

[H.A.S.C. No. 115-63]

**CHINA'S PURSUIT OF EMERGING AND
EXPONENTIAL TECHNOLOGIES**

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS
AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
JANUARY 9, 2018



U.S. GOVERNMENT PUBLISHING OFFICE

28-966

WASHINGTON : 2019

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ELISE M. STEFANIK, New York, *Chairwoman*

BILL SHUSTER, Pennsylvania
BRAD R. WENSTRUP, Ohio
RALPH LEE ABRAHAM, Louisiana
LIZ CHENEY, Wyoming, *Vice Chair*
JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
(Vacancy)

JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
STEPHANIE N. MURPHY, Florida

PETE VILLANO, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Langevin, Hon. James R., a Representative from Rhode Island, Ranking Member, Subcommittee on Emerging Threats and Capabilities	3
Stefanik, Hon. Elise M., a Representative from New York, Chairwoman, Subcommittee on Emerging Threats and Capabilities	1
WITNESSES	
Carter, William, Deputy Director and Fellow, Technology Policy Program, Center for Strategic and International Studies	7
Cheng, Dean, Senior Research Fellow, Asia Studies Center, The Heritage Foundation	4
Scharre, Paul, Director and Senior Fellow, Technology and National Security Program, Center for a New American Security	6
APPENDIX	
PREPARED STATEMENTS:	
Carter, William	66
Cheng, Dean	41
Scharre, Paul	51
Stefanik, Hon. Elise M.	39
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
[There were no Questions submitted during the hearing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
[There were no Questions submitted post hearing.]	

CHINA'S PURSUIT OF EMERGING AND EXPONENTIAL TECHNOLOGIES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, January 9, 2018.

The subcommittee met, pursuant to call, at 2:00 p.m., in room 2118, Rayburn House Office Building, Hon. Elise M. Stefanik (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, CHAIRWOMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. The subcommittee will come to order. I would like to welcome everyone to our first subcommittee event for 2018. Today we will examine China's pursuit of emerging and exponential technologies and the resultant impact on U.S. national security. This is a critically important topic and will inform our future hearings, including the science and technology budget for the Department of Defense [DOD] and the continuation of the reform and innovation efforts this committee has promoted over the past several years.

Our committee, and ETC [Emerging Threats and Capabilities] Subcommittee in particular, has most recently reviewed in detail China's advances in cyber capabilities and information warfare, and also monitored their development of advanced weapons systems such as hypersonics and directed energy [DE]. But this hearing today will take a broader focus and touch on many of the newer technologies that China is investing in to support their national objectives.

China continues to increase their research and development investments at an alarming pace and is rapidly closing many of their technology gaps. More and more we see China using only domestic Chinese firms and creating high market access barriers to support domestic capacity. The effect is to replace any and all dependency on foreign companies, investments, and technologies.

Aside from the obvious economic benefit of China being able to create millions of high-paying, high-skilled jobs, there are also obvious national security implications should they corner the market on advanced technologies critical to national security. We also see them aggressively moving to acquire enabling commodities such as data, and current trajectories have China on track to have roughly 30 percent of the world's data by 2030.

Many of China's published national level plans, such as achieving dominance in artificial intelligence [AI] by 2030, indicate a top-

down government-driven agenda that provides a roadmap for strategic collaboration between industry, academia, and their civil society. These plans, when combined with resourcing effort and patience, may propel China to leap ahead in many of the technology sectors we will talk about today.

Most notably China's leadership appears to recognize the connection between the development of many of these advance technologies and economic growth. This is something we should remind ourselves of as we continue to examine this important topic. Perhaps it is a lesson we need to relearn amidst our debates on sequestration and continuing resolutions.

But China's dominance in many of the technology sectors we will discuss today is not a foregone conclusion. What we learn today and in future hearings must be translated into action to inform and reform the Department of Defense in support of national-level efforts so that the United States remains home to the world's leading experts, researchers, and technological breakthroughs.

Today's hearing is also timely because of the organizational changes currently underway in the Pentagon, namely the reestablishment of the Under Secretary of Defense for Research and Engineering [R&E]. I firmly believe that the Under Secretary for R&E needs to be the prime mover to drive change and foster innovation within the Department. A primary mission of this office should be to provide distinct direction and leadership to energize the defense industrial base, the military services, the Department of Defense labs, and to guide even newer initiatives such as the Strategic Capabilities Office [SCO] and the Defense Innovation Unit Experimental, or DIUx, the Defense Digital Service, and the Algorithmic Warfare Working Group.

And while many of these newer initiatives have created tremendous momentum and energized a conversation about changing the culture of the Department of Defense, much more work needs to be done to make these more than one-off quick gains

If properly empowered and resourced, I also believe that the Under Secretary for R&E will be in a unique position to drive a national-level dialogue for science and technology [S&T] policy that will, in addition to helping maintain a battlefield advantage, energize our domestic industrial base, and provide technology jobs and opportunities across many of the sectors we will talk about today.

So therefore, we have significant expectations of Dr. Mike Griffin, the nominee to be Under Secretary for Research and Engineering, but we do so while also offering him our support and confidence because the threats we face from China and others demand that we energize and organize our government to ensure that policy keeps pace with technology in order to define a national science and technology strategy and to close the gap with China.

To guide us through this important topic of China's pursuit of emerging and exponential technologies, we have before us a panel of experts: Mr. Dean Cheng, Senior Research Fellow with the Asia Studies Center at The Heritage Foundation; Mr. Paul Scharre, Director and Senior Fellow with the Technology and National Security Program at the Center for a New American Security; and Mr. William Carter, Deputy Director and Fellow with the Technology

Policy Program at the Center for Strategic and International Studies.

Welcome to the three of our witnesses. We look forward to hearing your testimony, and now I would like to recognize my friend, the ranking member, Jim Langevin of Rhode Island for his opening comments.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 39.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Madam Chair, and I want to thank the witnesses for being here today. I am looking forward to your testimony.

