotechnology companies, rates China’s government and VC funding for start-up at 6.3 versus the US 8 (out of 10), and 6.7 in China versus 8 (also out of 10) in the United States for developed biotechnology companies in 2016.[13]

In general, funding from central and local governments for specific programs to accelerate innovation in China’s biotechnology sector should be understood as primarily emphasizing the creation of new infrastructure in the form of biotech industrial parks, expansion of the CFDA’s presence at the sub-national level, and select funding to academic institutions. Additionally, the Chinese government has moved aggressively to incentivize Chinese companies and academics to file patents. Municipal governments such as Shenzhen currently subsidize patent filings in biotechnology less to secure meaningful IP, and more to build a culture that values IP and that thinks about IP in the ways western companies and investors do. The pace of these investments has increased since the 12th 5YP, but still widely lags that of the combined public and private sector investments into biotechnology in the United States.

Comparison Between US and Chinese Biotechnology Capabilities

In the last decade, China’s efforts to develop an indigenous biotechnology sector have gone from being purely aspirational, with resources directed primarily to capacity building in the form of biotech parks, to much more intentional and focused, with the results to match. Last year saw three domestic Chinese biotechnology companies file for their IPOs (two of which – BeiGene and Chi-Med – were listed on the NASDAQ, and one of which – BETTA – was listed in Shenzhen). As would be expected if the public sector’s initial incentives were going to bear commercial fruit, private capital in China has followed, with VC biotechnology funds more than quadrupling since 2011 (from $600 million to $2.7 billion).[14]

---

[11] “Worldwide R&D Incentives Reference Guide: 2014-15,” EY, 42, http://www.ey.com/Publication/vwLUAssets?EY-worldwide-randd-incentives-reference-guide/$FILE/EY-worldwide-randd-incentives-reference-guide.pdf.
[12] http://www.1000plan.org/en/
[13] Franck Le Deu, “Building Bridges to Innovation,” McKinsey and Company, October 2016, 31.
[14] Ibid., 32.

While the growth in private sector activity in China's biotechnology sector has accelerated, much of it remains focused on molecules that were passed over by foreign MNCs, either because the market was deemed too small to justify the investment, or because the molecule was viewed as a "me-too" by established industry players. Various MNC and VC experts have voiced caution over the flurry of public and private sector activity and investment that has flowed into China's biotechnology sector: the relative immaturity of China's R&D infrastructure, its uneven enforcement of clinical trial standards, and its patchy regulatory scheme all combine to create a situation where academics and entrepreneurs can rush both less than desired "innovations" or what are essentially de-risked assets to the market and cloud the picture as to the effectiveness of China's various incentive schemes. This has all been captured with the phrase used in China's biotechnology community, that much of what is happening thus far is "not yet efficient or effective, but may some day become the latter, even if it never becomes the former." In addition, 2016 saw reports that up to 80% of clinical trial data that had been submitted to the CFDA in support of domestic pharmaceutical companies' various filings was withdrawn.[15] Stories like this speak to the relative immaturity of China's biotechnology space, and equally reinforce the need for caution when thinking about the efficacy and scalability of China's capabilities.

Where Chinese firms have demonstrated technological advantages over American businesses is primarily in gene sequencing. Led by BGI in Shenzhen, China's gene sequencing industry has been successful for two primary reasons, neither of which are purely the result of direct investment or subsidization by the Chinese government. First, BGI's gene sequencing relies on a chip array whose manufacturing techniques are analogs to much of what constitutes semiconductor chip manufacturing. Modifications to semiconductor chip manufacturing processes were necessary for gene sequencing chip manufacturing, and companies like BGI showed great process engineering competency in their ability to make these changes and drive down costs. While this chip manufacturing capability can be directly associated to semiconductor chip manufacturing, there were significant deviations BGI had to design and develop that led its capabilities to ultimately diverge from those of traditional semiconductor chip manufacturing. Second, while gene sequencing as a technology platform has become more automated, which is partially responsible for driving the price down for genetic testing, there is still a significant part of the underlying diagnostic processes that require human interaction. The ability of a company such as BGI to access a cost-effective highly skilled labor force in China has been an important feature that has allowed the field of gene sequencing to explode in China and around the world.[16]

It should be said that gene sequencing's ultimate impact to global health will be the insights it creates around personalized medicine (tailoring molecules and treatment therapies to meet the unique genetic make-up of each individual person). Many of the previously mentioned challenges that face domestic innovation for the biotechnology sector across China suggest the country's potential to become a leader in gene sequencing might never reach its full potential. This disconnect is because personalized medicine requires the unique ecosystem that China lacks, and in particular because China's

[15] Phil Taylor, "CFDA disputes claim that 80% of Chinese trials faked data but admits serious problems," Fierce Pharma, October 24, 2016, http://www.fiercepharma.com/pharma-asia/cfda-disputes-claim-80-chinese-clinical-trials-were-faked.

[16] Benjamin Shobert, "Meet The Chinese Company That Wants To Be The Intel of Personalized Medicine," Forbes, January 18, 2017, https://www.forbes.com/sites/benjaminshobert/2017/01/18/meet-the-chinese-company-that-wants-to-be-the-intel-of-personalized-medicine/#314b86247555.

reimbursement for innovation is no where near close enough to be a trigger for the type of spending on personalized medicine interventions genomics has the potential to reveal. This remains a challenge even in developed markets, where the costs related to personalized medicine stand as one of the looming obstacles that could govern the speed with which personalized medicine expands.

Where personalized medicine's advance could prove problematic to US-China relations are in artificial intelligence, computing and data storage. In each of these three areas, China's currently stated polices on cloud computing run counter to the sort of bilateral, scientifically transparent and globally portable arrangements that would ensure a level playing field between domestic and foreign companies. These are particularly of note because the next field of research in personalized medicine will require the aggregation, synthesis and analysis of large bodies of genomic data. Individual gene sequences can create between 100 GB and 1 TB of raw data, which must be stored and then analyzed on its own, and in comparison to other data sets, in order for basic scientific insights to emerge. To say this differently: the first obstacle to personalized medicine was the cost of gene sequencing itself, and the second obstacle will be the ability to analyze the resulting data at scale. It remains to be seen as to whether these data sets will readily reveal meaningful scientific insights, or if additional core science needs to be done in order for personalized therapies to be developed and commercialized.

If the insights from personalized medicine do not reveal themselves through the brute force of AI, then human endeavor will be required. Should that prove to require significant expenditure of time and money, it is realistic to assume that China could develop a meaningful lead over American business in this field. In addition, should China's early efforts to develop a National Gene Bank move at a velocity and scale beyond that of America's own endeavors, it is equally possible that the most vibrant and scalable set of data would be domiciled in China, and not the United States. According to current policies on data storage and data privacy, the computational work supporting this all would need to take place in China, leaving American businesses with many of the same questions as other American cloud computing and software as service companies currently see as not only unresolved, but benefiting Chinese companies.

Assessment of US and Foreign Firms Operations in China

In the aftermath of GSK's 2014 corruption scandal and subsequent $492 million fine from the Chinese government, there was wide consternation within the MNC pharmaceutical industry as to the government's intentions.[17] At the time, much of what constituted GSK's non-FCPA compliant business practices were the direct result of long-standing funding shortfalls within China's public hospitals. Because of these, GSK's behavior was understood as being more or less the same type, if at a different scale, that many other domestic and foreign companies were also guilty of.[18] Many MNCs feared the

[17] Keith Bradsher and Chris Buckley, "China Fines GlaxoSmithKline Nearly $500 Million in Bribery Case," New York Times, September 19, 2014, https://www.nytimes.com/2014/09/20/business/international/gsk-china-fines.html?_r=0.
[18] Natasha Khan, "Novartis to Settle SEC's China Bribe Case for $25 Million," Bloomberg, March 23, 2016, https://www.bloomberg.com/news/articles/2016-03-24/novartis-agrees-to-settle-sec-china-bribe-case-for-25-million.

Chinese government was getting ready to blame foreign pharmaceutical and medical device companies for the problems Chinese families face around access to affordable healthcare. Since the summer of 2014, these fears have more or less subsided, with the exception of a December 2016 expose on CCTV where six Chinese physicians were shown on video taking bribes from pharmaceutical companies.[19] Any time the government allows a story like this to be elevated by the national media, it re-introduces fear to domestic and foreign pharmaceutical companies that the government again has designs on them as a proxy for pervasive problems specific to China's publicly managed healthcare system.

Beyond FCPA related concerns, American companies continue to struggle with the trade between volume and price that characterizes the China market. In late February 2017, the National Reimbursed Drug List (NRDL) was finally updated after over seven years without revision. Inclusion to the NRDL allows Chinese patients to get reimbursed through China's Basic Medical Insurance (BMI) for specific medicines that previously would have been paid for entirely out of pocket. The actual price reductions pharmaceutical companies put forward in order to be included by the NRDL varies, but can be substantial (GSK's Viread offered a 67% price reduction for inclusion to the NRDL).[20] The backdrop to much of what animates American biotechnology companies' market access discussions in China today is at what price their products can be either paid for out of pocket by the consumer, or ultimately be reimbursed for (at any level) through the BMI. Absent additional expansion of the BMI in general, and in particular available funding for provincial level expansion of reimbursement policies, many western innovative biotechnology platforms may never come to the Chinese market. This partially explains the wide disparities in revenue performance specific to the Chinese market over the last two years that exist between various western pharmaceutical companies.

China's CFDA has made incredible progress over the last three years as it has addressed many of the problems around drug lag that have plagued American pharmaceutical companies. The CFDA is a fairly new regulatory agency in China, and as such has been characterized by inadequate funding, too little in the way of skilled technocrats with experience in drug and device approvals, and an approval process that was neither transparent nor particularly scientific. The net of these problems had been that MNC pharma and device companies could not predict how the CFDA would respond to a new filing, which meant most companies tabled their China market entry strategy until they had moved forward in more developed markets. The exceptions to this were few and far between, and tended to be only those molecules that had specific relevance to a peculiar problem in China's public health.[21] A number of pilot projects going back to late 2014 have accelerated the approval of innovative products through the CFDA, and have also dramatically reduced the number of invalid submittals the CFDA was working through.

---

[19] Liu Jiaying, Ge Mingning, Wu Jing and Li Rongde, "Doctors and Red Envelopes: How Corruption has Blighted China's Public Health System," Caixin, June 20, 2017, http://www.caixinglobal.com/2017-01-20/101047316.html.

[20] Angus Liu, "China updates national drug list, adding some blockbuster western meds," February 23, 2017, http://www.fiercepharma.com/pharma-asia/china-updates-basic-medical-insurance-drug-list-adds-133-western-style-meds.

[21] Benjamin Shobert, "A Decade Old Drug Launch in China With Important Insights Today," Forbes, March 18, 2015, https://www.forbes.com/sites/benjaminshobert/2015/03/18/a-decade-old-drug-launch-in-china-with-important-insights-today/#75f3ee1d644a.

American biotechnology companies have also embarked on an aggressive series of co-investments, joint ventures and licensing deals with domestic Chinese players. Notable examples of this include Bayer's additional EUR 100 million investment in its Beijing facility, Sanofi's JV with China Resources Sanjiu Medical and Pharma, and Pfizer's R&D collaboration with PegBio.[22] Of note are several outbound deals on the part of Chinese companies, such as WuXi Apptec's investment in a new gene therapy manufacturing facility in the Philadelphia Navy Yard, Humanwell's acquisition of the American company Epic Pharma (with a follow-on investment in a US R&D facility by Humanwell) and Athenex Pharmaceutical and Beijing Sciecure Pharma's FDA approval of five injectables for the North American market. Overall, cross border R&D deals that involve Chinese biotechnology companies have increased by 70% from 2012 to today.[23]

Foreign Firms Market Access

To date, the Chinese government has avoided triggering any of the problems specific to the biotechnology sector that have developed in India around compulsory licensing or other localization requirements. In addition, where the Chinese government greatly desires to see MNCs invest in local manufacturing and R&D capabilities, it has not explicitly linked these objectives to market access. If anything, ongoing problems in China's public healthcare finances prevent any such linkage from having teeth, simply because the Chinese government's reimbursement system does not have the ability to deliver on their side of the deal. As has been previously discussed, where market access problems do persist in China is around the timely updating of hospital, provincial and national drug reimbursement lists and a CFDA regulatory review process that is predictable and runs at a schedule that ensures American innovation can access the China market under adequate patent protections.

Where problems continue that are relevant to the biotechnology sector are around specific IP issues. First, China's State Intellectual Property Office (SIPO) has been badly remiss in addressing MNCs concerns that when they file for marketing approval in China through the CFDA, the submission requires that they disclose what is ambiguously defined as a "new chemical entity" as part of the application. Upon approval, the submission is supposed to create six years of proprietary coverage of the product in question. Industry has brought forward several examples where domestic Chinese manufacturers have produced generic versions of the newly submitted products within the six-year period of protection the CFDA's filing stipulates a foreign company should enjoy. This type of IP slippage will need to be monitored as the CFDA's reforms continue to accelerate. Hopefully, these cases are artifacts of a previous era when the CFDA was an unreliable partner and that this type of slippage will not continue given commitments the central government has made during recent SE&Ds to maintain the integrity and focus of the CFDA's reforms.

Second, problems specific to the SIPO examination process continue where SIPO rejects applications that in form and function are equivalent to those filed and approved in western markets. This problem

[22] James Shen, "A New Storm is Breeding for China Healthcare in New Year," WiCON Pharma China, January 2, 2017.
[23] Le Deu, 40.

goes back to concerns in the language of Article 26.3 of China's SIPO that requires a level of disclosure beyond what is required in other developed markets.

Third, the CFDA continues to inconsistently solicit industry feedback when developing new policies. The most recent example of this, beyond the already referenced NRDL and its nearly 8-year gap in being updated, is the April 2016 "Announcement Concerning the Undertaking on the Sales Price of Newly Marketed Drug."[24] This aspirational document required an up-front commitment to cascading price concessions in order to obtain CFDA approval for the launch of new drugs in China. While this was rescinded later in the year as part of the ongoing JCCT meetings, it reflects both the clumsy inner workings of the CFDA as a government agency, as well as the ongoing willingness to associate market access to aggressive price concessions.

Opportunities for Collaboration

Relationships between US and Chinese academic and commercial entities have thus far been sporadic. China has managed to cultivate three advantages relative to these collaborations. First, China does enjoy a cost advantage related specific to lab scientists that has resulted in nearly 250 Contract Research Organizations (CROs) taking root in China. Estimates are that conducting R&D in China as opposed to western markets can result in up to an 80% cost savings.[25] This cost savings has to be understood within the previous comment about China's biotechnology capability as "not being efficient, but effective." As biotechnology MNCs and start-ups seek to drive R&D costs down, CROs have become a more important part of the path to market, and China's CROs enjoy meaningful cost advantages that create collaborative opportunities. The learning that is being gathered by Chinese CROs will serve to help China's biotechnology companies improve themselves in much the same way as has happened in other high technology sectors where China's initial foray was limited to low value-added functions.

Second, a pattern has emerged around the ability to scale manufacturing pilots more cost effectively in China than in developed markets. This capability does reflect similar structural advantages that began to present to clean-technology start-ups who viewed China as a more amenable location to make the transition from concept to reality.

Third, much of what is driving Chinese biotechnology innovation – outside of personalized medicine – is the desire to identify cost effective therapies. As Yanzhong Huang noted in his 2016 testimony before the Commission, "It is estimated that diabetes alone may consume more than half of China's annual budget if routine, state-funded care is extended to all the diabetes sufferers."[26] Cost pressures of this nature will require that China's domestic biotechnology sector dual path its efforts and not purely focus on opportunities in developed markets, with their lucrative price points, margin and ROI, but also address pressing public health and chronic disease management issues for countries like China with

[24] "NAM Priorities for 2016 U.S.-China Joint Commission on Commerce and Trade," National Association of Manufacturers, April 2016, http://documents.nam.org/IEA/NAM_2016_U.S.-China_JCCT_Submission.pdf.
[25] Ivy Teh, "China's Biotech Long March," Asia Biotech, Volume 11, Number 14, 2007, 3.
[26] Yanzhong Huang, "China's Healthcare Sector and U.S.-China Health Cooperation," Council on Foreign Relations, April 27, 2016.

under-developed healthcare systems and a vulnerable consumer.

These opportunities to collaborate are taking place at a time of significant capital outflows from China into western markets, in particular towards sectors such as biotechnology that align with the central governments 5YP. Thus far, foreign companies have been able to invest in domestic Chinese biotechnology companies with relative ease. The limiting factor of inbound investment is not unfair or artificially constructed market access issues, but rather that most of the domestic biotechnology investment opportunities in China remain de-risked "me-too" platforms that do not rise to meet the investment criteria of western MNC biotechnology companies. As China's domestic capabilities in the biotechnology sector increase, it will be critical to watch and ensure today's market access standards do not revert to norms seen in other high technology spaces where foreign investment has been either entirely prohibited, or limited.