The members of the Emerging Threats and Capabilities Subcommittee have long been champions for Department of Defense investments in emerging technologies to advance U.S. warfighting and deterrence capabilities. Congress recently restructured the DOD to create an Under Secretary for Research and Engineering to enhance the Department's ability to foster and harness innovation, and Congress has also provided significant funding and authorities for progression of R&D [research and development] and prototypes including other transaction authorities.

DOD has also made several efforts on this front. The Strategic Capabilities Office, as the Chair mentioned, DIUx, and the third offset strategy are just a few of the recent initiatives that are working to ensure that our warfighters are never sent into a fair fight by providing them with the very best tools and capabilities that are available.

But despite significant efforts by Congress and the Department, other nation-state actors have made advances of their own in emerging technology areas that endanger and in some cases obviate U.S. technological superiority.

Today's witnesses will provide us with their insight on China's technological advancements and how such advancements impact U.S. national security. I am particularly interested in hearing about China's advancement in hypersonics, artificial intelligence, cyber tools, and directed energy. Application of these technologies in the battlefield are absolute game changers in the areas where I believe the United States must maintain its superiority.

In addition to insight on China's specific technological advancements it is important to understand what strategy, practices, policies, and investments China has employed and what they have exploited to achieve parity with or superiority to the United States.

In addition, it should trouble us all that the Organization for Economic Cooperation and Development has predicted that China could overtake the United States in total R&D spending by 2019. Such an understanding will allow us to fine-tune our own strategy, policies, and priorities, and investments to maintain our technological edge.

That said, I believe it is imperative U.S. strategy be holistic in nature, one that fosters technological superiority as opposed to a strategy that simply attempts to counter one country's activities. It

is equally important that the U.S. continues to promote collaboration and sharing, rather than closing ranks in alienating the global S&T community. We must also focus on the future of our S&T workforce and promote education in the STEM [science, technology, engineering, and math] fields of science, technology, engineering, art and design, and mathematics.

So with all of that said, in closing, I just want to again thank our witnesses for being here today before us on this important issue. I look forward to your testimony, and with that I yield back.

Ms. STEFANIK. Thank you, Mr. Langevin. I ask unanimous consent that nonsubcommittee members be allowed to participate in today's hearing after all subcommittee members have had an opportunity to ask questions. Is there objection? Without objection, nonsubcommittee members will be recognized at the appropriate time for 5 minutes.

Thank you again to our witnesses for being here today. Mr. Cheng, I will start with you for your opening statement.

**STATEMENT OF DEAN CHENG, SENIOR RESEARCH FELLOW,
ASIA STUDIES CENTER, THE HERITAGE FOUNDATION**

Mr. CHENG. Chairwoman Stefanik, Ranking Member Langevin, distinguished members. My name is Dean Cheng. I am the senior research fellow for Chinese political and security affairs at The Heritage Foundation. I want to thank you for the opportunity to testify before you this afternoon. Let me note here, however, that my testimony reflects only my own views and do not represent the views of The Heritage Foundation.

To begin, it is essential to recognize that the PRC [People's Republic of China] sees itself as competing with the United States in the Information Age. What this means is first that China is competing with the United States in a long-term struggle for ultimately political supremacy, but that is founded upon economic and technological bases. This does not preclude cooperation with other countries in pursuit of economic benefits, but it does require recognizing that China sees this ultimately as a political struggle. And by the Information Age we mean that the currency of power in the Chinese view is information as much as the amount of the electricity generated or the steel smelted was the foundation for power during the Industrial Age.

Information dominance is the key to the Information Age in the Chinese view. This means the ability to gather, to generate, to transmit, to assess, and to exploit information more rapidly and accurately than others. And this is all reflected in the broader concept of "comprehensive national power (zonghe guojia liliang)," which includes military, economic, and cultural aspects, but also the level of the nation's science and technology base.

It is important to recognize the aspect of comprehensive national power because it reflects the reality that China is engaged in a whole-of-society, not simply a whole-of-government approach to this competition.

In terms of science and technology, the top Chinese leadership has long recognized the central role of S&T and innovation in this competition. There have been longstanding efforts dating back three decades beginning with Plan 863, which was approved by

Deng Xiaoping. This is a sustained effort that every Chinese leader has supported. Various strands to this effort reflecting the comprehensive approach includes improving Chinese universities; leveraging foreign investment through things such as mandatory joint ventures or the requirement to set up R&D campuses in China; economic espionage, including by governmental entities as reflected by the DOJ's [Department of Justice's] indictment of PLA [People's Liberation Army] hackers; and increasingly including the funding of foreign technology development, as well as outright acquisition.

As China's science and technology base has improved, China is increasingly competing as a technology developer, not simply a technology acquirer. Where in the past there has been perhaps more emphasis on legal and illegal acquisition of technology, now China is developing technology on its own, which means both a reduced time lag and a greater ability of China to set the very terms of the technology debate.

Increasingly we see China developing technology as fast or faster than the United States. The fastest super computer in the world, the top two, in fact, are both Chinese. And the Sunway TaihuLight, the number one in the world, is entirely powered with Chinese-manufactured microchips. China was the first to deploy a quantum communication satellite and has engaged in longer distance quantum encrypted communications than any other country.

The national security implications of this I would hope are obvious. The level of competition means that from the Chinese perspective improving the economy and S&T base benefits the military, while the military is available as part of the larger effort at strengthening the economy.

In the context of information dominance this is a very broad set of concepts which goes beyond cyber, and therefore, touches on an enormous array of technologies. When the Chinese talk about improving information gathering, we are not talking about just cyber, we are talking about space capabilities, including countering potential adversaries through things like ASATs [anti-satellite weapons], as well as jamming.

Information monitoring, supercomputers, even genetic information. Information transmission improvements include quantum computing, 5G, better processors. Information exploitation includes artificial intelligence, virtual reality, and augmented reality. Information protection includes things like quantum encryption and inoculating the Chinese people through instruments such as the Great Firewall of China.

It is important, therefore, when we think about the future and the possible policies that you, the Congress, may help pursue to recognize above all else that from the Chinese perspective innovation comes in many different forms. We, as Americans, tend to focus on technology specific innovation individual items, but there is also innovation in production processes. Japan's competition with the United States in the 1980s was not that they invented the VCR [videocassette recorder]—they didn't; it was the United States—but in the ability to manufacture them by the container shipload with low failure rates. Toyota, the machine that would go of itself is another example of production innovation.

Doctrinal innovation, the German blitzkrieg harnessed known technologies in different ways. And finally organizational innovation. We see this with the Chinese and the PLA Strategic Support Force, which has brought together their electronic network warfare and cyber warfare capabilities.

The various combinations and synergies that the Chinese are hoping to exploit pose a challenge across a variety of areas. Thank you very much.

[The prepared statement of Mr. Cheng can be found in the Appendix on page 41.]

Ms. STEFANIK. Thank you, Mr. Cheng.

Mr. Scharre.

STATEMENT OF PAUL SCHARRE, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND NATIONAL SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Mr. SCHARRE. Chairman Stefanik, Ranking Member Langevin, and distinguished members, thank you for inviting me to testify today. Chinese is a major and fast-growing player in information technology. As the world's third largest economy and most populous nation in the world, China has major structural advantages. China's population is a key source of strength because it is a potential source of data on human behavior and genomics. Combined with a more lax cultural attitude towards data protection and personal privacy, this data can help fuel advances in artificial intelligence and synthetic biology.

China also combines a dynamic private sector with a government that plans and executes long-term strategies to increase China's competitiveness. China has used this in recent years to execute plans to move forward on artificial intelligence, synthetic biology, and quantum computing.

China is a global leader in artificial intelligence, second only to the United States. Baidu, Tencent, and Alibaba are all Chinese firms that are top tier AI companies, and China also has a vibrant AI startup scene.

Since 2014 China has surpassed the United States in the total number of publications in deep learning, an important subfield of AI. While the quantity of publications does not necessarily equate to quality, Chinese AI researchers have won a number of recent high-profile competitions, including one sponsored by the U.S. Intelligence Advanced Research Projects Activity, IARPA. At the 2017 meeting of the Association for the Advancement of Artificial Intelligence, there were roughly as many papers accepted from China as there were from the United States. The U.S. still leads the world in AI patents, but China is growing at a faster rate.

Earlier last year, in July 2017, China published a national strategy for artificial intelligence. Under this plan China's goal is to be the global leader in AI by 2030. China's plan includes focusing on the education and recruitment of top AI talent, and they have followed this through with notable acquisitions of top-tier Silicon Valley AI researchers.

News reports indicate that Chinese firms see the Trump administration's anti-immigrant policies as an opportunity to draw away

top U.S. technology talent, as immigrants are responsible for one quarter of startups in the United States.

China also has significant advantages in translating private sector advances in AI into national security applications because of its model of military-civil fusion. In the United States, the Defense Department has struggled to break down largely self-imposed barriers to working with nontraditional defense companies that lock the DOD out of crucial innovation in places like Silicon Valley.

China has a closer relationship between the public and private sector and is able to more easily spin in private sector innovations into the military. This means that not only is China a significant player in AI, with the plan to be the world leader by 2030, but that China has major advantages in translating these private sector gains into national security applications.

The information revolution has opened up new opportunities in biotechnology as computers have made genome sequencing increasingly affordable. A Chinese company, Beijing Genomics Institute, BGI, is the world's largest genetic research center. BGI has a U.S.-based center and has sequenced the genomes of millions of Americans. BGI has robust support from the Chinese Government and partnerships to the Chinese military research institutes.

The Chinese Government has created multiple national-level biotechnology development plans. One of the strategies China uses is going out and bringing in foreign innovation by investing in foreign companies. For example, in 2013 BGI acquired next-generation genome sequencing technologies by purchasing the U.S. company, Complete Genomics.

Quantum computing is another area of important information-related technologies and one in which China has seen striking recent advances. In 2017 Chinese researchers made major breakthroughs in developing a 10-qubit quantum processor and a quantum communications satellite. China is following up on these advances with national-level investments, including a \$10 billion national laboratory for quantum technology.

In these and other areas, one of China's biggest strengths relative to the United States is the government's willingness to develop and follow through on large scale long-term investment plans. China has repeatedly demonstrated an ability to acquire foreign expertise by investing in foreign companies and then use that to improve Chinese indigenous capabilities. Chinese capacity for executing long-term strategies for technology development should not be underestimated, and Chinese plans to be the global leader in critical technology areas such as artificial intelligence should be taken seriously. Thank you.

[The prepared statement of Mr. Scharre can be found in the Appendix on page 51.]

Ms. STEFANIK. Thank you, Mr. Scharre.

Mr. Carter, you are recognized.

STATEMENT OF WILLIAM CARTER, DEPUTY DIRECTOR AND FELLOW, TECHNOLOGY POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. CARTER. Chairwoman Stefanik, Ranking Member Langevin, members of the committee, thank you for the opportunity to partic-

ipate in today's hearing. As you mentioned in your opening statements, China's significant progress in key emerging technologies like artificial intelligence, cyber, space-based capabilities and anti-satellite weapons, electronic warfare, and quantum computing have transformed the global economy and global security environment and require a rethink of the way we approach securing our Nation.

Asia is a critical part of America's future economically and strategically, and we find ourselves in a new era of strategic competition with China, one defined by competing progress in advanced technologies. Our response to China's progress in technology is essential to our future.

As we look at what China is doing, they have taken a page out of our playbook pursuing an offset strategy to overcome our conventional superiority by beating us in the race to the next generation of transformative technology. They are evaluating our military technology, our future strategy and doctrine, looking for gaps and weaknesses in our approach so they can exploit them for their own advantage, and developing national strategies to leverage both the private sector and their military complex to advance their own agenda. We must develop a national security technology strategy of our own to overcome China's efforts to undermine our global position.