American policy makers will need to remain vigilant as to how the Chinese government responds in pursuit of its biotechnology aspirations. Should the Chinese government come up short of its economic objectives, it is possible Beijing could become more assertive around market access, IP transfer, or compulsory licensing. To date, China deserves credit for not relying on these heavy-handed tools in pursuit of its economic goals. In addition, should the Chinese government's ongoing problems specific to the nation's healthcare system continue to mount, MNCs could well again face uneven application of AML or other corruption standards that are designed to extract concessions from foreign businesses. Finally, the ability of foreign MNCs to invest in, manage, and extract knowledge from targets in China's biotechnology sector must not encounter the same type of limitations as has been the case in other high technology sectors.

Maintaining the United States' Strategic Advantages

In order for the American biotechnology sector to maintain its advantage over China and other global players, the American government needs to pursue five policies. First, the government must continue to emphasize its investments in pure R&D. Amidst the current administration's stated goals of revitalizing the nation's infrastructure and seeing additional capital be directed towards traditional manufacturing, parallel efforts must be made to ensure funding to the NIH in particular is expanded. According to the Federation of American Societies For Experimental Biology (FASEB), "From FY 2003 to 2015, the National Institutes of Health (NIH) lost 22% of its capacity to fund research due to budget cuts, sequestration, and inflationary losses."[27] While the 2016 NIH budget reversed this trend with a 5.9% increase, current inflation adjusted spending on the NIH is still well below its 2003 level. The biotechnology community employs over 800,000 people directly, and supports 3.4 million jobs in the United States.[28] These jobs are the direct result of decades of investment, partnerships and shared risk between the American government, academia, venture capital and biotechnology companies. The net of these investments has been the ecosystem that China very much wants to re-create in order to compete

[27] "NIH Research Funding Trends," Federation of American Societies For Experimental Biology, http://faseb.org/Science-Policy-and-Advocacy/Federal-Funding-Data/NIH-Research-Funding-Trends.aspx.
[28] Alden F. Abbot, "FDA Reform: A Prescription for More and Better Drugs and Medical Devices," The Heritage Foundation, June 20, 2016.

with American biotechnology companies. American policy makers should not assume this ecosystem is self-sustaining; it will also require similar tending to as its counterpart is receiving in China, at the hands of the Chinese government.

Second, America's regulatory infrastructure, in particular that embodied through the FDA, needs to be updated. Drug and medical device approvals remain a critical component that ensure patient safety; however, like any regulatory scheme, they also can take on a life of their own and become a bottleneck that stifles innovation. Various reforms have been put forward specific to the FDA. The most interesting is a reform proposal that would allow other foreign regulatory agencies who conform to global standards, and who have approved a particular drug or device, to use this foreign approval for sale and marketing in the United States.[29] Such an approach would require additional emphasis around global standards in order to ensure competition does not lead to cutting corners around approvals. The framework that would allow competition between the FDA and foreign regulatory agencies could also be deployed to allow for private laboratories to compete with the FDA. This has been successful in the United States, in particular with companies such as UL and MET. A more immediately accessible reform would require the FDA to take its approach to clinical trials, which has understandably evolved and become more complex over many decades, to streamline itself specifically in response to biomarkers and new statistical methods that today's computational systems can illustrate are clinically accurate.[30] These reforms are particularly important given personalized medicine's ability to target specific patients and the un-necessary need to structure a double-blind clinical trial whose entire methodology assumes biological similarity, versus the ability to personalize therapies as the science behind genomics and personalized medicine makes possible today.[31]

Third, ongoing efforts to reform America's patent system need to address the challenges unique to biotechnology, in particular the time that can be lost when claims are challenged or additional data is required in order to support the claim. While improvements in these areas have been made over the last several years, the combined challenges of an unwieldy regulatory scheme, coupled to a patent law system that is not uniquely tailored to the needs of biotechnology, could act as a disincentive to conduct cutting edge research in the United States versus more responsive foreign markets.

Recommendations for Congress

- Protect, and where possible increase, NIH spending with particular emphasis on additional funding for those diseases that are likely to contribute the greatest cost to the American healthcare system (oncology and Alzheimer's in particular). The goal should be to match, in inflation-adjusted dollars, the NIH's 2003 budget.

---

[29] Adam Thierer and Michael Wilt, "The Need for FDA Reform: Four Models," The Mercatus Center, George Mason Center.
[30] "Policy Solutions: Delivering Innovative Treatments to Patients," PhRMA, March 2016, 3.
[31] James P. Evans and Michael S. Watson, "Genetic Testing and FDA Regulation Overregulation Threatens the Emergence of Genomic Medicine," January 5, 2015, http://www.law.uh.edu/assignments/spring2015/19040/jvp140181-jpevansmwatson.pdf.

- Continue to bring the market access issues within planned Strategic and Economic Dialogues (SE&D) that American biotechnology companies face, specific to the CFDA's regulatory model, lack of reimbursement, and concerns around the uneven application of Anti-Monopoly Law (AML) standards between domestic and foreign companies.

- Complete a comprehensive review of the FDA's ability to monitor the production of APIs and generic pharmaceutical products in China. This is likely going to require additional funding for the FDA to expand its presence in China. Such efforts may also encounter resistance from within China as to the ability of FDA inspectors to audit suppliers in China without notice; however, this type of transparency is critical especially if China is going to continue to consolidate the global production of generic pharmaceuticals.

- Ensure American biotechnology companies in the personalized medicine and genomics field do not run into market access issues around the ability to conduct business and engage in scientific research in China. This should include specific attention to outstanding matters around data privacy issues that cloud-computing companies are currently experiencing in other industrial sectors beyond healthcare.

- Pursue targeted reforms within the FDA that allow competition within global regulatory bodies, accelerated drug and device approvals, and that reflect insights from personalized medicine and new statistical methods that no longer require traditional double-blind placebo clinical trial protocols.

OPENING STATEMENT OF KENNETH A. OYE
PROFESSOR OF POLITICAL SCIENCE AND DATA SYSTEMS AND SOCIETY AND DIRECTOR, PROGRAM ON EMERGING TECHNOLOGIES, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

DR. OYE: It's a perfect segue here or setup. So I'm going to pick up directly where Ben left off on genomics, and I'm going to start by putting on two hats. The first hat is the techno nerd, which is what you expect of MIT, and the second is the hat of the policy wonk because I also teach at the Kennedy School and the Wilson School.

So, first, on techno nerd, to explain the revolution in genomics that Ben alluded to, what we have right now is a very interesting situation, where technical developments in a number of areas have converged to create an extraordinary burst of innovation. The areas include a revolution in DNA sequencing and the efficiency in that area has improved in a way that makes Moore's law look slow.

The information sequenced or provided by taking bits and pieces of DNA and analyzing them, have been deposited in databanks at a rate that makes Moore's law look even slower. It's a vertical line on exponential graphs if you look at the testimony.

You put that together with access to healthcare data, and that's critical because genomic information alone doesn't tell you that much. You have to know what it's associated with. And those records which now exist provide the potential for putting together the pieces of puzzles to be developing gene therapies or to be developing precision diagnostics, and at the same time you need other tools to do that.

The very first panel today focused on advances in computing and changes in computing and artificial intelligence are part of the picture as well because they allow us to be able to figure out the patterns, identify potential modifications of genes, to be able to do therapeutics or to be able to tell what works or doesn't work in medical space or in other spaces.

And then put all of that together with the thing that gets all of the attention on Washington, which is the revolution in gene editing, and everyone in the room has heard of CRISPR-Cas9, but it's merely one of a series of advances in gene editing that allow people to make modifications or adjustments, knocking out, reshuffling, occasionally creating a new, that together with the other components have led to what is a remarkable period of productivity and innovation in biotechnology.

Look, I come from MIT, and I spend my life hearing my colleagues talk about what is just around the corner. What is unusual in this space is that what has been happening, in fact, is remarkable. In agriculture, what you see are changes in the improvement of plants and animals that make for potentially more efficient conversion of matter into food.

If you turn to medicines, the changes have been extraordinary in terms of advances with 300 applications of somatic cell gene therapies in late stage development today. Precision medicines, which is actually the space that China is going to be working big on by taking advantage of and putting things together.

Methods of discovery that pool the information. A potential switch for obesity is something that a colleague at MIT has developed. But the IT was a key part of it, putting together data to know what part of the genome to tweak to get the effects.

In fact, the advances certainly continue through industry with methods for production of industrial materials, be they fuels or high-value chemicals or drugs. Through yeast, converting sugar into artemisinin or sugar into morphine. Again, these things are not way off in the distance. They're happening today.

And some colleagues, they've even worked up methods for editing the genes of plants and animals in wild populations with the potential for reshaping environments or doing remediation through technologies that are called gene drives.

And all of this, most of what I've discussed has happened just in the last couple years. Now, I spent that time, and I'm removing geek hat and putting on policy wonk hat because an understanding of the technology is critical to understand what policies are best used to promote innovation or to promote or limit diffusion. You have to understand the technology well enough to be able to really answer those questions.

So what has China been doing and the U.S. been doing? Much of what's going on would be familiar to you because your commission has been looking at state-centric industrial policy, sectoral industrial policy for a long time. So it of no surprise that the development banks are providing subsidies to firms. This is a standard method of operation.

It's also not surprising that a high quality secondary educational system for STEM education is providing the foundations of much that we're talking about in China, that international exchanges are critical with the significant numbers of Chinese graduate students here providing a foundation for much of what is going on in this country, and I've heard much discussion of return, the return of those students being one mechanism for technology transfer.

I recommend against cutting off access to education in the United States because I would actually suspect that the cost to the United States would be far greater than the losses of technology that are proceeding to China, but that's something that we could turn back to.

You put all these things together and add to them regulation, and part of it we hear much about burdens of regulation, but regulations in the United States have at times created demand for products. If you take the advanced biofuels blending mandate, for example, it created demand for the technologies that were being developed out largely in California, but elsewhere as well, for the production of biofuels through synthetic biology.

In the last 54 seconds, two quick notes. If you're talking about where this leads in terms of economic and security implications, there is good news and bad news from one common phenomenon. The common phenomenon is rapid diffusion of the technologies. In fact, no one can sit there and bottle up synthetic biology or bottle up, if you will, the fact that this particular strain of yeast is good for producing stuff. It's very, very difficult to limit access to information or the physical specimens.

What that means in economic terms is that our advantage is, in fact, likely to erode to some degree, and that happens in most areas where a country has an advance, but the good news is that the potential for exploitation of advantage will be somewhat limited. You can't jerk the chain and maintain an advantage if the thresholds or barriers to entry are relatively low. So the opportunities for manipulation for strategic advantage, in fact, are going to be fairly limited because the capacity or potential independent innovation and for diffusion will limit that.

But that's bad news for security, and its bad news for security because what we have is a situation where a variety of actors will have access to technologies with the potential for doing harm as well as good. I'm worried in some ways less about state action in this space--the Bioweapons

Convention has been working pretty well--than I am about sub-state actors.

And I would put forward as sort of the central challenge on security a challenge of shared security looking across countries, but looking across countries to be able to maintain and develop and deepen mechanisms for limiting threats of inadvertent misuse or malevolent misuse by sub-state actors. So let me stop on those notes, and we can return to themes as you wish.

Thank you.

HEARING CO-CHAIR TOBIN: Thank you, Dr. Oye.

Mr. You. I think this is going to be an easy transition, too; don't you?

PREPARED STATEMENT OF KENNETH A. OYE
PROFESSOR OF POLITICAL SCIENCE AND DATA SYSTEMS AND SOCIETY AND DIRECTOR, PROGRAM ON EMERGING TECHNOLOGIES, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

This statement describes the development of synthetic biology and genomics within the United States and China, analyzes opportunities and challenges facing the United States and suggests how the United States might better support high-quality, advanced biotechnology research and industry development going forward.

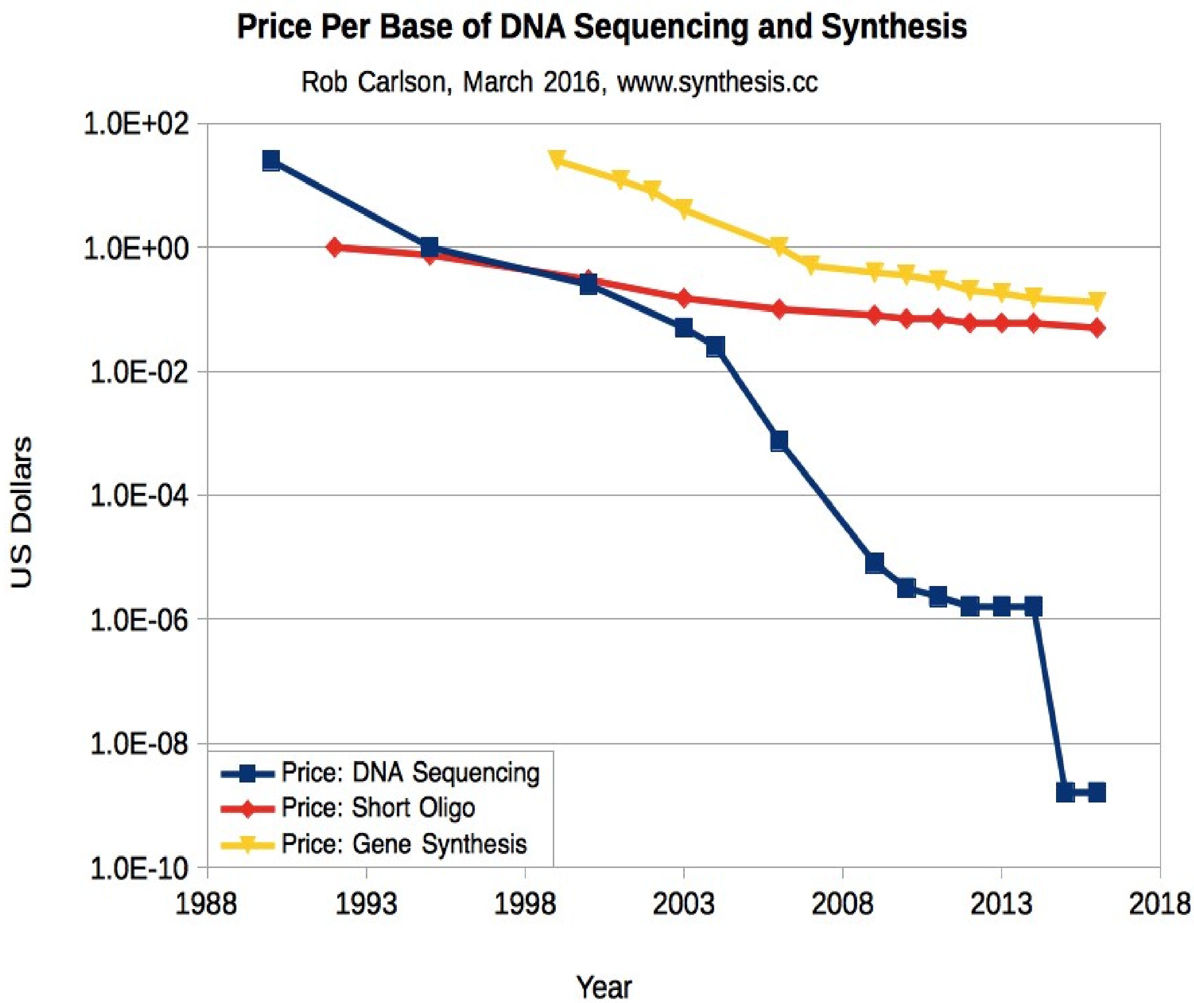
Section I: Biotechnology Fundamentals
This section reviews sources and consequences of extraordinarily rapid change in biotechnology, with attention to:
* How advances has been enabled by a "great conjunction" of improvements in DNA sequencing and synthesis; data storage and access; pattern recognition methods; tools for redesign of organisms; and tools for gene editing; and
* How foundational advances are enabling applications including synthesis of fuel, feedstocks, scents, drugs and flavors; redesign of food crops and livestock; somatic and germline gene therapies; control of vector borne diseases; and remediation of damaged environments.

Section II: U.S. and China Policy Comparisons
This section describes how the United States, China and other major nations have supported research and industry development, with comparisons of:
* Motives for priority development of biotechnology sectors;
* Policies to develop capacity, including research funding and educational policies;
* Regulations that address privacy, security, safety and environmental concerns; and *
Policies designed to foster or limit international flows of technology.