China's technological efforts can be divided into two broad categories. First, they are developing technologies to disrupt and degrade our military capabilities by exploiting our vulnerabilities in the information domain. Second, they are investing in technologies that will determine the future balance of both global economic and strategic power. They have made significant strides in both of these areas.

China has already demonstrated the ability to significantly disrupt, degrade, and even destroy the infrastructure on which our military depends. The PLA has tested a range of antisatellite weapons, expanded their electronic warfare capabilities, and developed some of the most sophisticated offensive cyber capabilities in the world. China is also investing heavily in building its technological base to dominate the technologies of the future.

In particular, China sees artificial intelligence and quantum technology as foundational to both economic and military competitiveness in the long term, and has become not just a copycat or adopter of these technologies, but an innovator in their own right. Competition in AI between the U.S. and China has become neck and neck. Chinese researchers are now a fixture at AI conferences. Chinese companies have made significant breakthroughs in AI applications, including natural language processing, real-time translation, imagery analysis, facial recognition, and autonomous driving. And China has an advantage in translating these private sector gains and innovations into national security outcomes.

In quantum, China may already be ahead. As Paul mentioned, China has launched a quantum communications satellite, established a quantum link between Beijing and Shanghai, has invested billions of dollars into quantum computing, and even claims to have tested quantum radar. Some of China's claimed advances in quantum technology and in AI are likely embellished. We have

seen enough of China's capabilities in this field that we must take them seriously.

Our strategy to address China's rise in technology and power must address both the long-term and the short-term threats. In the short term, we must counter China's efforts to exploit our military's dependence on ICT [information and communications technology] technologies by investing in resiliency and ensuring that China never has enough confidence in their abilities to compromise our systems to justify a first strike.

In the long term, we must ensure that our world-leading education system and business environment work for us, not for China. We must rethink the relationship between private sector innovation and our military's technological edge to better leverage our greatest strength, our private technology industry. We must push back against China's efforts to acquire our technology and innovation, but not push away China's brightest minds and innovation capital if they want to send them to the United States.

We must invest in fundamental R&D that will form the basis of the next generation of technologies, not by replicating or subsidizing the private sector's efforts, but by supporting the kind of long-term research that private companies are less willing to fund.

And we should build a strong base on which our private sector innovators can thrive by investing in education, creating strong commercial markets for transformative technologies, and by protecting our companies' ability to compete in international markets.

I thank the committee for the opportunity to testify, and I would be happy to answer any questions.

[The prepared statement of Mr. Carter can be found in the Appendix on page 66.]

Ms. STEFANIK. Thank you, Mr. Carter.

We will now move to questions. My question is for each of you since all of you touched upon this. I am concerned about China's national-level plans, as Dean Cheng describes it, this whole-of-society approach. How do we, knowing that we have a fundamentally different form of government and fundamentally different society in the U.S., how do we compete? What are our limitations?

Mr. Scharre, you talked about some of the self-imposed barriers between the Department of Defense and the private sector. What specifically do we need to do as policymakers to ensure that we are able to have a moonshot goal when it comes to technological advancements. I will start with you, Mr. Cheng.

Mr. CHENG. Ma'am, I think that one of the key parallels was the Eisenhower administration. Confronted with the Soviet Union, President Eisenhower had a choice between trying to replicate a very top-down government-led approach, which is what we ultimately saw in the Soviet military industrial base, and an American approach, which ultimately relied more on the private sector, certain incentives, taxes, tax policies, things like that.

I would suggest that the same will be true. As all of us here have noted, the Chinese are pursuing a top-down approach. At the end of the day they believe that a small group at the top is smarter than the broad set of people pursuing various elements. I would suggest, therefore, that a less top-down, more broadly incentivized set of structures that nonetheless allows our private sector to push

across an array of new technologies, driven ultimately by the profit motive, may well prove strategically better off just as our defense industrial complex ultimately defeated the Soviet one.

Mr. SCHARRE. Yeah, I mean I would agree that our system is clearly better in the sense that it enables the private sector to come up with these solutions on their own, and we don't want to try to strangle that or choke that off, but how do we create kind of the right conditions to make sure that we are bringing in the top talent from around the world? I think education and recruitment of human capital is really critical. Making sure that we are educating people in the United States, we are encouraging others to come here, the best researchers, the best entrepreneurs, and then stay here is really critical. China is very proactive about this, and we need to be proactive, too.

I think there are some places where we want to protect some of these innovations from others, so that could be involved with export control reform or CFIUS [Committee on Foreign Investment in the United States] reform. And then I think in particular there is a lot more we can do on defense reform, as you mentioned initially in your opening statement, to try to free up some of the money that DOD is spending so that it is available to some of these more emerging technology areas because we do have a lot of barriers—some are legislative, some are policy—in place that make it very difficult for nontraditional defense companies to work with DOD.

And so some of these initiatives like DIUx and SCO and others to kind of build on those to continue to make it easier for DOD to access this innovation.

Mr. CARTER. I agree. I would also add that I think that there is a tendency in the U.S. to think that freedom is both a necessary and a sufficient condition for innovation. I don't think that is necessarily true. If you look at what Russia was able to do in the space race, for example, they lacked freedom and they innovated. But also, if you look at what is happening now, we give freedom to our private sector, but there are other things that we need to do to enable them to innovate.

Building our human capital is I think one essential one, but another is to ensure that we create markets for these commercial innovations so that the private sector is incentivized to invest.

There are a huge number of policy hurdles to new technologies like AI, so think of the example of autonomous driving. There are huge potential implications both in what the fundamental research into autonomous driving will yield in terms of better knowledge of how to build learning systems that deal in complex, unstructured environments, and direct applications of self-driving vehicles in military contexts.

But we need to remove some of the liability, regulatory, and governance hurdles and questions around what our approach will be so that the private sector will invest.

Ms. STEFANIK. Thank you. I now recognize Mr. Langevin for his questions.

Mr. LANGEVIN. Thank you, Madam Chairwoman, and I thank our witnesses for your testimony once again.

One question that I wanted to raise off the bat since, Mr. Scharre, you touched on it and the others have touched on it, as

well, the issue of quantum computing is something that I have followed for quite some time, and I don't know if you are in a position to assess this, but who do you feel right now has the advantage in who is going to develop the first quantum computer, the United States or China? I understand that the overall strategic importance of quantum computing as one former four-star general that I deeply respect stated to me that whoever develops the next quantum computer—first quantum computer holds the keys to the kingdom, so this is a big deal.

Mr. SCHARRE. Yeah, it is clearly a critical issue in terms of cryptography and protected communications. I think it is difficult from like open source materials to assess because—and reasonably so. So much of what is being done is classified. It is clear that what China is doing at a basic science level they are making some serious breakthroughs that all of us have mentioned, so I think they certainly should be taken serious as a competitor.

Mr. CARTER. I would just add to that that if you speak to researchers in the quantum field in the U.S. they may not always be able to tell you exactly what they are doing, but they will tell you about some of the challenges that they are facing. Just getting money for a lot of their projects is difficult, if not impossible, and a lot of them see China offering them funding for this research. It is the best option that they have, and they ask themselves the question of do I give up my research, which I know is valuable, or do I allow it to be funded by China and possibly co-opted by China?

Mr. LANGEVIN. Good point. Next to all of our witnesses, China obviously is pursuing policies and subsidies, as well as demonstrating a willingness to experiment on things like directed energy technology. Can you describe China's approach to DE and how does their approach impact our edge in this field specifically as it pertains to electromagnetic railgun?

Mr. SCHARRE. Yeah, I don't have a lot of details on China's advancement in DE and electromagnetic railgun. They are certainly doing things and they are making investments, but I don't have a lot of details on that.

Mr. LANGEVIN. Okay. Mr. Cheng.

Mr. CHENG. My understanding is that the Chinese in their own reporting do seem to be engaging in a broad set of directed energy efforts. One of my focuses is on space issues, and it does seem that China views directed energy as potentially overcoming the political problem of kinetic energy kill against satellites. That is, if you hit one with something like what they did in 2007 you generate a lot of debris, but if you fire up a sufficiently high-powered laser or particle beam you can fry the electronics, you can destroy the sensor package, but you don't generate a lot of debris in orbit, which has important political implications.

Mr. LANGEVIN. So oftentimes the lack of policies and doctrine I think we found can stymie the Department of Defense's willingness to invest in and transition technology. Mr. Scharre, based on your experience in the Department of Defense work in issues such as the use of autonomous weapons systems what is your assessment on the impact of current policy on investment in technological development and transition? And what more remains to be done on the policy front to foster technological transfer and development of

doctrine with respect to autonomous weapons systems and other technologies?

Mr. SCHARRE. Thanks. We have some ad hoc policies in place for some emerging technologies where these issues come up like autonomous weapons, directed energy weapons. There is no overarching process in the Department for dealing with policies that might arise in some kind of new technology.

Now, many new technologies don't raise interesting policy questions, but some of them do. Hypersonics might raise interesting questions for strategic stability. Anything involving genomics or human enhancement or human performance modification raises a whole host of interesting and challenging policy questions.

There is no process or organization inside the Department to harness and deal with these things as they come up, and so the biggest gap that exists today in terms of policy is on the human enhancement side. There is simply no—there is no policy decision-making process, there is no mechanism in DOD, to try to guide investments or applications.

So things are happening inside the Department in various research labs, but there is actually no decision-making body that you can go to if you wanted to either do research or actually operationally use something that would modify people in some significant way, give them a drug to make them, you know, perform better on some task. There is no, like, way to actually do that right now in the Department. I think that is a significant gap.

Mr. LANGEVIN. Thank you. I yield back. Thank you for your testimony.

Ms. STEFANIK. Dr. Abraham.

Dr. ABRAHAM. Thank you, Madam Chair. My basic understanding of AI is that you have this computer that not only is reacting to programming, but actually thinks for itself, but not only does that, but then acts on that thought process. And Mr. Cheng said that China not only develops, but has the fastest computers in the world.

We on HASC [House Armed Services Committee] have had the discussion of the cumbersome acquisition process that we in America face with DOD that sometimes it may take 18 months simply to do a study and by the time the technology comes out we are already way behind the curve and certainly with the testimony we heard today that certainly could be true.

My question is we know that many, many Chinese private companies are vested, are owned—very elite and very sophisticated American companies not only in the navigational field, aviation field, you name it they have a piece of the pie in some of these companies. Mr. Scharre, you alluded to it about protecting some of these technologies with some export prohibits something like that, but, again, China owns these companies already in the United States.

So the question to each of you gentlemen just quickly, what organizational, what bureaucratic barriers can we throw up, are there any that can protect our technology on this side of the ocean?

Mr. Cheng, you go first.

Mr. CHENG. Yes, sir. I think that obviously we have CFIUS, the Committee on Foreign Investment in the United States. One of the

key things to keep in mind, however, is that CFIUS is a gatekeeper entity. It keeps new acquisitions of already existing companies, it reviews those. What we now confront is the distinct possibility of corporate entities perhaps set up by China or others within the United States who would then be able to acquire. So it is not China Comp Corp. buying something, it is Orange Venture Capital investing in something headquartered in New York or Delaware.

So what we would seem to need here is a new entity that would at least monitor, and perhaps also be able to pass judgment, on investments that would be able to demand background, perhaps embedded with something like the SEC [U.S. Securities and Exchange Commission] so that Orange Investments would have to report who are their members, where is there are money coming from.