Section III: U.S. Policy Options
This section offers policy recommendations for sustaining U.S. innovation in biotechnology with regard for competitive economic interests and for common safety, health, security and environmental concerns.

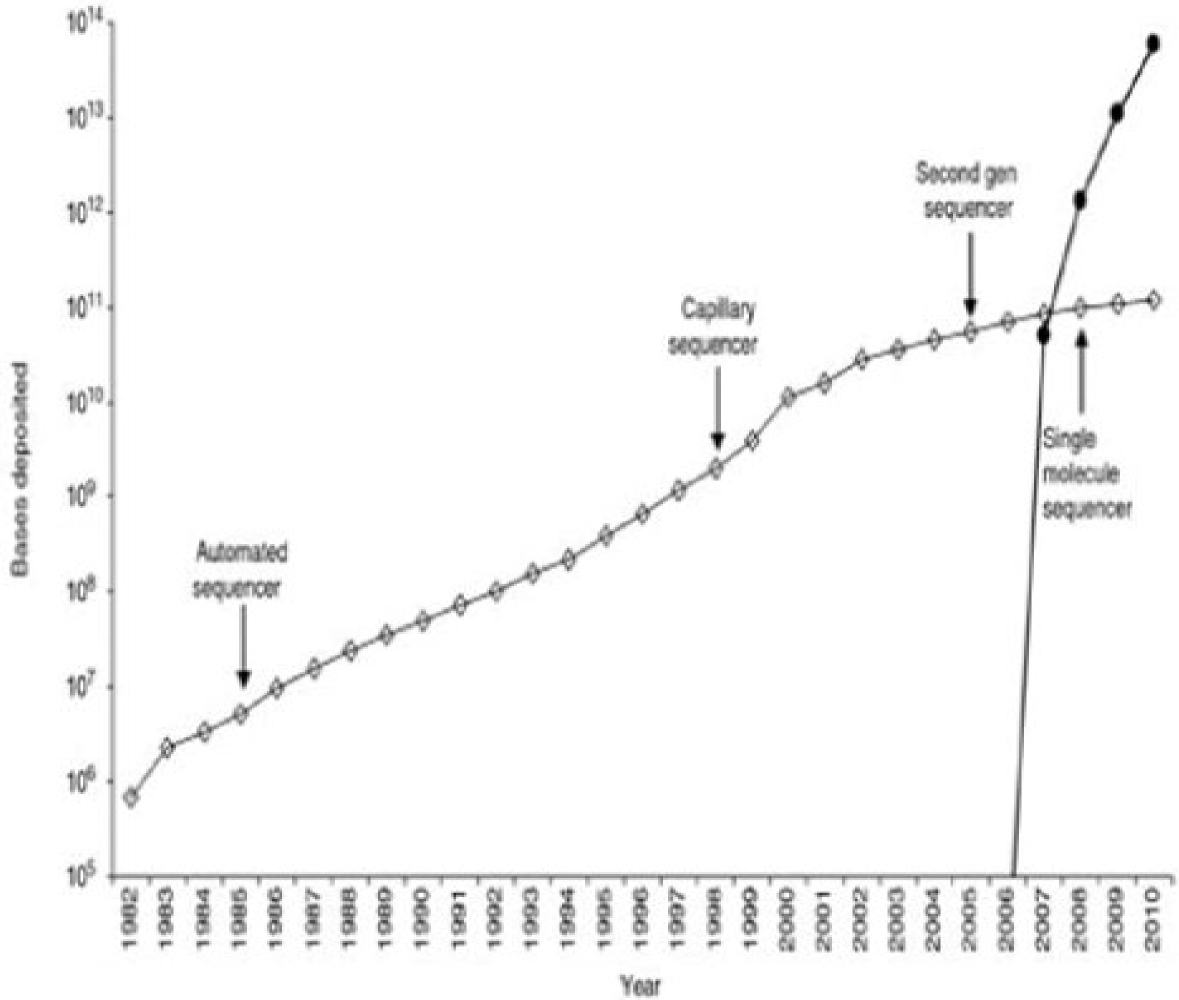
Section I: Explaining Rapid Innovation in Biotechnology

In the past five years, the field of synthetic biology has come of age. Tales of unrealized promise have been supplanted by partially and fully realized applications in agriculture, materials synthesis, and therapeutics, with next generation bio-remediation of contaminants, control of invasive species, and limitation of vector borne diseases on the horizon. This remarkable burst of innovation has been enabled by an unusual conjunction of several technological developments.



First, the efficiency of DNA sequencing and oligo and gene synthesis has increased dramatically. In the figure above, compiled by Rob Carlson, the vertical axis is an exponential.

Reductions in the cost of sequencing, shown in the blue line, are at a rate that makes Moore's law look slow.[1]



Second, the revolution in sequencing has, in turn, fostered an explosion in the amount of genomic data deposited in data bases. In the figure above, also with an exponential vertical axis, genomic information deposited rockets upward.

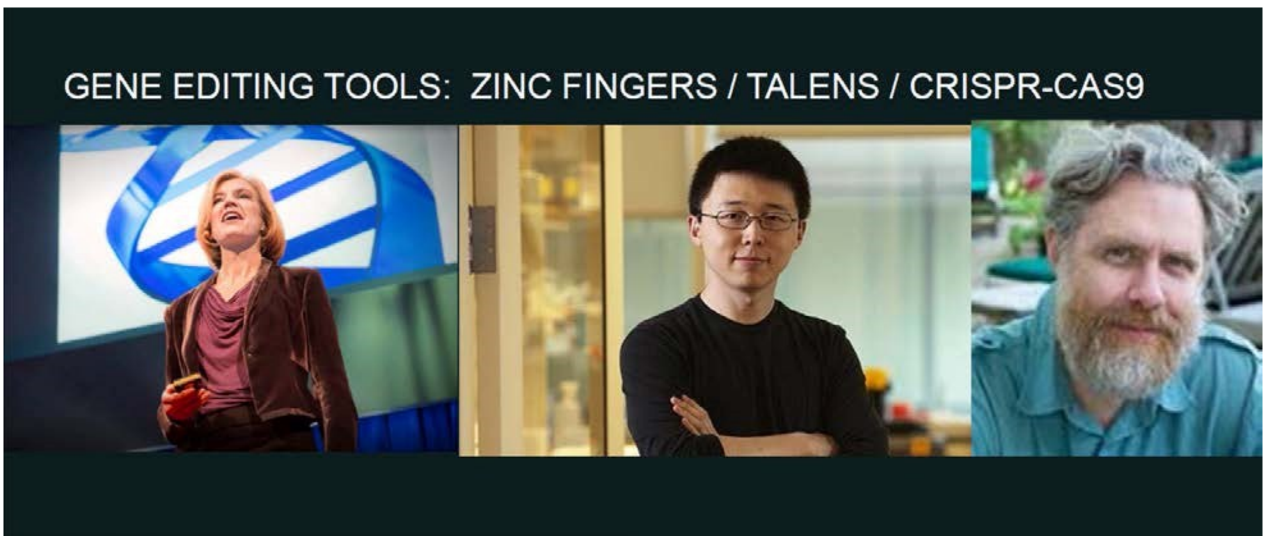
Third, the revolution in applied biotechnology has also been enabled by improved access to phenotypic information and health care records that are linked to genomic information including the spread of electronic health records.

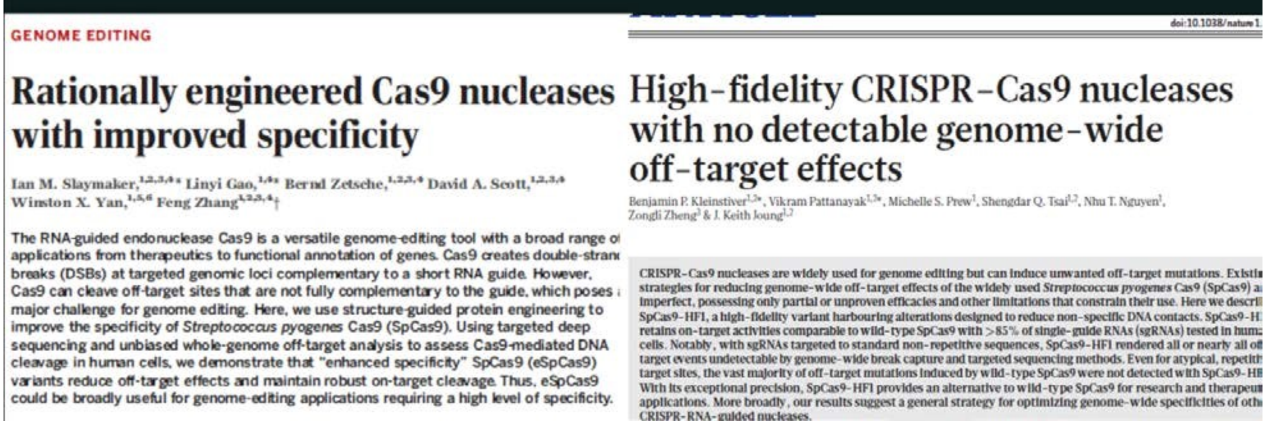
[1] http://www.synthesis.cc/synthesis/2016/03/on_dna_and_transistors

Fourth, the development of advanced computational tools has aided in inferring the effects of genetic alterations and in constructing data bases on the functions served by genetic elements and parts.

Fifth, the development of software tools to aid in the redesign of biological systems such as SGI Archetype have improved the predictability and reduced the cost of producing blueprints for biological engineering.

Finally, improved gene editing tools have greatly reduced the cost of translating blueprints into alterations of genetic material and have increased the accuracy of alterations. The development of CRISPR-Cas9 by the Doudna group at UC Berkeley and Zhang and Church groups at MIT-Harvard-Broad represents a substantial improvement over zinc fingers and talens.
Further advances in gene editing tools including base editing are certain to come.





GENOME EDITING

Rationally engineered Cas9 nucleases with improved specificity

Ian M. Slaymaker,[1,2,3,4*] Linyi Gao,[1,4*] Bernd Zetsche,[1,2,3,4] David A. Scott,[1,2,3,4] Winston X. Yan,[1,5,6] Feng Zhang[1,2,3,4]†

The RNA-guided endonuclease Cas9 is a versatile genome-editing tool with a broad range o applications from therapeutics to functional annotation of genes. Cas9 creates double-stran breaks (DSBs) at targeted genomic loci complementary to a short RNA guide. However, Cas9 can cleave off-target sites that are not fully complementary to the guide, which poses a major challenge for genome editing. Here, we use structure-guided protein engineering to improve the specificity of *Streptococcus pyogenes* Cas9 (SpCas9). Using targeted deep sequencing and unbiased whole-genome off-target analysis to assess Cas9-mediated DNA cleavage in human cells, we demonstrate that "enhanced specificity" SpCas9 (eSpCas9) variants reduce off-target effects and maintain robust on-target cleavage. Thus, eSpCas9 could be broadly useful for genome-editing applications requiring a high level of specificity.

doi:10.1038/nature1

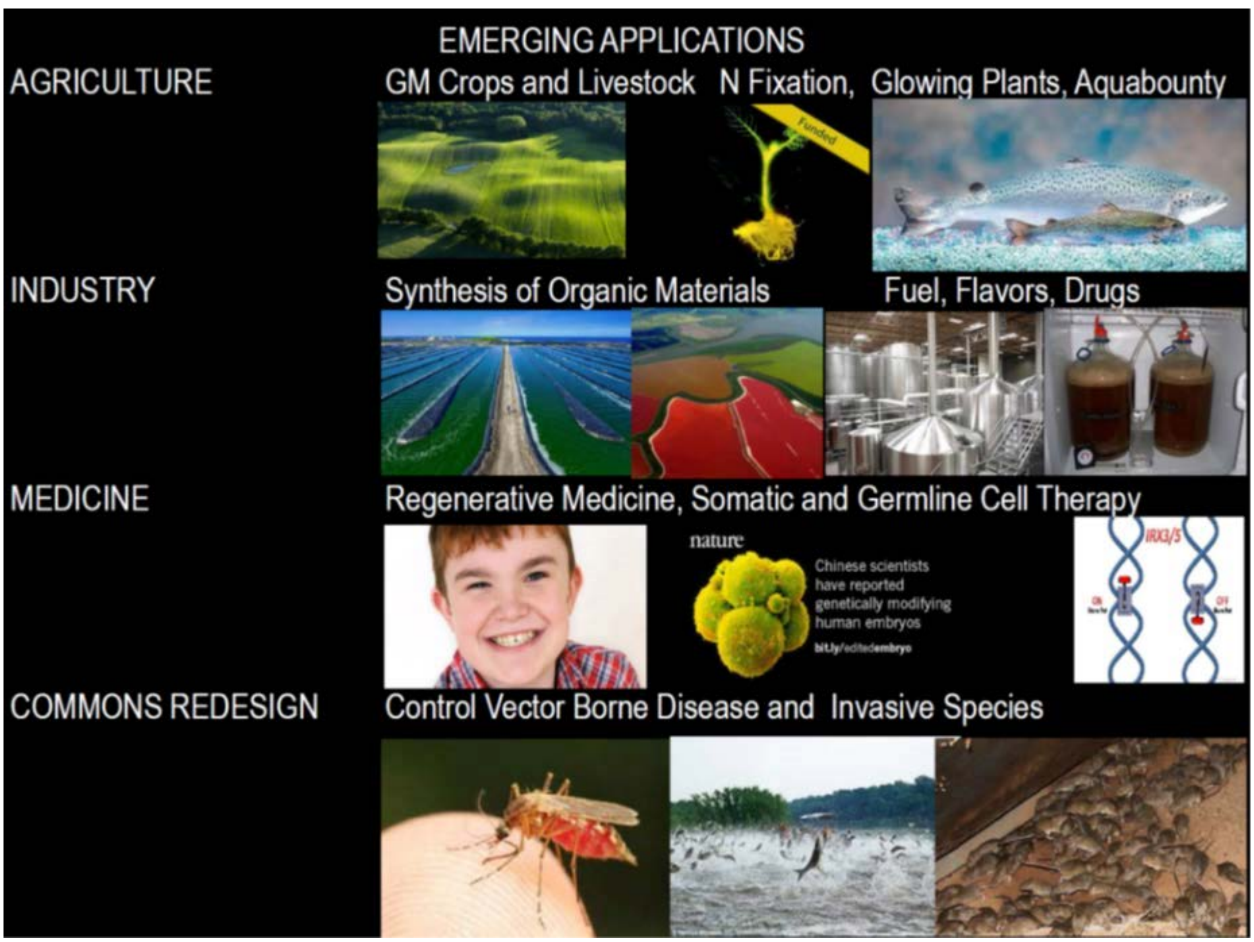
High-fidelity CRISPR–Cas9 nucleases with no detectable genome-wide off-target effects

Benjamin P. Kleinstiver[1,2*], Vikram Pattanayak[1,2*], Michelle S. Prew[1], Shengdar Q. Tsai[1,2], Nhu T. Nguyen[1], Zongli Zheng[3] & J. Keith Joung[1,2]

CRISPR–Cas9 nucleases are widely used for genome editing but can induce unwanted off-target mutations. Existi strategies for reducing genome-wide off-target effects of the widely used *Streptococcus pyogenes* Cas9 (SpCas9) a imperfect, possessing only partial or unproven efficacies and other limitations that constrain their use. Here we descri SpCas9-HF1, a high-fidelity variant harbouring alterations designed to reduce non-specific DNA contacts. SpCas9-H retains on-target activities comparable to wild-type SpCas9 with >85% of single-guide RNAs (sgRNAs) tested in hum cells. Notably, with sgRNAs targeted to standard non-repetitive sequences, SpCas9-HF1 rendered all or nearly all o target events undetectable by genome-wide break capture and targeted sequencing methods. Even for atypical, repetiti target sites, the vast majority of off-target mutations induced by wild-type SpCas9 were not detected with SpCas9-H With its exceptional precision, SpCas9-HF1 provides an alternative to wild-type SpCas9 for research and therapeu applications. More broadly, our results suggest a general strategy for optimizing genome-wide specificities of oth CRISPR-RNA-guided nucleases.

It is important to note that the revolutionary pace of change in biotechnology is the product of all of these developments, not improvements in gene editing tools alone. We can expect further acceleration in biotechnological innovation as synthetic biology comes to interface more effectively with systems biology.

These advances in fundamentals of biotechnology have enabled a broad range of applications. MIT technologists are developing nitrogen fixating non-legumes and Aquabounty has developed a variety of salmon that is more efficient in converting feed into fish. Firms have modified algae to produce low value biofuels and redesigned yeast to produce high value anti-malarial drugs, scents, and flavors. Laboratories at Stanford, University of California and Concordia have even created pathways in yeast to convert glucose into hydrocodone and morphine. The Church lab at Harvard took a large step toward xenotransplantation by using multiplex gene editing to eliminate over 60 Porcine Embedded Retro-Viruses (PERVs). Medical researchers now have over 300 somatic cell gene therapies under development and a team at Sun Yat Sen University has attempted human germline modification for a genetic blood disorder. Finally, teams in London, San Diego and MIT are developing gene drive technologies to edit the genes of plants and animals in wild populations, with the potential to contain vector borne diseases and to eradicate invasive species.