The other aspect here that I would like to emphasize here is as our allies, countries like Germany and Japan think about creating their version of CFIUS would be coordinating our experience and our lessons learned with their efforts because at the end of the day nations like China exploit a variety of different methods and approaches. If they are shut down here they may try to acquire it through a Canadian subsidiary or a German subsidiary, and that is one of the other things to keep in mind, sir.

Mr. SCHARRE. Yes, sir, I think CFIUS reform probably makes sense in probably two key dimensions that would give—expand the scope of it and give greater flexibility to the executive. One would be in the types of commercial activities that it applies to, lowering the threshold for foreign investment that would trigger it, and if you are looking at other types of, say, joint ventures that might fall under the scope of CFIUS.

But also from a substantive standpoint expanding the scope of technologies, and so giving the executive branch more flexibility to establish some critical technologies, emerging technologies like we are discussing today that would then fall under the scope of CFIUS.

Mr. CARTER. I would agree with Mr. Scharre on expanding the scope, giving the government more flexibility. I also think that as we saw in the case with Ant Financial, the recent acquisition that was blocked, thinking about those enabling commodities that the chairwoman mentioned in her opening statement is another important dimension that we have to add to CFIUS. What are some enabling commodities and enabling technologies that may not themselves be a huge national security threat, but could enable China to develop a significant national security threat. But I would also just caution that I think this will be extremely difficult to do.

As you mentioned, when you think about AI, the real value of AI, particularly from a national security perspective, is the integration of a bunch of technologies that individually might not seem very threatening.

And so I think looking at it on a deal basis, looking on it on an individual technology basis is going to be a really challenging thing to do.

Dr. ABRAHAM. Thank you, Madam Chair.

Ms. STEFANIK. Mr. Larsen.

Mr. LARSEN. Thanks for all coming in. And along those lines as well sort of talking about playing defense, talk CFIUS reform or

export control reform and wondering about offense, what can we do in the U.S.

Before I get to that point though I do want to go back to defense and the point that Mr. Carter has made about on CFIUS reform. The challenge of sort of outlining this technology or that technology because when we wrote CFIUS, in fact, when—I wasn't here, but when we last reformed it I was here, and this was not an issue at all. It was about whether or not ports should be purchased by Middle Eastern companies. That was the deal. It wasn't anything else.

And so how to rewrite a CFIUS to anticipate, make it broad enough to address these issues, and I wonder if you've thought about that in particular as opposed to chasing the next, you know, quantum computing issue or the next AI issue. Anyone thought through that more broadly?

Mr. SCHARRE. Yeah, I mean, certainly one approach could simply be to give the executive branch, in fact, require them to come up with a list of critical technology areas that are regularly updated. That might be one area that bakes in more flexibility to the law.

Mr. LARSEN. Kind of like what you do with export control.

Mr. CHENG. Sir, the problem actually though is exactly what we have seen with export controls. There is every incentive to add yet another technology to the list and every disincentive to ever remove any technology from the list; and therefore, I respectfully disagree with my colleagues here on this panel because one of the things that worries me is we want to maintain a positive investment environment and economic environment.

We do not want to kill that golden goose. And in particular when we talk about increasing the flexibility of the executive branch, too often what that means is, well, that is great, I will be flexible and I will add four more new technologies that are now going to have to be reviewed.

I think that is why I mentioned President Eisenhower earlier, is he felt it important to maintain a light touch, that, yes, there should be the option of flexibility, but at the same time there still needs to be that check and balance because at the end of the day an overly regulatory emphasizing top-down emphasize the executive branch could easily wind up strangling as much as nurturing key technologies.

Mr. LARSEN. Thank you, sir.

Mr. CARTER. Maybe just to build off of Dean's comments, I agree that it is extremely difficult to outline any list of technology that doesn't suddenly become, you know, all-encompassing. I think you have to differentiate the current situation from some of the past arms control efforts in that maybe the parallel is this is more a discussion around computers than it is around stealth technology or hypersonics, for example.

There are technologies that are easier to control, but when you think about AI, when you think about quantum, the potential in the commercial sector and the civilian uses are so massive, and particularly the importance of developing those technologies to our economic competitiveness is so vast that I think that any effort to create a list that would actually capture the technologies that will have the greatest national security implications risks crippling our future economic potential.

Mr. LARSEN. Yes. I have about a minute and a half left. So a little bit more on offense than playing defense and thinking about how we organize or reorganize. It is my impression that, you know, perhaps in the past the Defense Department has defined the defense industrial base as much too narrow, that it has been about steel and airplanes, large platforms and things when, in fact, what you are talking about is an industrial base that is a lot of electrons, a lot of wires, and a lot of people.

So on that point organizationally is the Pentagon—other than DIUx—is the Pentagon thinking beyond the traditional defense industrial base, what is your thought on that?

Mr. SCHARRE. I think it is a challenge. If you talk to the services their key metric is still metrics in steel and iron and people. If you talk to the Navy they are going to talk about ships and number of aircraft carriers. If you talk to the Air Force they are going to talk about number of tactical fighter aircraft and bombers. And the Army cares about number of brigade combat teams. And those are the kind of key metrics of national power.

And, you know, in World War II that was a war won by steel and iron, right? The Allies outproduced the Axis powers. That is not the era we are in today and so those are not necessarily the right metrics. And so I think there are obviously some people thinking this kind of way inside the Department, but it is still a challenge.

Mr. LARSEN. I have got 17 seconds left. I will just take that and yield back. Thanks.

Ms. STEFANIK. Mr. Scott.

Mr. SCOTT. Thank you, Madam Chair. Is it Scharre?

Mr. SCHARRE. Yes.

Mr. SCOTT. Mr. Scharre, I wrote down your comment about self-imposed barriers, and I know you were in the Army. You know, it took 10 years to pick out a pistol for the Army, and obviously with technology we don't have a decade to wait to pick a new system.

And so I have got another line of questions for Mr. Carter, but assuming I have time I want to come back to what you think the self-imposed barriers are and what can be done to remove them, and if I don't get there if you have any suggestions on that I would appreciate that for the committee in writing.