The blurring of the line between information technology and biotechnology is fundamental to most of these applications. For example, Manolis Kellis of MIT combined genomic, phenotypic and health record information and applied advanced methods from artificial intelligence to generate a hypothesis on the location of an obesity switch, then tested his proposition through gene editing, culturing cells and conducting trials on animals. Access to and analysis of information is now as critical to biological engineering as editing, splicing and synthesizing genes.[2]

Section II: Comparing U.S. and Chinese Biotechnology Policies

This section describes how the United States, China and other major nations have supported research and industry development, with comparisons of:

- Motives for priority development of biotechnology sectors;
- Policies to develop capacity, including research funding and educational policies
- Regulations that address privacy, security, safety and environmental concerns; an
- Policies designed to foster or limit international flows of tech2.

Why is China seeking to develop its biotech sector? China's motives for development of biotechnologies are similar to those of the US, Europe, Japan, and India. All OECD nations and most rapidly industrializing developing countries have made development of biotechnologies a priority. Across the board, there is recognition of the increasing economic significance of biotechnology in materials fabrication, redesign of plants and animals for production of food, and development of advanced therapeutics.

China's interest in biotechnology is also driven by peculiarities of Chinese circumstance. The need for enhanced efficiency in agriculture and aquaculture is stoked by the scarcity of arable land and water. The need for cleaner fuels is stoked by world class pollution problems with rapid growth and dependency on coal and traditional biomass and by dependency on imported oil. The need for advanced methods of environmental remediation and restoration is stoked by loads imposed by traditional methods of reprocessing E waste and recycling paper and metals. Most fundamentally, advanced biotechnologies are a key element of Chinese plans to substitute high value clean sectors for low value dirty manufacturing.

China's interest in advanced biotechnology is also driven by a belief that this is an area where China can excel relative to the U.S. and Europe. As other nations commit resources to biotechnologies, China has advantages that may contribute to competitive success over the long term. Relative to the US, Chinese enjoys an advantage with respect to excellence in secondary level STEM education and the ability to direct substantial public resources to biotechnology sectoral development.

---

[2] "FTO Obesity Variant Circuitry and Adipocyte Browning in Humans," New England Journal of Medicine 2015;
373:895-907September 3, 2015DOI: 10.1056/NEJMoa1502214
http://www.nejm.org/doi/full/10.1056/NEJMoa1502214?rss=searchAndBrowse#t=article

Relative to Europe, China enjoys an advantage in ability to tune regulations and policies on privacy, intellectual property and environment.

How is China building its domestic capabilities in biotechnology?

Public financial resources are being used to develop industrial and educational infrastructure. The emergence of firms like BGI as the lowest cost highest volume gene sequencing firms in the world and the emergence of high quality synthetic biology educational programs in top tier and second tier Chinese universities and the headline advances by Chinese researchers in areas such as human germline modification have been fostered by strategically coherent and substantial infusions of funds. Official numbers on Chinese public funding are both hard to come by and are inherently suspect. While it is clear that Chinese public funding for development of biotechnologies is significant and has had substantial effects, we do not have a credible basis for determining whether it is commensurate with U.S. public funding via DARPA, IARPA, NIH, DoE and NSF.

Chinese biotechnology firms have been active in international mergers and acquisitions to secure ownership of key technologies. For example, back in 2012, BGI substantially enhanced its capacity for sequencing by acquiring Complete Genomics for $120 million. [3] More recent acquisitions appear to also improve market access as well as ownership of technologies. ChemChina acquire Syngenta AG for about $43 billion. Humanwell Healthcare Group acquired Epic Pharma for $550 million. Creat Group Corp acquire Bio Products Laboratory Ltd., a maker of human blood plasma products in the U.K., for $1.2 billion. Shanghai Fosun Pharmaceutical Group Co offered to India's Gland Pharma Ltd., which is focused on injectable drugs.[4]

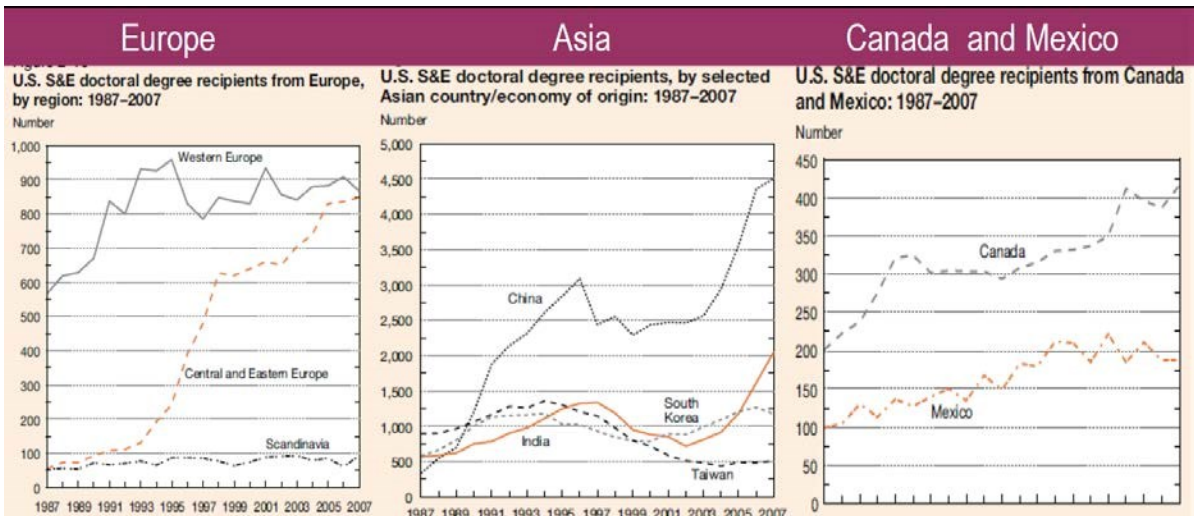
The effect of regulatory differences on development of biotechnology is complex. Chinese rules on environmental protection appear to be far less constraining than equivalent regulations in Europe, where uncontained agricultural and environmental applications of synthetic biology are effectively barred, and slightly less stringent than regulations in North America, with less clear standards for presentation of evidence on environmental effects. Chinese rules on biosecurity appear to be less stringent and explicit than U.S. equivalents, with DURC policies governing research and Australia Group guidelines on licensing and documentation governing transborder movements. Chinese rules on privacy and data utilization are unclear, but appear to be less restrictive than U.S. or European protections. On balance, it appears that Chinese firms are likely to have greater freedom to operate than their US or European counterparts, but the opacity of regulations and firm level practices precludes definitive statements on this point.

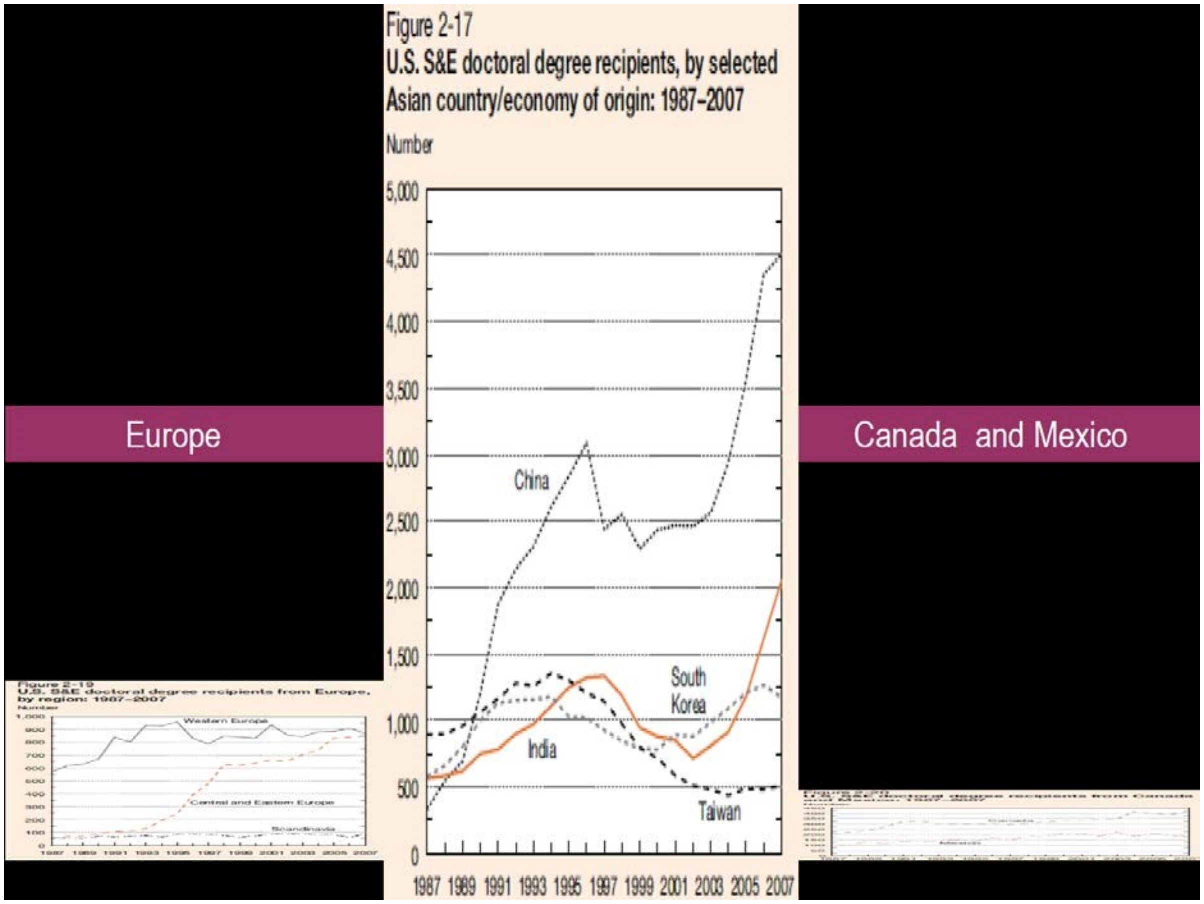
[3] https://dealbook.nytimes.com/2012/09/17/chinese-company-to-acquire-dna-sequencing-firm/ and https://www.genomeweb.com/sequencing-technology/bgi-halts-revolocity-launch-cuts-complete-genomics-staffpart-strategic-shift

[4] https://www.bloomberg.com/news/articles/2016-07-05/china-inc-goes-on-a-buying-spree-for-global-healthcare-assets

What relationships have Chinese firms, research institutes, or universities developed with U.S. universities and research institutions in biotechnology?

Chinese universities have engaged in a typical array of international exchange and outreach activities, with research partnerships with US, European and Japanese counterparts and with substantial participation in international educational collaborations. The most significant educational activity is Chinese participation in U.S. doctoral programs in biological engineering, molecular biology, systems biology, chemical engineering and computer science. To provide some sense of the scale of Chinese engagement in U.S. S&E education, consider the following figures.





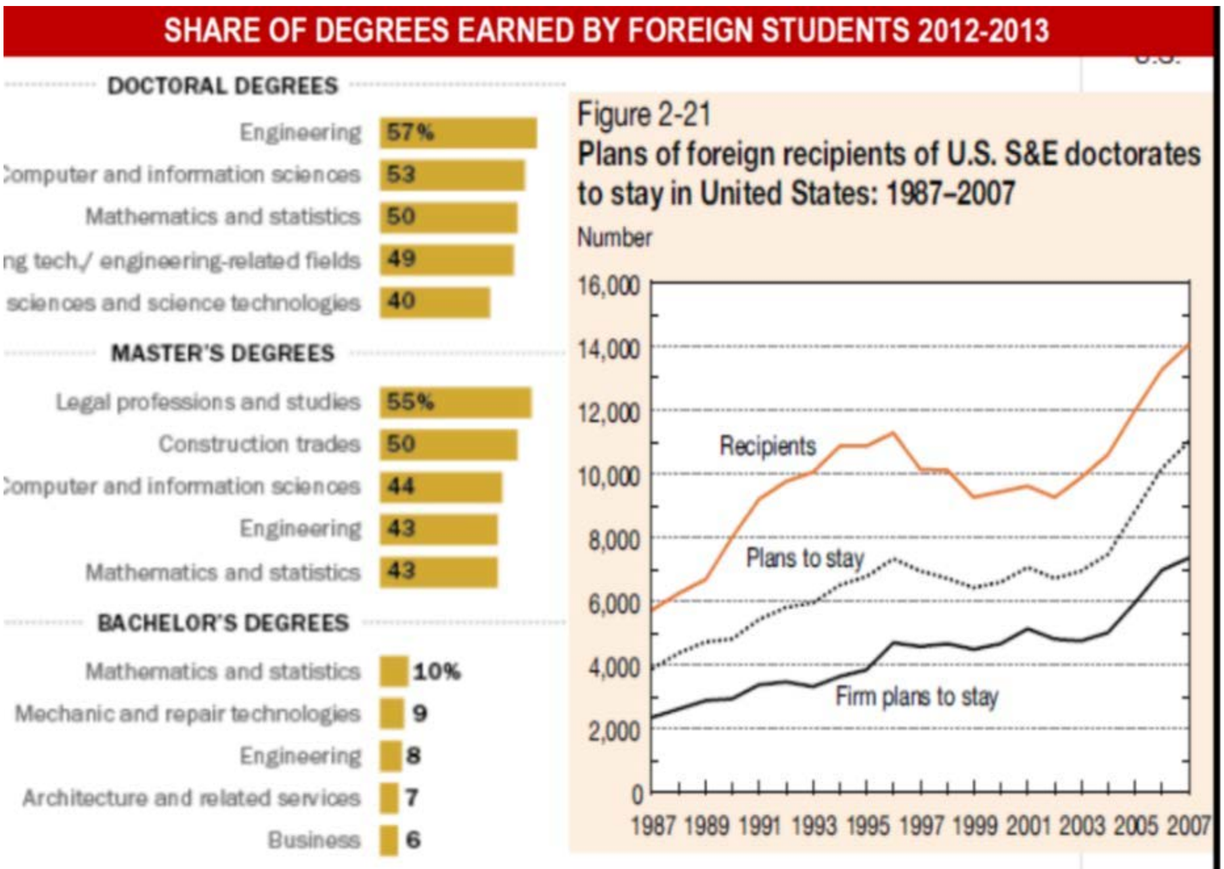
The first figure above presents international student data in S&E doctoral programs by region of origin. The second figure presents the same data rescaled on equivalent vertical axes to underscore the extent to which Chinese students are found in U.S. doctoral programs.

International collaborative activities appear to be valued highly by the government of China. One informal indicator may be found in the International Genetically Engineered Machine Competition (iGEM), where the number teams from China increased from 30 out of 230 in 2013 to 60 out of 300 in 2016.[5] U.S. partners have structured collaborative relationships to address some risks. For example, the FBI and iGEM have cooperated in developing a biosecurity and biosafety program to reduce the risk of malicious or accidental misuse of biotechnologies. Firms and universities typically take care to protect intellectual property from appropriation, but many firms and academics have failed to take even the most basic precaution of applying for patents in China. Finally, academic researchers and scholarly journals continue to have difficulty defending themselves against fabricated research and

[5] http://igem.org/Team_List?year=2013 http://igem.org/Team_Wikis?year=2016

clinical data from researchers in all settings including China. The problem of irreproducible results is not unique to the PRC.

How have these relationships benefited U.S. researchers or advancements in the field? Are there potential collaboration, research and development, exchange opportunities that should be pursued? What challenges remain?



As the figure above suggests, a high proportion of Chinese students who come to the US for graduate study would like to stay in the U.S. after they secure their degrees. CRISPR inventor Feng Zhang immigrated to the U.S. from China as a child. At present, the U.S. benefits from this combination of education and immigration. Over the longer term, as educational programs, standards of living and research opportunities in China improve and more students choose to return to China, this imbalance favoring U.S. interests will decline. Such was the case with Japan, Korea and Taiwan as the proportion of students choosing to stay in the US declined as opportunities at home improved. Such will be the case with China.

How will these developments affect U.S. global competitiveness and national security?

Movement toward technological parity is likely with some effects on U.S. economic competitiveness and national security. The current preeminence of American biotechnology will decline as domestic Chinese capacity increases and as technology diffuses from the U.S. to China. The effects of these developments on U.S. competitiveness and security are complex.