Mr. Carter, you put in your testimony, and I agree with you on this, we must retrain our military to operate in analog mode without access to data and technology. We must ensure that any new systems or platforms DOD buys has at least some basic level of functionality without access to space-based capabilities. Is that because of our vulnerabilities?

Mr. CARTER. Yes, it is.

Mr. SCOTT. And would you agree with me that the DOD is actually moving in the opposite direction and becoming more and more dependent on the space-based capabilities?

Mr. CARTER. I would agree with that. I think there is a recognition of that vulnerability in the Department and that they would like to move away from it, but they find themselves balancing the impressive new capabilities they can get out of some of these platforms that are dependent on these technologies with the vulnerability that it creates and also they are struggling with the fact that

the conflicts that we are actually engaged in today are not conflicts where our space-based assets are threatened——

Mr. SCOTT. That's right, that's absolutely right

Mr. CARTER [continuing]. Are not conflicts where our networks are really threatened.

So I think that leadership from Congress can be really meaningful in this area of pointing them towards the next era of threats.

Mr. SCOTT. Sure. And I suppose, and this is a personal thing for me, but one of the things that bothers me about the DOD's actions is they propose to eliminate weapons systems that work in the current environment for a system that may work in a future environment.

And so when you talk about getting rid of the A-10 or getting rid of the JSTARS [Joint Surveillance and Target Attack Radar System], which are currently being used in the conflicts that we are in today, for a system that may work in a conflict that may or may not exist 10 or 15 or 20 years from now, it just doesn't follow logic to me. But a specific question with PLA's assessment of the U.S. military and our vulnerability in space, do you believe there should be an increased emphasis on the development of defensive space capabilities, as well as application of quantum communications to overcome challenges in the electromagnetic spectrum?

Mr. CARTER. I do. I think that defensive space capabilities are important. Also thinking of our space-based capabilities in terms of resilience, so, you know, one key area I think is creating more survivable, more replaceable, space-based architectures, larger constellations of smaller, less sophisticated satellites that together generate a lot of capability, but are not individually as sophisticated. They are cheaper, they are easier to replace when they break, they are faster to produce. That is an example of the kind of thinking that I think we need to bring to DOD.

Mr. SCOTT. And if they kill one, there are three or four others out there to take its place?

Mr. CARTER. Exactly.

Mr. SCOTT. Mr. Scharre, could you explain some of the self-imposed barriers and how we could remove them, and do you believe that—it is pretty clear you believe we are better off partnering with private industry rather than holding all of this inside the DOD.

Mr. SCHARRE. Yeah, we have a very vibrant private industry in the United States willing to harness that technology and bring that in. The problem is that we have created this acquisition system that works very well if you are working with a traditional defense company to build a large capital asset over several years.

So if you are building an aircraft carrier, it is kind of the right system to have actually. You are going to keep it for 50 years. It costs a heck of a lot of money. And you want to take your time to do it right. So a deliberative process makes sense. It is completely unsuitable for these kinds of rapidly evolving technologies. You want to be able to tap into a whole wide range of companies, including those that don't specialize in working with DOD and we move very, very quickly.

And so some of the concerns I hear of people in the private sector are things about red tape dealing with the government, slowness

of the process, the government trying to acquire intellectual property, which for many of these companies that is really what is most vital to them, and then the profit margins actually not being as significant as in the private sector.

Mr. SCOTT. I am almost out of time. If I could just to follow up, one of the things that also has to be thought of though is if you have partnered with those private sectors they are private companies and the Chinese do have the ability to buy private companies and then, therefore, highjack that technology, and I think that is just kind of one of the highlights of the complexity of the issues we face here, but thank you for being here.

Ms. STEFANIK. Mr. O'Rourke.

Mr. O'ROURKE. A couple questions. Mr. Scharre, you had mentioned the opportunity cost of either really being or just being perceived as being anti-immigrant in terms of attracting intellectual capital and the kind of people that are going to come up with the innovations that will allow us to excel in these areas. How long-lasting is the damage that you are already seeing? What would it take for the United States to correct the balance and be able to lead in the race to attract the best and the brightest from around the world?

Mr. SCHARRE. I think it is absolutely critical. We had Eric Schmidt, the Chairman of Alphabet, at an event a couple months ago and he raised this as his top concern coming from a major, you know, U.S. company that he wants to be able to draw in the best help from around the world and have them work for them.

I think it is too early to tell whether we will see significant damage from the current administration's policies and how long-lasting it will be. Some of them have been challenged in court, like the entrepreneur rule, and if not, you know, basically the administration's policy change has not survived in court.

But the cultural perception is certainly very damaging if people simply say, look, there is too much uncertainty, and if I am going to figure out where to pursue a degree or where to try to pursue a visa or where to pursue a postdoctorate or set up a company I am going to go elsewhere, and that can have major long-lasting effects.

Mr. O'ROURKE. And we are just reading story after story about graduate institutions having a hard time attracting foreign graduate students, and it seems to be totally connected to what we are talking about today.

And then I don't know if you want to start in answer to this question, the ranking member talked about mastery of quantum technologies being the keys to the kingdom and others have likened it to the U.S.-Soviet space race about who is going to get there first and what we are willing to invest.

And Mr. Carter talked about there is some things that the government will need to invest in that the private sector is just not willing to or doesn't have the capacity to do it. Tell me why this matters? I think I only if I am honest barely understand the importance of quantum radar, quantum communications, quantum processors, quantum satellites. Can you put it into big picture perspective for me?

Mr. SCHARRE. Sure. So there is a couple things that quantum technology can do that you simply cannot do with existing computers. Remote sensing is one of them, but probably the most significant national security applications are in cryptography. In essence a quantum computer in principle can be used to crack all known cryptography. That is a sort of theoretical concept. Building one that is practical would be very, very challenging.

Mr. O'ROURKE. We wouldn't have any more secrets of the Chinese if the Chinese were able to master this before we did.