The central issue is the extent to which superiority in biotechnology translates into market power and political power. This is not an area where cornering markets or forming cartels is viable. No country including China and the U.S. will be able to dominate biotechnology. The ability to do first rate biological engineering is diffusing rapidly from the U.S. to many other countries including China. This is most evident in the iGEM competition, with its exponential growth in numbers of participants and extraordinary gains in the quality of work. While some view the magnitude of technology transfer as a critical problem, the ease with which biotechnology is moving and developing in many centers suggests that this is not an area where cornering markets or forming cartels is viable. Efforts to exercise market power through collusion to extract rents, through the strategic denial of access to secure political leverage, through the control of strategic inputs into weapons systems seem likely to strengthen incentives for entry. It is difficult-to impossible to withhold a cure for cancer, a method of producing a fuel, a drought or blight resistant strain of rice or a yeast strain that produces a pharmaceutical. Lasting advantages will be hard to obtain and harder to defend. Technological genies with the potential to address substantial environmental, economic and health problems will proliferate and cannot be captured by any one master. This is the good news.

But the good news on economic effects is the bad news on security effects. If diffusion of relevant skills, technologies and data is a hallmark of emerging biotechnologies, then it will be difficult to check the potential for malevolent or unintentional misuse of advanced biotechnologies by nations, groups or individuals. Potential misuses include the modification of existing pathogens to increase virulence, with H5N1 gain-of-function adjustments as a possible model for other diseases; circumvention of materials controls through synthesis of a listed pathogen; production of controlled substances; and novel threats that I do not wish to discuss in an open hearing. Because advanced biotechnologies cannot be stuffed back in the bottle and will diffuse, addressing potential security risks is a wicked difficult problem.[6]

[6] “What rough beast? Synthetic biology, uncertainty, and the future of biosecurity” Gautam Mukunda, Kenneth A. Oye and Scott C. Mohr Politics and the Life Sciences Vol. 28, No. 2 (September 2009), pp. 2-26 https://www.jstor.org/stable/40587998?seq=1#page_scan_tab_contents; “On Regulating Gene Drives” KA Oye, K Esvelt et al, Science 08 Aug 2014: Vol. 345, Issue 6197, pp. 626-628 DOI: 10.1126/science.1254287http://science.sciencemag.org/content/345/6197/626; “On Regulating Home Brew Opiates” KA Oye, C Lawson, T Bubela, Nature 18 May 2015 http://www.nature.com/news/drugs-regulate-homebrew-opiates-1.17563

Section III: U.S. Policy Options

The U.S. current enjoys significant advantages relative to China in terms of clusters of innovation, the openness of U.S. educational and research systems, and continuing utilization of talents of international students. The options offered below include policies that the U.S. should take to strengthen these advantages and wrong actions that the U.S. should avoid to avoid weakening these advantages.

A. Do – Recommended Policies

A1. Enhance data access and sharing while protecting privacy: At present, U.S. development of advanced therapeutics is impeded by limits on effective access to genomic, phenotypic and health care records and by the side effects of privacy protections on ability to curate data. The U.S. should consider adopting an "opt out" system modelled on Finland to enable more effective utilization and curation of data for purposes of medical research.[7] Considerations should be given to international pooling of data to enhance medical research.

A2. Address Security Commons Problems: The U.S. should expand current activities and initiatives directed at strengthening international norms and conventions that prohibit malicious misuse of biotechnologies, including the US Department of State Biosecurity Engagement Program, expand the institutional capacity of the UN Biological Weapons Convention, enlarge FBI programs with iGEM, and strengthen the Australia Group Guidelines with explicit attention to drawing China into the Australia Group.

A3. Address Environmental Commons Problems: The U.S. should expand current activities and initiatives directed at generating early information on potential environmental benefits and risks and fostering national actions and international agreements to mitigate risks.

A4. Address Pharmaceutical Licensing Problems: To improve management of safety and efficacy over the life cycle of drugs and to improve competition in smaller-and-smaller treatment groups, the U.S. should move toward adaptive pathways in pharmaceuticals licensing, based on FDA experience with Breakthrough Product Designation and accelerated approval and with Health Canada and European Medicines Agency experience with adaptive licensing pilots.

---

[7] "The next frontier: Fostering innovation by improving health data access and utilization," KA Oye et al, Clinical Pharmacology and Therapeutics, 10 September 2015 http://onlinelibrary.wiley.com/doi/10.1002/cpt.191/abstract.

A5. Expand Research Funding for Fundamental Research: DARPA, IARPA, NIH, DOE and NSF funding for applications of synthetic biology should continue with expansion of funding for the development of fundamental tools and methods and for work to assess environmental, security and safety risks. This should include strengthening and expanding the USDA-FDAEPA BRAG program.

A6. Implement Reforms of Coordinated Framework on Biotechnology: In 2016, the White House OSTP completed an evaluation of the Coordinated Framework on Biotechnology, with active engagement of industry, academia, regulators and civil society. Ongoing interagency consultations on unresolved matters should be continued.

B. Don't – Avoid these Policies

B1. Resist the impulse to extend DURC guidelines and to expand the scope of classification. Moving sensitive research behind closed doors would have the effect of limiting free and full evaluation of claims on benefits and risks of genomic research and would stoke concern over possible state led activities in tension with obligations under the UN Biological Weapons Convention.

B2. Resist the temptation to strengthen or weaken IPR protections. The current intellectual property rights system is of necessity an imperfect response to the complex tradeoff across creating incentives for investment through private ownership vs facilitating synergism through sharing. Both are requisites of innovation. Major adjustments to the IPR system are likely to increase ambiguity and uncertainty to the detriment of both private investment and synergistic sharing.

B3. Resist the temptation to limit the number of international students entering U.S. doctoral programs, to extend "deemed exports" and to cut visas for graduating students in a manner that would reduce the appeal of the U.S. academic-industrial complex to student immigrants. The current system has produced an extraordinary burst of innovation that has strengthened the U.S. economy.

OPENING STATEMENT OF EDWARD H. YOU SUPERVISORY SPECIAL AGENT, BIOLOGICAL COUNTERMEASURES UNIT, WEAPONS OF MASS DESTRUCTION DIRECTORATE, FEDERAL BUREAU OF INVESTIGATION

MR. YOU: Yes. So good afternoon. I'd like to thank the Commission on behalf of the FBI WMD Directorate for the opportunity to present. And I also appreciate the fact that I have the luxury of coming last to build upon the prior speakers.

So very quickly, to sort of set the stage, one thing I will put out right now, that the FBI is charged in protecting the United States from a biosecurity perspective, and one of the unique challenges right from the get-go is that for decades now when you talk about biosecurity, even to this day, most of the policy surrounds and focuses on pathogens, bacteria, viruses and toxins. And I think because we've narrowly defined what constitutes a potential biological threat has hampered us and has rendered us somewhat vulnerable, and which is one of the reasons why we're here today to testify, that we haven't have our eyes on the ball as where biotech is taking us.

So to start things off, with that in mind, to build off of what's happening in the biotechnology, basically everything that you heard today as far as the different applications, new pharmaceutical developments, new treatments, new therapies, all those are going to become incredibly data dependent, and so the hallmark of that is looking at things like the precision medicine initiative, and bear in mind that the way this is going to work is it's a straight-up statistics problem, is having, generating a large enough data set population scale, and then if you have an individual potential patient and requirement for treatment, you could pair that individual to that large pool to identify the similarities and differences, and that will dictate what the targeted therapies, what the targeted pharmaceuticals will look like.

So with that in mind, with everything you've heard, the bottom line is whoever has the largest, most diverse data sets of different populations wins the day. So with that, there's a stark security issue that we're facing. If you look at the historical aspects of the specific targeting of the healthcare sector and the cyber intrusions over the last few years, you're looking at tens of millions of U.S. individuals who have been impacted.

Many of those have been perpetrated by what has been identified, attributed to Chinese-based hacking groups. And, unfortunately, again, a different type of lack of security focus has always been on the potential loss of PII or the potential fraud angle. But what was truly disturbing is in some of those instances, there was actual penetration and acquisition of clinical data.

So that means that to the tune of potentially tens of millions U.S. persons, they have access to individuals' demographics, their medical state, what treatments are being provided, what pharmaceuticals are being administered, at what timeframe. So potentially unique insight into our ongoing clinical trial information, which renders all of that, the fraud angle, almost penny ante in comparison and the potential loss, not only in the clinical trial aspects, but if the future development of new pharmaceuticals at stake, then that's a treasure trove of information that could be built off of and exploiting both in commercial aspects, among other things.

But that's just the criminal acquisition of data. In this context, it doesn't help that we're also giving it away as well, too. So there are instances now of specific Chinese firms that with government support and private investments have set themselves up to be one of the largest DNA sequencing providers out there. So they sequence DNA. They provide other health diagnostic tests, and they do it well. They do it at scale, and I think that, most importantly, they do it the most cost effectively.

And as a direct result of that, many of our U.S. health institutions and academic institutions have partnered with some of these companies. So in the name of cancer research, diabetes research, autism, you name it, there's tens of thousands of samples being provided to these firms for sequencing, and, yes, our scientists, our clinicians get that information back for their own work, but at the end of the day, they have it too.

So if you do a retrospective of what happened and what is currently happening, the combination of the criminal acquisition of very valuable data over time so you're looking at insight into lifestyle information, family history, individual medical history, combined with, quote-unquote, "sharing of genetic information under legitimate practices," theoretically speaking, they're getting the whole ball of wax, and it's just a matter of time. It becomes a ticking time bomb on when they eventually overcome the analytical hurdle, they're off to the races.

And that poses yet another challenge in that existing agreements, things like trade regulations, export control, they don't work in this space. Your genetic information is not export controlled. It's not arms controlled. And even our existing trade agreements are all based on finished intellectual property or finished API, but now you're looking at data in residence that have yet to be realized.

Once the translation and the analytics come to determine how you design a therapy, how do you design a pharmaceutical, it's IP that has yet to be realized. So because of our lack of foresight, we're giving away the crown jewels without realizing it.

So some of the concerns we have are, are we undercutting the U.S.' ability to stay competitive? Are we inadvertently giving them the opportunity to corner the global pharmaceutical market? And to kind of expand upon these issues, the FBI partnered with the American Association for the Advancement of Science and the National Academies of Sciences, and we convened a series of meetings looking at expanding the themes of biosecurity, looking at where the future of bio-economy is going as far as data is concerned in these large data sets.

And I just wanted to share some of the comments that were provided by the stakeholders and experts that attended the meeting, that as I stated, there is currently no single entity within the U.S. government that has the responsibility or the capability to scope out what does this bio-economy look for for us. There is no articulable strategy on the biotechnology space.

And as a result of that, there's a lack of real understanding of who can holistically assess what are the vulnerabilities, what are the opportunities, and especially what are the security concerns that are going to be happening in this space, that the convergence of the life sciences with the cyber realm, the digital realm, renders existing policies challenged.

Do we need to revisit them? Do we need to make new ones? For example, HIPAA, the Health Information Portability and Accountability Act, is very good at securing information exchanged between two U.S. institutions without the explicit patient's consent. HIPAA doesn't quite apply when you ship data overseas, and a good example of that is another Chinese institution received, was accredited by the College of American Pathologists and got CLIA certification, rendering them accessible to get Medicare and Medicaid reimbursements, and as a result the entire state of California is looking at offshoring patient diagnosis testing. So, again, there's another incidence of potential U.S.-based information going overseas.

And finally, any holistic assessment that goes along with security assessments. Nowhere did the

FBI ever come to find the recommendation that we need to come to a full hard stop on any of this, that there's too much to be gained, there's too much beneficial applications at the health level, at the economic level, that this needs to move forward. What we're asking is that there has to be a concomitant parallel security endeavor that goes along with it.

So how do you resource and invest in the innovation but then also address the security as well too? So with that, I'll go ahead and close, and leave time for the questions and answers.

Thank you.

PREPARED STATEMENT OF EDWARD H. YOU
SUPERVISORY SPECIAL AGENT, BIOLOGICAL COUNTERMEASURES UNIT, WEAPONS OF MASS DESTRUCTION DIRECTORATE, FEDERAL BUREAU OF INVESTIGATION

"China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology"

Testimony before
The U.S.-China Economic and Security Review Commission

March 16, 2017

This statement describes the development of the bioeconomy within the United States and China, identifies the opportunities and security challenges facing the United States, and how the United States might better expand the scope of what is determined to be a biological threat and support biotechnology research and industry development for national security.

Background

The Federal Bureau of Investigation (FBI) is the lead law enforcement agency responsible for investigation of Weapons of Mass Destruction (WMD) threats. In particular, the FBI has authorities relating to the investigation, prevention, and response regarding individuals that attempt to obtain or use WMD materials, technology, and expertise. In 2004, the 9/11 Commission recommended that FBI create a new specialized and integrated national security branch to include agents, analysts, linguists, and surveillance specialists to cover the counterterrorism and counterintelligence missions. The WMD Commission Report, generated in response to the anthrax mailings, echoed this recommendation and the FBI responded by creating the National Security Branch (NSB). In 2005, the FBI Director assigned the newly formed NSB to design an operational element to meet the WMD threat. The Weapons of Mass Destruction Directorate (WMD Directorate; WMDD) was created in July 2006, consolidating WMD investigation and prevention efforts to create a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise focused on chemical, biological, radiological, nuclear, and explosive matters.

Advancements in biotechnologies have led to significant progress such as the production of synthetic microbial genomes and novel methods of pharmaceutical production. The capabilities of these technologies have increased by orders of magnitude over the past few years, and the costs associated with them have decreased by similar orders of magnitude. While these technologies offer amazing promise, they also remain inherently dual-use and just as applicable for nefarious use as reputable use. To that end, the FBI has established various initiatives and working groups, which include the advanced/emerging biotechnology initiative, which is a proactive approach to identify and mitigate current and over-thehorizon risks posed by the exploitation of advancements in research and development of scientific fields such as synthetic biology and genomics. The advanced/emerging biotechnology initiative has FBI partnered with synthetic biology companies to render resources and federal reach-back capabilities to evaluate uncertainties in commercial orders. WMDD is working to develop countermeasures, in partnership with scientific industry and academia, to prevent adversaries from acquiring and exploiting material and technology that may pose a national security concern. However, biological threat issues have historically focused upon the potential acquisition, development, and use of materials such as viruses, bacteria, and toxins. With the advent of new biotechnologies and the convergence of biology with the cyber/digital realm, current policies and practices to address biological threats may be challenged.

1. **Describe the current status of synthetic biology, genomics, and precision medicine research and applications. What is driving developments in these areas? How, if at all, are artificial intelligence, computing, and data storage playing a role in further advancements? How will advancements in biotechnology affect a country's health, food supply, global competitiveness, and military capabilities?**

Advances in synthetic biology have enabled microbial engineering and facilitated the ability to synthesize and sequence DNA at scale. This has led to the generation of very large data sets and the development of analytical tools as a means to leverage the information for research and practical health applications. The U.S. Precision Medicine Initiative (PMI) is a good example of the direct application of biotechnology and data. PMI is a long-term program that seeks to utilize population genetic data, biological samples, and diet/lifestyle information which are all linked to electronic health records. Research based upon the population data can:

- Advance pharmacogenomics, the right drug for the right patient at the right dose
- Identify new targets for treatment and prevention
- Test whether mobile devices can serve as diagnostic tools and encourage healthy behaviors
- Lay the scientific foundation for precision medicine for many other diseases and conditions

The potential positive impact of PMI to health and the economy has incentivized academia and the private sector to aggregate and agglomerate data from various sources as a means to recapitulate the PMI model. This in turn necessitates the investment and development of artificial intelligence, super-computing, machine learning and algorithm design capabilities as a means to analyze very large data sets and infer causal relationships. The results can then be used to design diagnostics and therapeutics which would benefit existing efforts to bolster national health, biodefense capabilities, and advance countermeasure development. The fundamental aspect of these activities is that the monetization of aggregate data has now transformed it into a significant commodity. However, the challenge is that existing legal frameworks focus upon protecting finished intellectual property or licensed/patented products, whereas large bodies of data, such as patient health records or genetic sequence data, represent near-term, unrealized development of products and applications.

2. Describe China's access to U.S. genomic data and biological samples. Is this access reciprocal for U.S. researchers and firms? What advantages and disadvantages does this access provide? How is China seeking to expand this access through legal such as joint partnerships or investments and illegal means?

China has gained significant access to U.S. genomic data and biological samples through research partnerships, investments, mergers, and acquisitions. An example of such access is the accreditation of a China-based DNA sequencing firm by the College of American Pathologists, and as a result, the State of California is now seeking to export patient samples to the firm for diagnostic processing. Moreover, the storage and transfer of patient health information are strictly regulated within the U.S. (i.e. Health Information Portability and Accountability Act [HIPAA]; Common Rule) preventing sharing of information without consent. Yet, the regulatory frameworks that are put in place to protect patient identity may not apply to the transfer of data overseas. And if breaches or indications of misuse of U.S. person data in an overseas entity are identified, there is no legal recourse for investigation or adjudication by the relevant federal government agencies (Dept. of Health and Human Services and Dept. of Justice).

The current financial environment in the U.S. has also incentivized research institutions and healthcare facilities to contract genetic sequencing services to Chinese or Chinese-affiliated firms. Several major Chinese firms have established genetic sequencing and analytics as a fee-for-service or entered into research collaborations. This has manifested into relationships between U.S. companies, universities, and healthcare facilities. The near term benefits for U.S. entities are realized through acquisition of data to support disease research, health diagnostics, genealogy studies, and personal health information. However, the long-term implications based on China's potential access to the same data (usage contracts notwithstanding) have not been assessed.

Cyber intrusions has had a significant impact on the healthcare sector, affecting millions of U.S. persons. Some of the major intrusions were attributed to China-based hacking groups. The subsequent investigations have focused primarily on the loss of personally identifiable information (PII) or the potential for fraud, as dictated by existing legal frameworks and current threat assessments (HIPAA). However, as described above, data incorporating health conditions, treatments, and diagnoses are qualitatively more valuable than financial/insurance information. Theoretically, the combination of genetic data through research collaborations, legitimate business agreements, and hacked information being exfiltrated to China would be the largest, most diverse dataset ever compiled.

3. Assess the emerging economic and national security risks from the bioeconomy for the United States. How is the U.S. government and industry seeking to address these risks? How successful have those efforts been? What are the remaining challenges? What risks, if any, does China pose to the U.S. bioeconomy?

In 2016 the Obama Administration officially launched PMI with an initial investment of $215 million. By comparison, China announced their own precision medicine initiative with the release of their 13th 5year plan which will dedicate $9.2 billion USD over a 15-year project. The asymmetry does not exist solely in program funding, but also access to data. As previously described, China may potentially have access to large scale U.S. genomic data through contract work, business partnerships, and research collaborations. However, personal information of Chinese nationals is closely guarded and not shared beyond limited release of very specific data (e.g. biomarkers, database of genomic structural variation [dbGaP]). This was reinforced by the passage of China's Cyber Security Law earlier this year which will provide the government more supervisory jurisdiction over cyberspace, defines security obligations for network operators, and enhances the protection of personal information. In the context of PMI, there is an almost direct correlation between the likelihood of success (i.e. statistical significance) and the size and diversity of the data sets that are analyzed.

Compounding the issues is the fact that biological data is not currently considered "security-related"; therefore, information, such as genetic sequences and electronic health records, is not covered by existing security regimes dealing with export and arms control. As a result, investments, mergers, and acquisitions of U.S. entities may not rise to the level of concern necessitating review and scrutiny for potential security issues (e.g. Committee on Foreign Investments in the U.S. [CFIUS]).

The lack of understanding the breadth and scope of the bioeconomy and the reliance upon the generation and aggregation of data has led to the potential asymmetry in access and capabilities which could impact overall security. If a proper assessment of the vulnerabilities is not conducted to establish the proper balance between protection and innovation, there is a theoretical risk that the U.S. may become marginalized in the global pharmaceutical market and cede the lead in innovation in the burgeoning and dynamic biological-cyber realm. This could have significant implications on the U.S. at the level of the individual, the economy, for biodefense, and overall national security.

4. **The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. Assess the implications of China's developments in biotechnology for the United States. What are your specific recommendations for legislative and administrative action?**

Since 2014, the FBI WMDD has identified the security issues involving the bioeconomy and has partnered with the American Association for the Advancement of Science (AAAS)[1] and subsequently the National Academies of Sciences (NAS)[2][3]to convene a series of meetings to further elucidate the current and future challenges. Comments regarding the bioeconomy and that were germane to the security issues were provided by meeting participants (these are not formal recommendations or

[1] https://www.aaas.org/oisa/aaas-fbi/bigdata
[2] https://www.ibpforum.org/resources/safeguarding-bioeconomy-applications-and-implications-emergingscience-meeting-recap

[3] https://www.ibpforum.org/resources/safeguarding-bioeconomy-iii-securing-life-sciences-data-meeting-recap

consensus statements):

- Currently, there is no single entity that has the responsibility to assess developments in biotechnology and the impact on the bioeconomy.
- A lack of understanding of the bioeconomy and a focus on biosecurity as it relates to only pathogens and toxins may have left potential gaps in assessing risk and asymmetric access to data.
- The convergence of the life sciences and data science will continue to challenge existing legal frameworks (e.g. HIPAA, export control).
- The holistic assessment of security implications of the bioeconomy must be coupled with activities that will promote U.S. innovation.

PANEL III QUESTION AND ANSWER

HEARING CO-CHAIR TOBIN: Thank you, gentlemen.

Now for the most interesting part, the questions. Mr. Wessel.

COMMISSIONER WESSEL: I found the testimony to be very interesting.

[Laughter.]

HEARING CO-CHAIR TOBIN: I did too.

COMMISSIONER WESSEL: Thank you all for being here. And Mr. You, please share the thanks of the Commission with the leadership of the FBI for authorizing you to be here today because it's a great help and deeply appreciated. You've helped advance the discussion.

Let me tie two things together, if I can, and Dr. Oye, I think you were referring to some of my earlier questions about students and some security risks, and Mr. You, you raised as part of your last comments that, you know, we're not trying to close the doors to the kind of broad international cooperation on science, medicine, et cetera. That's vital to the kind of changes, the kind of treatments, et cetera, that we're looking to promote over the years, over the coming years. That's vital.

At the same time, we have deep security interests, both national security and economic security that are at risk, and let me turn to that. Mr. You, we met a couple of weeks ago, and afterwards, I started looking to try and determine whether anyone had calculated the true value of the biotech, biopharmaceutical, the whole health welfare economy going forward, and I found dramatic numbers that go well into the trillions, if you will, over many years.

And we talked earlier today about robotics, high-performance computing, and many of these industries are really the future lifeblood or many are perceived to be the future lifeblood of this economy. Yet, all of them seem to be at risk through acts of omission and commission by this country.

Mr. You, you talked about this being a treasure trove, and as I look at the hacks of Anthem and others, you know, there have been questions raised as to whether it was going after PII or whether it was going after the underlying patient data, which seems to have a much greater value.

And we seem to be giving the Chinese the keys to that treasure trove both legally and illegally. What initial steps can we take--your comment about the state of California, not by active commission, just sharing the data, which can be then used for the kind of development activities that China may want to engage in. What other steps might we take that ensure the lifeblood of this, this sector in our economy, while also not threatening the kind of progress that we all want in the future?

MR. YOU: So thank you for that. I think it goes back to one of the prior recommendations, is until we do a proper assessment on what the, not only the opportunities but what the vulnerabilities are, then you can approach that question.

So, for example, one of the easiest things--I shouldn't say easiest--but one of the very first things is providing a very healthy caveat emptor, buyer beware, for the consumers. For example, some of those who are actually actively donating their DNA for diagnostic purposes or for genealogy purposes, some of those companies are being invested or outright acquired by Chinese firms, and there is no further dissemination of information to the end-user that that is going to be happening.

So that, it's no fault of their own. The companies may feel like that they're doing their due diligence, but until we get a healthy recognition that there are certain consequences and potential security vulnerabilities, we're not able to do that. And, again, at the same time, as I said, these are not, we're not talking about export controlled or ITAR issue materials or data, and so some of these investments and the outright mergers and acquisitions don't rise to the level of review at the government level, that if you think about the security consequences in this context, it may warrant further review.

But things like CFIUS, the Committee on Foreign Investment in the U.S., it probably would not raise a blip on their radar.

COMMISSIONER WESSEL: Well, but BGI, the transaction, 2013, if I recall of BGI and Complete Genomics, if I remember, some of those issues were raised, and CFIUS chose to still allow the transaction to go through.

Have we now passed a tipping point where that recognition is greater both as to the value but also the potential threats from bio-hacking?

MR. YOU: I think it's a bit of a challenge. I think even, I can't speak specifically to that particular transaction, but even at that time, it was looking at whether or not unique technology was at play and not looking at the downstream acquisition of data once you actually acquire the technology.

COMMISSIONER WESSEL: Right.

MR. YOU: So the technology in and of itself is not unique, but it does empower them to be able to then showcase their capabilities of DNA sequencing at an efficient and cheap way. So it's looking at the downstream, second, third order effects that may not come under review.

So that's something, again, it's somewhat unique in the biotechnology space because we're not talking about aerospace. We're not talking about missile technology. We're talking about your health records, your family medical history, your own genetics, and right now it doesn't warrant the same kind of scrutiny that other technologies do, and that already is a huge challenge.

COMMISSIONER WESSEL: Understand. Any others? No. Okay. Thank you

HEARING CO-CHAIR TOBIN: Thank you.

Commissioner Stivers.

COMMISSIONER STIVERS: Thank you. Thank you all for your testimonies.

There are a lot of concerns that come from all three of your testimonies, but I'm trying to break down what we need to worry about the most, and Mr. You, you speak very persuasively about the theft and transfer of biotechnology data to Chinese hackers, who I would presume would have to give it to those who can actually utilize that data, and there probably aren't that many firms that can do that on a large scale.

Dr. Oye, you talked about your concerns with non-state actors. I want to try to figure out what can non-state actors do with this kind of information if we're talking about the same types of information, and I might be missing something there.

Who should we be worried about in terms of non-state actorsis my first question. My second question is do we have any information about what Chinese firms (or whomever is getting this information) might be doing to protect this sensitive information from non-state actors or others?

Dr. Oye.

DR. OYE: Okay. A point of clarification. When Ed was talking about acquisition of information through the hacking, the potential uses of that information were not necessarily malevolent in the traditional sense of that. It's not necessarily developing a bio-weapon or something nasty or a dual-use virus.

In fact, it would be used for the development of therapeutics or for medical applications. It would create economic advantage for Chinese entities relative to U.S. entities. Is that fair?

MR. YOU: Yes.

DR. OYE: Okay. So when I was talking about non-state actors and danger, I was actually not referring to anything in the sphere that Ed was talking about.

COMMISSIONER STIVERS: Yeah.

DR. OYE: What I was talking about would be the potential not even for malevolent misuse but for people making mistakes, for messing up, for doing things with unanticipated adverse effects. If you take that infamous H5N1 mammal-to-mammal transmissibility, gain-of-function work, the danger there was not so much that Fouchier or Kawaoka were deliberately going to be trying to unleash on the world, but the people doing research in an area with that degree of sensitivity could make mistakes.

And most of the things that I worry about when I get down into particulars are people who aren't necessarily trying to do bad things. It's not the classic terrorist example but people working in areas with potential misapplication making mistake coupled to the possibility of malevolent misapplication as well.

And who would these people be? It could be ordinary groups working in laboratories on matters that are sensitive but not taking enough care with inadvertent release or it could be a medical team that is working on something, maybe control of rodents in Australia, but making the mistake and inadvertently turning those mice and putting them into a situation where they have absolutely no immune protection against a virus, and that happened for real in Australia.

And so there are a range of considerations which don't quite fit the classic bad guy terrorist trying to do ill and blowing up the whole world, the movie script stuff, which we also worry about, that are worthy of concern, and those are the situations, all of them, that require state-to-state cooperation in order to address them, and so it's a little bit different from the rivalry which we certainly have on the economics. It may be that on security affairs we need more cooperation.

MR. YOU: May I respond?

COMMISSIONER STIVERS: Mr. You.

MR. YOU: So to the heart of your question, though, also is that it all boils down to looking at identifying intent, and that is something that is not clearly covered because we haven't done that security assessment right now because, again, it goes back to my prior statement that we're focused, when it comes to biological threats, looking at who's developing that weapon, whereas here is something that is wholly biological in nature, but just because it's in data sets, it doesn't quite fit how we traditionally approach bio-security issues.

My hope is that if there's a broader understanding of these on the vulnerabilities that we can start asking those questions on where is the data going? Are there any indicators that it is going to be utilized that way? And for the fact of the matter, it's very difficult because for a lack of a better term, we're being killed by kindness because the most near-term downstream how it's going to be applied is you're going to probably see targeted healthcare.

Who else wouldn't want that? So if you see a global, you know, rise in the health care tide and floats all boats, that's the near-term benefit. But what's still lacking is what is a long-term strategic security implications for the U.S. if we suddenly become incredibly dependent upon an outside source for our future healthcare among other things?

And how that might also impact if there's a disparity between not only--there absolutely is going to be, looks like it would be a disparity, asymmetry on who's collecting and who has access to data even within the only U.S. because of the privacy limitations, whereas if somebody else is acquiring them, they're not, they're completely unfettered by the same privacy laws that we have here--for good reason--but if someone else has it, they're not bound by those same limitations.

COMMISSIONER STIVERS: Thank you.

Dr. Oye.

DR. OYE: So very quickly, one set of actions that we should consider in this country as a response to the issues that we've been treating are to address ourselves the problems with IP, the problems with our legitimate defense of privacy concerns and considerations, to foster or to enable more effective sharing of information by medical researchers.

The idea that it might be easier to steal information and analyze it in China than to do it here is a little bizarre. And there are policy issues that are associated with enabling the use of data for precision medicine and for discovery of advanced genetic therapeutics that are within scope.

COMMISSIONER STIVERS: Thank you.

HEARING CO-CHAIR TOBIN: Chairman Bartholomew.

CHAIRMAN BARTHOLOMEW: Thank you. And as always, thank you to our witnesses. It's interesting. It's like brain stretching to think about some of these things that you guys think about on a daily basis. I also want to thank all of you for the service that you've done working in the government and with the government, and Mr. You, in particular, thank you for your service. You could be making a ton of money out there in the private sector, and you have chosen to work on behalf of the people of the United States. So thank you for that.

Dr. Oye, a comment, and then I'll get to the thing, the issues, that I wanted to raise. But when you were talking about not worrying about non-state actors, I could not help but think about VX gas, and a month ago I would have felt a little bit more comfortable about what you are saying about non-state actors than I am today knowing that a state poisoned one of its own people with VX gas.

I'd like to take this in a slightly different direction, which is to talk about some of the kinds of restrictions that we have. You guys mentioned HIPAA. Anybody who has to deal with an ill relative in the hospital would be irate to know that they can't learn the information but the information can be shared with somebody overseas.

So one of my questions is does the Chinese government, for example, is there anything like HIPAA there? And we've talked about this a little bit also with drug testing. I mean the ethical questions that come up. Again, Dr. Oye, you talk about sort of the sharing of information, but we still haven't even resolved the Henrietta Lacks situation and how we have exploited information from somebody that they have never benefited from.

And then I'm just going to add sort of standard of care in labs. Are the Chinese, are you comfortable that the standards that the labs that are doing this kind of work in China are meeting the standards that we believe need to be met?

And then I'll add one more, which is IRBs. Do they have anything like an Institutional Review Board that is protecting people on whom some of these technologies will ultimately be tested? There's a kind of a competitive disadvantage for us, and I'm not--I'm not arguing that we loosen our regulations, but I'd like to understand more what, if any, they have in those contexts.

HEARING CO-CHAIR TOBIN: So let me just say you can take a little longer because there were a nested set of questions there that are all important.

DR. OYE: So let's actually start with your question on Chinese protections for privacy, and the answer is that they're a lot weaker. One little story that pops up every time that I talk to anyone in China about these issues is the story of a gentleman who took a test for a job, a state position, and, you know, there are thousands of applicants. He does well. He's one of the top three. They're required to take a physical. Part of the physical involves testing--genetic testing.

And the guy was denied employment because he had recessive gene for beta thalassemia, a blood disorder. It doesn't make any sense. Who cares about a recessive gene? And all the doctors only want to talk about that part. But the other part is that if you're sitting there in a position where you're considering allowing people access to genomic information, but it can be used against your interests, that's a case that would bother you a lot, and the fact that everyone I talk to in China knows the case.

It gets worse. This guy did something unusual. He actually took it to court. Now you might say that's an act of supreme stupidity, but he did, and he lost. And then he appealed it, and he lost. And nothing too surprising about the story except that we often think about our disadvantages, but in this instance, the freedom to behave in that manner has both a benefit and a risk; right?

The benefit is that people are free to use the data, but the risk is that you're going to be very cautious about cooperating if you believe that the information could be used against your interests so blatantly and so explicitly.

In terms of other protections, they're kind of weak. Okay. And, in fact, I think that we as a country have an interest, sort of like the old Nuclear Threat Reduction program. I think that we have an interest in working with China to be strengthening some of those protections, not just for reasons of leveling playing fields and economics, but also because more attention to the way that work is done and to adverse effects that may be created for individuals or for the environment or for security serves our common interests. We have a shared security interest in that.

There are a lot of other points that you raise, but I'll stop there and give time to my co-panelists and happy to return to your questions as well.

MR. SHOBERT: Maybe let me speak specifically to the lab infrastructure question that you asked and the veracity of the data coming out of it.

So when you look at specifically genomics and personalized medicine, one of the barriers to that really taking off and becoming more a productive area for the Chinese biotech community is that the lab sector is broadly speaking not trusted, and there were a number of studies done last year looking at specifically just NIPT, prenatal testing, and the data veracity numbers there were terrible, just really bad.

So there's--and that's relevant because personalized medicine is going to be most impactful when you can do a gene panel and you can actually take that information, tie that to a specific innovative molecule or innovative therapy, but for that linkage to happen in the first place, you have to trust that the diagnostic lab that you're interacting with actually is something that can be trusted.

Now that type of regulatory environment, the CFDA is very aware is a shortcoming, and it's working diligently to address that, and it likely will address that at a very individual basis when there's an economic trigger for doing it. So when the Chinese economy realizes that to get, if this proves to actually be an opportunity, to actually get the opportunity to be a global center where diagnostics are done, then the CFDA will pay a lot of attention to that.

But until that time, there are very basic predicate questions about the data veracity coming out of the diagnostic sector.

MR. YOU: And again to talk a little bit about the privacy aspects of it, as Dr. Oye mentioned, there's very little as far as individual rights, but there's also yet again an asymmetry in that I've outlined aspects of data going into China and theoretically whether or not it's actually being housed properly, but there's none coming out of China.

And that was reinforced in the passage of a law in January of this year, their privacy and cybersecurity laws, that it is almost impossible for any data on a Chinese national to leave their shores. So despite the fact that there are these services and partnerships that occur not only in the U.S. but with the European Union, with some of these prenatal test kits that go along with the genetics, there's a lot of data going over there, but you're not seeing very much coming out. And that, those that do come out is very limited in scope.

CHAIRMAN BARTHOLOMEW: So even if we could trust the data, we don't have access to it?

MR. SHOBERT: And that, if I could add just very quickly, that's an excellent point because that's where this question becomes a proxy for bigger conversations that we're having in D.C. about globalization.

And so to the extent that we can look at biotechnology, very specifically, and say is there an opportunity to take some of the things that we didn't do quite right about how we created market access conditions for Chinese companies here and what we ask for in return in China--

CHAIRMAN BARTHOLOMEW: Reciprocity.

MR. SHOBERT: Data. Data is really critical. And there's an opportunity in this sector specifically to use data as a proxy for some broader conversations that we need to have and to do it in a constructive way because the Chinese are very receptive to this. It's very sensitive. It's extremely sensitive, but to the extent we can resolve it and elevate it in the right way, there are all sorts of adjacent conversations we can have that are very beneficial, and we should view biotechnology as an opportunity to do that.

CHAIRMAN BARTHOLOMEW: I might have a second round.

HEARING CO-CHAIR TOBIN: Okay. Great. So many thoughts. Dr. Oye, I'd like to start with you. As you were giving your oral testimony, you made the point of talking about the rapid diffusion of biotechnology and went on to say that there's an advantage and a disadvantage.

One of the areas that you think of as an opportunity was--or a challenge--is for shared security, and your time was up. So can you expand on that and give us a sense of shared security, the United States and China, but also-- how do we protect ourselves from the very issues that Mr. You was talking about?

DR. OYE: So I'd begin with the last point made on reciprocity, and I do think, I believe in reciprocity in a situation where multilateral norms and rules are going to be hard to negotiate. Under those conditions, bilateral negotiation on equivalent treatment is I think an appropriate standard. When I put on my policy wonk hat, I actually did a book on the advantages of this approach under conditions where you don't have a consensus but maybe you can cut a deal that makes sense, and I would recommend that as a starting point. And that's one way to begin to address some of the concerns that my panelists have raised.

In terms of shared security, this is a slightly different proposition. Both the governments, the states, here and in China, I think have a common interest, a mutual interest, in seeing that people don't do stupid things or that lab safety issues are understood in a manner that's appropriate for new technologies that don't fit the old approaches.

You take gene drives or you take a number of the other advances that I was alluding to in the techo nerd part of the remarks, and frankly you look to lab safety procedures, you look to international conventions for governing what to look for when you're shipping stuff, and they don't fit. And we have an interest in working with a number of other countries, not just China, in standardizing and improving our handling of those risks.

Beyond that, there's also a potential educational mission, and I know you're thinking professors talking educational mission is sort of like MIT talking about the need for more research funding.

HEARING CO-CHAIR TOBIN: I see.

DR. OYE: But there is, in fact, a legitimate educational mission to be accomplished with students all over the world that are working in this space to improve their appreciation of the need for a culture of safety and security, and it's not something simple because the technology keeps wiggling around. So you have to almost build the culture because you can't do it legislating it piece by piece.

And this guy Ed You, who you may have heard of, actually has been doing unusual work with the FBI working to educate not just American students but students abroad in this international genetically engineered machine competition.

HEARING CO-CHAIR TOBIN: So I can't resist asking you a follow-on question. Have you challenged your students to think about laying out policies that would address this?

DR. OYE: I actually sometimes use that as a final exam question.

[Laughter.]

HEARING CO-CHAIR TOBIN: There you go.

DR. OYE: In a course that I teach.

HEARING CO-CHAIR TOBIN: There you go.

DR. OYE: And the range of answers that you get is interesting. In fact, the range of answers that you get across countries because our students come from everywhere are also kind of interesting. That's also one of the reasons I think that it's appropriate to be working very hard to improve understandings and awareness within East Asia, within Africa, the Middle East, South Asia. Western Europe is so aware that I don't think they need more education, and, in fact, I wish they'd stop talking about it so much.

HEARING CO-CHAIR TOBIN: Yes.

DR. OYE: But the answer to your question is that people come up with a number of novel approaches, and the U.S. government has been working in this space as well. The Department of State has a program that's intended to be raising consciousness and awareness. I mentioned Ed's activities as well. So we're not starting from zero in this space.

HEARING CO-CHAIR TOBIN: Great. Next generation is important. Yes, Mr. You.

MR. YOU: So I want to expand upon that, too, in that we've been doing a lot of outreach, as Dr. Oye mentioned, in the synthetic biology space, even with this growing sector of bio-hackers, you know, do-it-yourself biologists. But especially when it comes to where cyber and the life sciences are converging, we're finding some unique challenges, and that I've been fortunate enough to be a guest speaker at DEFCON--

HEARING CO-CHAIR TOBIN: Hmm...

MR. YOU: And I was just at South by Southwest yesterday.

HEARING CO-CHAIR TOBIN: Wow.

MR. YOU: And so you're having the coders--

--getting galvanized in that they either have been victimized or will be victims in this new coming age as far as their data, the data exhaust that they're leaving. And the first, at DEFCON, I was mobbed afterwards in a good way.

[Laughter.]

MR. YOU: I mean so picture this, at the end of my presentation I was mobbed by all these hackers, and they wanted to come up and ask can we help you develop solutions--

DR. OYE: Yes.

MR. YOU: --on this space?

HEARING CO-CHAIR TOBIN: That's great.

MR. YOU: Like maybe tying your genetic sequence to a block chain.

DR. OYE: Yeah.

MR. YOU: Things of that nature. So creative thinking. And then the second thing was do you want us to hack them back?

DR. OYE: That's always the case.

MR. YOU: Yeah.

CHAIRMAN BARTHOLOMEW: Don't tell us how you answered that.

[Laughter.]

MR. YOU: But the point here--no. Officially, no.

COMMISSIONER STIVERS: You need to have a hackathon.

CHAIRMAN BARTHOLOMEW: Yeah.

MR. YOU: But even at our National Academies workshops where we had good representation from academia, it also showcased that there's a need for a different approach and how we train our up-and-coming generation.

HEARING CO-CHAIR TOBIN: Right.

MR. YOU: That we have to overcome some of these stovepipes, that if you're a bio, a pre-med student, it's maybe worth your while to take a course in international policy, in foreign trade, that it's going to be taking something like that, and I would love to have a computer science student take some intro bio courses and vice versa because there are going to be unique challenges in each sector where they're rapidly going to be meeting one another.

And one of our keynote speakers called for maybe we need to have something like a federally funded research and development center, an FFRDC, just on the bio-economy alone because there's such an amalgam of all these different things that are happening right now, and our existing research centers and National Labs, again, is so focused on the parochial traditional approaches to biological threats.

So something needs to change and evolve to address some of the things that Dr. Oye just mentioned and some of the things that we're finding out through our engagements with this growing trend of these cyber biologists for lack of a better term.

HEARING CO-CHAIR TOBIN: I think Director Comey will probably be very pleased that you're attracting new talent.

Mr. Shobert, anything you want to say on that? Okay. I'll have a question for you next round.

Next we have Vice Chair Dennis Shea.

VICE CHAIRMAN SHEA: Thank you and thank you for being here and offering such really interesting testimony.

As you know, we've kind of neatly organized this hearing into various subjects--supercomputing, quantum computing, robotics, nanotechnology, now we're talking about biotechnology--but I assume as someone who knows nothing about this, and sort of looking in any of these areas in any great depth, that there's a lot more overlap in these areas than one would think, and, you know, advances in nanotechnology could lead to incredible advances in biotechnology.

So I was just wondering if you could explain to us how these various disciplines are actually working together and integrated. I think an ex-MIT geek named Ray Kurzweil called it "the singularity" or something, where all these various disciplines were converging into a single point.

But if you could describe how they complement each other?

DR. OYE: Okay. Briefly put.

VICE CHAIRMAN SHEA: Briefly put. In three minutes.

[Laughter.]

DR. OYE: If you take your first panel this morning on supercomputing, there's a direct connection between that panel and what we're talking about right now.

I can recall one of the people giving testimony talking about the mystery of Chinese computers that are ostensibly for weather forecasting but having additional capacity. And it's true it could be used for simulating nuclear weapons and other things, but I think that one of the most significant applications of supercomputing capacity will be analyzing extremely large data sets in the area of health because if you really are interested in doing precision medicine or detecting an association between a combination of factors in a health outcome, this is actually something that requires tremendous computational capacity and the data that Ed was talking about.

So that would be one area where a singularity begins to emerge. That said, I'm not sure I would support Ray Kurzweil's general proposition on infinite life extension coming soon.

[Laughter.]

VICE CHAIRMAN SHEA: Well, you have to pop about 270 pills a day to be able to get to the singularity.

DR. OYE: I will spare you the story of sitting next to Ray Kurzweil in an airplane--

[Laughter.]

VICE CHAIRMAN SHEA: We'll talk about it after.

DR. OYE: --discussing these issues.

[Laughter.]

MR. SHOBERT: One comment on this. So to build on what was just said, there's an outstanding question in the field of personalized medicine, which is, is this going--is this problem that we see being fixed with personalized medicine genomics, is it going to subject itself to just brute force, is once we load all this data and we develop these algorithms, is it just going to manifest itself with some measurement of time elapse, or is there going to have to be some really innovative thinking done in the context of that computational environment?

And so one of the questions that I'm most interested in is not just where is the data domiciled and is there reciprocal access to it by parties on both sides of the Pacific, but it's also going to be is there an ecosystem in the United States that is uniquely able to foster the kind of innovative thinking that's going to access that data and do something with it because we don't know exactly if it's going to reveal itself--these insights--purely through the brute force of AI?

VICE CHAIRMAN SHEA: We still have time.

HEARING CO-CHAIR TOBIN: Yes.

DR. OYE: Very quickly, I have a colleague named Manolis Kellis, and Manolis is a guy who--you were talking about where does this happen and how can it be done--okay--he is AI and biological engineering. And what he does with his AI part is to put together the genomic information, phenotypic information, and health care records, to be able to generate hypotheses on what to change, where the switches are. And then he tests those propositions using his skills in gene editing, creating cell cultures and modifying animals, and he's actually the guy who discovered what is called the obesity switch.

And it's a model of let's call it--it's not random walk AI. It's structured and focused searching in ways that take advantage of theories coming out of genetics and genomics, but it is AI and pattern recognition on a scale and with a sophistication that is rare. So it's taking place now, and there's going to be more and more of that coming.

That said, our policies for licensing the therapeutics are going to be evolving, typically precision addressing smaller and smaller treatment groups. We're not well set up to do that now in terms of the information required at the time of initial licensing and insufficient attention being paid to follow-ups or making use of data on experience of the drug in use to be updating and revising.

FDA is thinking through ways of streamlining the licensing procedures to take account of or be a better fit with the new generations of therapeutics. The Europeans, and, yes, even the Canadians are also moving in the direction of more progressive or adaptive approaches, but all this or other adjustments in policy that we need to do to enable innovation ourselves.

VICE CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR TOBIN: You just said a smaller group.

VICE CHAIRMAN SHEA: A lot more precision.

DR. OYE: Smaller and smaller treatments, yeah.

HEARING CO-CHAIR TOBIN: Okay. Thank you.

VICE CHAIRMAN SHEA: Yes, Mr. You.

MR. YOU: So very quickly, bear in mind, as I said before, whoever has the largest, most diverse data sets wins the day. You're going to need AI and quantum computing to get through the morass of data. One of the key challenges that a lot of experts say that by 2025, it's not going to be data generation, but with the advent of Internet of Things, the challenge is going to be data storage and curation. That's going to be the huge challenge for us.

And there's another asymmetry that you should also recognize, is, as was mentioned, there needs to be robust investment in developing the tools and the talent to overcome some of these challenges. Look at where--if you look at China's 13th Five Year strategy, they call out precision medicine. They call out big data analytics with an initial outlay estimate of $9 billion U.S. compared to when President Obama launched the precision medicine initiative a few years ago, the initial outlay investment was $250 million for the U.S.

So they're absolutely on a mission to not only generate the data capabilities but also to have the infrastructure and also to develop the talent.

VICE CHAIRMAN SHEA: But just to reemphasize this point we heard earlier, they get access to our data either through purchasing companies or hacking, but we don't get access to their data, and they have 1.4 billion people, which is a lot of data.

MR. YOU: Correct.

VICE CHAIRMAN SHEA: And I think this is a great insight for me that there should be, we, the Commission has in the past talked about reciprocity. I think we've been a leader in pushing that notion, that there should be greater reciprocity, and I have noticed that many organizations who did not push this concept before, such as the American Chamber of Commerce in China and other are now--reciprocity is now the word of the day.

But I think pushing reciprocity on data access is a really great insight from this hearing. So thank you.

HEARING CO-CHAIR TOBIN: Thank you.

My co-chair, Commissioner Slane.

HEARING CO-CHAIR SLANE: The medical researchers at Ohio State tell me that they have the ability to identify every gene in the human body. They can identify those genes that have the potential to create a disease, modify the gene, and essentially extend the life of a human being many, many years, and I'm thinking what are the ramifications in a country like China that has such an enormous demographic population and now this technology is just going to make their problem much worse?

MR. SHOBERT: So in my verbal comments that was--in my mind, that actual question that you're asking is essential to understand what China's intentions here are. So you have two tracks. Again, economic development, public health. And I think right now, as we understand state-of-the-art personalized medicine, we're still wrestling with exactly what the cost burden is going to be.

We don't know; right? And if that proves to be highly targeted but highly expensive at an interventional level, then it's not going to be effective for China in a public health capacity. Conversely, if in the next decade, we find that personalized medicine is actually very cost effective at a public--excuse me--in a population health level, and especially if that's tied to insights from big data around behaviors, if that, in fact, happens, then I think you'll see China double down on this investment.

But one of the triggers that could very well disengage the Chinese central planners from looking at this as a sector of growth is that if they just fundamentally cannot ever identify a way for personalized medicine to become a cost-effective tool within their own, the context of their own healthcare economy.

DR. OYE: You have to differentiate or distinguish between curatives and treatments. So the point that I'd really begin with is that if you're looking at the advances in personalized medicines or genomic medicines leading to cures that can actually lighten the burdens, even if the up-front costs are pretty significant.

The much discussed case of Gilead and the cure for hepatitis C is an interesting one because over the life cycle of the patient, that may actually reduce costs.

On the other hand, if you're talking about lots and lots and lots of treatments that address tinier and tinier treatment groups, the economics become difficult. And, in fact, you have a financing problem with cures, but you have an ongoing burden of expense. That has not been resolved in any society.

In Europe, the payers are trying to decide whether to pay for stuff. We're trying to decide whether to pay for stuff. And this is all stuff that goes beyond our current debate within this building on health care. This is the next debate that's coming because if we have access to therapeutics that do good things but they're very expensive, who will have access and under what conditions? And this is something that no society on the face of the earth including China has yet really managed to figure out.

MR. YOU: So with respect to Ohio State University, because I am a proud UC Irvine alum, although Chancellor Drake, you took our former chancellor to there, but that, that correlation of the genetics I would classify as a good first step because as precision medicine has really found out, the genetics is just the one angle. Now, you have the challenge of tracking lifestyle.

So it's the genetics versus and the environment. And that's where the bulk data becomes even more relevant, looking at individuals with similar lifestyle, life habits, diet, sleep, family history. All that has to be agglomerated to be able to come up with a good analysis.

I want to note that because it incentivizes gaining access to all kinds of different data to accelerate that. So suddenly people who may be wearing wearable technology to find out, you know, how much exercise they're getting, that suddenly becomes a different type of treasure trove information that on its, at first blush may not mean all that much, but as soon as you aggregate that combined with the genetics, combined with other things, suddenly you get some more value out of it.

Even some of the social media companies are getting into this because when you put an entry, it's time date stamped and geo-tagged, and that becomes a very powerful epidemiological tool so if there's an outbreak, you can track when was, who was that patient zero, what location, who else was there at what time.

But then you can also translate that to other potential health applications because you're tracking people and their behaviors. So it's looking also, if you look at the bio-economy, it's not just genetics, it's not just health records, but very disparate sources of data suddenly become very attractive, and until we do that security assessment, we don't know what suddenly becomes vulnerable.

HEARING CO-CHAIR SLANE: At the end of the day, guys, this technology is going to extend the lives of human beings and all of the social ramifications that that presents.

MR. YOU: Oh, this may be--so you can cut me off at the time--but this also came up in one of our bio-economy meetings with the National Academies, is that there's going to become an even more dependence on somewhat finite resources, and the aspect of renewable sources of food, energy, manufacturing capabilities is going to become more and more relevant.

And if you think about it that way, by extension, this takes synthetic biology to a whole other level. Then you're going to need biodiversity and pure biomass, changing vegetation sugars into petroleum-based chemical replacements or food replacements or additive manufacturing.

This becomes suddenly an interesting downstream foreign policy interest because right now most of our focus is on petroleum-based economies. But if you're looking at who in the near future or in the very far future has access to very large biomass and biodiversity, suddenly the entire Southeast Asia becomes very attractive and potentially very lucrative.

And to that end, if you're going to have a longer living society that's going to be completely dependent upon renewable resources, then we should be looking at strategically speaking where we engage and how we invest.

HEARING CO-CHAIR TOBIN: Okay. Are we all set?

HEARING CO-CHAIR SLANE: Thank you. Yeah. Thank you.

HEARING CO-CHAIR TOBIN: Terrific. So now we're going to do somewhat of a lightning round, but three of our commissioners, not too fast, just a steady roll.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you.

And Mr. You, I certainly agree on the need for an assessment and, you know, the discussions we've had here, you know, are going to confound policymakers for a while. But in the interim and in light of current politics and policy, it feels like we're outsourcing our security and outsourcing our jobs.

We are putting at risk the future U.S. leadership here, and in the industry, as well as, you know, if we're allowing California to send its Medicare and Medicaid data, which is subsidized by the federal government, we're using U.S. taxpayer funds to support jobs in another country, something that I've heard some of our political leaders say is not something we should be doing.

So correct me if I'm wrong in that assessment. But also you've been at South by Southwest, you know, the others of you, you know, this is not the first time you've had this discussion. Is that assessment ongoing? Is there at the senior levels of government a discussion? We're a U.S.-China Commission so we're not looking at the future of healthcare globally and what the rules on HIPAA, et cetera, should be, but rather than impact on the bilateral relationship. In other venues, is this discussion reaching a fever pitch?

DR. OYE: No.

MR. YOU: No. But having said that, though, I want to express my thanks for this opportunity because, again, from the FBI WMD Directorate standpoint, our mission is focusing on the biological modality, and what we've identified is this potentially huge opportunity in biotech but then also a parallel huge vulnerability, and it just so happens that China is one of the biggest players in this space.

So if anything, the challenge for us is that, historically speaking, as again I'm sorry if I'm repeating myself, but when it comes to biological threats, the tendency is always to focus on the pending engineered virus or just general global health security, which is, I don't mean to play it short shrift, but because of the focus being almost entirely on that angle, we've rendered ourselves to be blindsided in this other aspect.

So I completely agree that this needs to be a whole-of-government assessment that occurs because we are in the middle of overcoming our own existing silos because if there's no specific bio WMD so then I may end up getting referred to cybersecurity. Cybersecurity may then refer me to economic espionage. Economic espionage may reroute me back to WMD. And that's just how the things stand right now.

So until, again, there's a broader understanding and appreciation of where biotech is taking us, there needs to be a more holistic approach to address the issue.

DR. OYE: There have been repeated inquiries into the development of a national bio strategy, and they always end the same way. Badly. Okay. Even reforms of basic regulations, the Coordinated Framework, no follow-up. We'll see what happens.

Your question really does--it's very important. And the answer, you notice that all of us are sort of nodding no as soon as you asked the question. I don't want to be too pessimistic about it. The significance of this sector is obvious. And it shouldn't be something that is a partisan issue. And it's something that does require, and it's not just bipartisan attention but integrated attention because the pieces that have to be put together here are incredible. I mean Ed has made the point very clearly.

The other point I think is also linking the long-term to the short-term. You know we were talking, for example, about the policy issues on data, and we talked reciprocity, but again how do you frame that issue of reciprocity in a way that is sensitive to American interests narrowly put but also to a global interest in pooling that data in a way that is essential to discovery of advanced therapeutics improving health outcomes?

And in a sense, I think that this is a prime area where you can take the points of potential competition but there's a big mutual interest sitting there that might be a better way of framing it with a little bit of a push along the way to be clear, but to get there long-term, we're so far from that right now.

And I just want to applaud you for pulling together folks, and I'm not just talking about the panel, but the Commission, to be raising these issues and concerns, long-term global and national.

MR. SHOBERT: Not on the national security front but on the economic development front, where it is reaching a fever pitch is at the gubernatorial and at the state level, and the reason for that is if you're a mayor or you're a governor, you've seen a lot of your traditional manufacturing sector disappear. You've built your convention center in your tier one city, in your state, and protecting your biotech community is really important.

And so where you are seeing a high level conversation is at the state level, at the governors, at the mayoral level, where people are saying what do we have to do to make sure that the next round, the next tranche of investment in biotech happens here?

DR. OYE: But what's going on at that state and local level is nothing more interesting in some ways than the old we're going to cut you a tax break in order to get your investment here. And the discussion has to be better than that.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR TOBIN: Commissioner Bartholomew.

CHAIRMAN BARTHOLOMEW: Thank you.

I'm going to sound really old-fashioned here because we talk about data, but the data starts somewhere, and it starts with the people who the data is coming from, and one of the things I'm concerned about is the ability of the Chinese government because of the nature of China's political system to coerce the population. I mean there are some alarming reports, for example, that Uighurs, young Uighur men, are being arrested and they're being blood-tested.

Now they're being blood-tested primarily, people believe, actually for organ harvesting, but it's still a gathering of data against people's will or against--they don't have any choice of saying no, and I will note of concern is that the House healthcare plan actually would allow employers in this country--it has a clause that would allow employers in this country to mandate genetic testing and turn those results over, which for me personally is going in the wrong direction.

But how, have people just walked away sort of from the ethics of all this because I know we're talking about data security, and we're talking about all the good things that can be done with data as well as some of the bad? But what about the ethics of taking the data from people in the first place?

DR. OYE: Great question. The answer is complicated. I know that's typical of academics; right?

[Laughter.]

DR. OYE: But there are two things that are going on. One is your trust or lack of trust in the institutions, public and private, within, that define your environment. And the other is the issue of, well, how do you want your data to be used? Okay.

So I'm going to point to a tiny little country called Finland, and it's an example actually of a place where these issues have been managed pretty well. What goes on in Finland with reference to data is that they have a system where unless if you opt out, you're in. And that means that the healthcare records, the genomic information, all the stuff that you want to be combining for purposes of medical research, is available unless if you say no.

Now, in practice, whenever you go to that kind of an opt-out system, very few people say no. Okay. And in Finland because people have this peculiar property of trusting their state and institutions, the rate of refusal is very low, and Finland occupies a very interesting place because they're actually a leader in terms of genomic medical research.

This raises a big question. In China, would you say no? I think I'd be more inclined to say no in China than I would certainly in MIT medical.

CHAIRMAN BARTHOLOMEW: Only if you felt that you had the freedom to say no.

DR. OYE: And that's the other issue.

CHAIRMAN BARTHOLOMEW: Because there are consequences.

DR. OYE: Because your point is coercion in the larger sense. People are trying to reason through these problems. The ethical issues that are associated where compulsion is sitting there, be it in the United States--and that legislation is problematic--or in China is entirely fair.

The Finnish solution works well if you actually have a situation where you're not being compelled and where there is this basic trust in institutions that even we don't have.

HEARING CO-CHAIR TOBIN: Our last question and--

CHAIRMAN BARTHOLOMEW: I think Mr. You had some--

HEARING CO-CHAIR TOBIN: Oh, excuse me.

MR. YOU: So just a couple of challenges based on that, too, is that sometimes we're so focused on the immediate return, the benefit that you glean, that maybe it's okay for you to give up a blood sample or a cheek swab for the DNA sequencing is because you get an immediate return on that contribution. But what's lacking, it goes back to that caveat emptor, that data stays in residence, and you don't know--we're not set up to determine how could it potentially be used later down the line.

That aspect is very difficult to not only assess the ethics component, but I will call out, too, that as far as looking at law enforcement, you know, right now we have the biological weapons anti-terrorism statutes, you know, Title 18, Section 175, and I'm a good agent because I know that by heart.

[Laughter.]

MR. YOU: But again that is still focused only on the misuse of biological agents--a bacteria, a virus, toxin or delivery system for use specifically as a weapon--but now we're talking about a very near future where there potentially could be biological extortion, exploitation. Think of the OPM hacks; now compound that with biological information. If an adversary knows what your potential medical fate might be or those of your family members or your children, and that then could be leveraged against an individual, the policies and even some of the criminal statutes for agencies like the FBI or law enforcement in general to exercise that is going to very much challenged in that future too.

So it's not just the ethics, but even when you have an overt criminal act, it may be very difficult to be able to respond to it.

CHAIRMAN BARTHOLOMEW: Thank you.

HEARING CO-CHAIR TOBIN: Thank you.

Commissioner Stivers, and then after that, I'll have a few closing remarks.

COMMISSIONER STIVERS: Thanks.

Let me, since I'm the last question, let me try to enlarge this a little bit, especially in terms of what's going on in China. Mr. Shobert, you've done a lot of work on aging in Asia. I read a statistic recently that in the next 20 years, China's median age is going to rise an eye-popping nine years to 46 years old.

By comparison, we worry about the baby boomers retiring here, and the U.S. median age is going to go up by about two years during the same timeframe. So China has some serious demographic issues that they're very concerned about trying to deal with in the next 20 years in terms of their population.

And Mr. You, you mentioned a couple times now that whomever has the data wins the day, and I think we have a lot of concerns about what anyone would do with all of this data, whether it's the Chinese government or our government or any kind of firm.

And so can you kind of explain what's going on domestically in China on this issue? Why these issues are so important in China? And then maybe to play a little bit of a devil's advocate here from the discussion we've had, if a Chinese firm uses all this data to produce some sort of great health outcome or cure for something, isn't that a good thing? I mean aside from the theft and the compulsion and those things that are obviously wrong. But if they can use these massive amounts of data to produce a positive health outcome for the world, should we be concerned about that or not? Or is that a good thing?

And then Mr. Shobert, the question about Chinese demographics and why this is important to them?

MR. SHOBERT: Yeah, so Tom Barnett has famously written that no country in the history of human kind will ever get as old or as rich as fast as China is going to. My caveat to that is that getting old is a demographic certainly. Getting rich is not.

So the challenge for the Chinese economy is to continue to create enough top level growth that the current healthcare system with some minor stimulus to specifically take care of the rural and urban poor, that the overall economy still continues to grow at such a rate where people can afford to pay out-of-pocket for healthcare and age- related services.

So at the highest level in the Chinese government, one of the basic concerns that they have is not just the transition from manufacturing to services; it's also making sure that the economy continues to grow in a way that those downstream positive effects can be created, and that those accrued healthcare liabilities that are specific to aging can be paid for.

China by 2050 will have more people with Alzheimer's than we have in the entire United States--okay--so to give you a sense of the scale of the problem. And they have currently 50 dementia care facilities across the country, and those are very, very, very remedial. So they have an overarching need to develop sectors of the economy that continue to hold the promise for future growth.

So if you're going to try and construct an overarching narrative that encompasses our discussion today, it's finding high-technology sectors that have the ability to continue to incentivize the economy's growth and to create higher-wage jobs.

Your second question, is this a good thing, yeah, it should be. And I think to the extent that right now we have a little bit of cynicism about globalization in general, there's reasons to look at biotech and say there are good things that could very well come out of China, but a lot of the concerns that have been voiced today do need to be addressed, and they need to be addressed in a timely fashion because this is an industry that moves very quickly.

COMMISSIONER STIVERS: Thank you.

Dr. Oye.

DR. OYE: I'd like to see, to take that question, is it a good thing, and the answer is that if people discover a cure for cancer or a cure for these tiny little personalized problems, it's good.

The issue that it raises in American context is who's or how much do we pay for those cures and access to those cures? And I'm going to put my co-panelists on the spot. I know we're not allowed to do it this way. But you were talking about India and Brazil and compulsory licensing. And the question that I want to ask to you is that if China came up with a cure for cancer, how long do you think it would take for us to engage in a wee bit of compulsory licensing if they were asking a lot for it?

[Laughter.]

DR. OYE: I also want to note that in this very room, I believe, Senator Schumer began talking about the need for compulsory licensing of Cipro during the anthrax scare because Bayer wasn't producing it fast enough. But--

MR. SHOBERT: You could use the minute hand on your watch.

[Laughter.]

COMMISSIONER STIVERS: Thank you.

Mr. You.

MR. YOU: I'll caveat my response with two things. One is you just outlined that anywhere else in the world where there's an absolute incentive to make this happen, you've just heard it. There's enormous pressure to be able to address some very near-term risks for that part of the world. So there is a huge need and a huge push to overcome some of these immediate challenges.

And then also the other caveat is, again, the FBI recognizes that all of the things that we've just articulated, especially with precision medicine--and by the way, precision medicine, as I said, is just one really powerful proof of concept--there's a lot of activity happening in other parts of academia and the private sector looking at what other data holdings do they have and how can those be monetized and leveraged. And most of the near-term application is in health.

So with all of that, we need that to happen, but, yes, if there is a global increase in health and quality of life, absolutely, that's a good thing. But I would classify that a near-term issue, and I'll take Dr. Oye's comments one step further, is how much will that cost? And I'm not talking about at an individual level.

If there is an overall increase benefit in health, is it okay if the U.S. is second or third fiddle on the global pharmaceutical stage? Are we okay with that? Is the U.S. from a national security standpoint okay with being completely reliant on another source of potential healthcare or health innovation or pharmaceutical innovation? Are we okay with that?

So it does pose that we need to be asking what the second, third order effects are going to be based on this. It's one thing to look at the immediate application and what the benefits are, and some of the costs and risks are going to be somewhat self-evident. But we need to take a step back and look at what are the further downstream impacts going to be? Because these are the questions we're asking for today. We need to ask where is the technology going to take us five years from now? Ten years from now? 20 years from now? It's going to be a completely different environment.

But the data is going to be the same. What's going to be different is how we're able to analyze that data and then turn that around into a useful application.

COMMISSIONER STIVERS: Right. Thank you.

HEARING CO-CHAIR TOBIN: Mr. Shobert, Dr. Oye, Mr. You, this has been outstanding. Thank you very much. We really appreciate your testimony.

We're grateful to all our witnesses today. The Commission and guests online and guests here in the audience leave with a much keener understanding of where China is going with their technology initiatives, all of which are supported by the PRC's 13th Five Year Plan and the associated funding.

And you've got us started in thinking about the implications and what we need to do in these same sectors.

I want to echo what was said by Commissioner Slane--special thanks to Katherine Koleski--right here--who is the research director and a policy analyst on the Commission's economics and trade team. She worked closely with Commissioner Slane and me and with our witnesses to make this hearing possible. We're very grateful for her commitment to and her expertise on these new technologies. She's as passionate as you are, and thank you so much, Katherine.

We stand adjourned.

[Whereupon, at 3:16 p.m., the hearing was adjourned.]