Mr. SCHARRE. Well, you would have to sort of upgrade cryptography now because it is not even the question of when it is broken, it is that one could go back and then if you have stored data for communications you could go back and analyze this and crack old codes, which can be very damaging from a national security standpoint.

Quantum cryptography also enables more secure communications. So it is both a way to break current cryptography and then a solution to that problem; but yes, you have got to get there first.

Mr. O'ROURKE. And, Mr. Cheng, do you have anything to add to that?

Mr. CHENG. Michael Howard, the noted British military historian, has said that we need to reexamine the entire history of World War II now that the scale of cryptography, how much we and the British have broken the German codes has now finally come to light, that most of our decisions were actually made in light of the fact that we were reading the German mail and they were not reading ours. To have that kind of conclusion about World War II suggests the scale upon which successful encryption by a country like China would influence our ability to operate against them and conversely their ability to operate against us.

Mr. O'ROURKE. And, Mr. Carter, since you brought the question of public sector investment to compliment private sector investment, can you give us an idea of what this would take?

Mr. CARTER. Yes, I think that just to build very quickly on my colleagues, I think that, yes, there are the applications in cryptography. There is communications radar, but really kind of the cross-cutting theme for quantum is that it renders a whole bunch of technologies we depend upon ineffective, and it enables a whole generation of technologies against which we are utterly defenseless if we don't also have quantum computing capabilities.

In terms of investment I think I mentioned, you know, speaking to quantum researchers one theme that comes up is they just can't get money. The private sector doesn't want to put a lot of money into this. Some of them just don't believe it will work. There is a school of thought that shouldn't be completely discounted that quantum computing will never actually work at scale, but even if it does it will be a long time before we actually see the fruits of any of that, and the commercial value of it has yet to be demonstrated.

So I would put a lot of money into quantum computing, particularly the fundamental technologies, so computing and communications that we can build a lot of other things on top of.

Mr. O'ROURKE. Thank you.

Ms. STEFANIK. Dr. Wenstrup.

Dr. WENSTRUP. Thank you, Madam Chair. Thank you all for being here today. I appreciate the input you are giving us.

As I look at the members of CFIUS, the Chair from the Department of Treasury and then we have Justice, Homeland Security, Commerce, Defense, State, Energy, U.S. Trade Representative, and Science and Technology Policy. From a national security standpoint, is that ideal? Is that working well for us or what would your suggestions be as far as who actually makes up CFIUS?

Mr. SCHARRE. It is as we have discussed in some of the responses to CFIUS there are a lot of competing concerns that you need to have, so I think it makes sense to have a wide variety of government actors to have a seat at the table. I think the best thing to do would be to give them more flexibility on what they can actually respond to in terms of potential investments, but I think it does make sense to people to have all those equities raised.

Mr. CARTER. The other thing I would add to that is it may depend on the case who you want to have the strongest voice. I think having a system that is flexible, that gives everyone the opportunity to participate gives everyone who has an important point of view the opportunity to be louder than the other folks.

Mr. CHENG. I mean, the issue here, sir, is that every one of these folks has a different set of incentives, and not one of them obviously where naturally should dominate. If you are talking to the intelligence community [IC] and the national security establishment that should obviously take priority over commercial opportunities.

On the other hand very few economists seem to work for DOD and the intelligence community seems to sometimes lack economic background, as well. That has distinct implications for the ability to foster new business. You know, they may well consider fostering business to be secondary to protecting certain technologies.

I think that at the end of the day it is messy, but it is probably better than handing it to a much more limited set of perspectives.

Dr. WENSTRUP. And I can see the advantages of having variety of input, everyone looking at it a little bit differently, and I guess what my concern is that can work two ways. One, it can be very beneficial because you get so many opinions, or two, you can get so many opinions you get nothing done. And you kind of alluded to that before about taking some things away as opposed to adding things, et cetera.

And so I wondered if you had an opinion does it happen both ways, one way more than the other or is it smooth sailing? I just think, you know, we do things the way we do things. Is it always the best way to do things is really where I am coming from.

Mr. CHENG. I think, sir, when we look abroad and we look at the Germans as an example where they had no CFIUS at all, and it was pretty much open season, they are now coming to the scared realization of just how much has probably left the borders of Germany. So clearly, you know, this is not perfect, but it is probably—it is a little bit like the old story about the bear that walks on its hind legs. It is not that it walks poorly, it is that it walks at all, and I think that that may be perhaps the best we can hope for here is good enough.

Dr. WENSTRUP. Anyone else? Thank you. I yield back.

Ms. STEFANIK. Ms. Speier.

Ms. SPEIER. Thank you, Madam Chairwoman. Thank you for your sobering testimony today.

I have a series of questions, but let me just start with this one. The White House has an Office of Science and Technology Policy [OSTP]. For the last year there has been no one who has been appointed by the administration as the director and it is responsible for emerging and exponential technologies, and it appears that the OSTP division of national security has no personnel whatsoever.

So I guess I am concerned that we from—the White House has not the conveyed an alarm really that this function is critical, and I wonder to what extent you think that this is serious and whether or not it is creating a national security risk.

Yes, Mr. Cheng.

Mr. CHENG. Ma'am, under the previous administration there was an OSTP director who felt it incumbent to promote U.S.-China space cooperation, who wanted to see more interaction between the American space program, which as we know is vital to American national security, and China's space program, which is run pretty much through the military.

I would say that if we were to adopt a Hippocratic approach, which is to say first do no harm, I think I might prefer to have an absent seat, rather than someone who is actively pushing for greater interaction and cooperation with the People's Republic of China in high-technology areas.

Ms. SPEIER. Mr. Scharre.

Mr. SCHARRE. Yeah. So thank you. I do think the lack of leadership in the White House on this issue is a concern. For example, in artificial intelligence there were a number of initiatives taken at the end of the last administration. At the sort of working level of the government, a lot of these things are still moving forward. There is inertia, people that are trying to execute things.

But there are a lot of critical things where you are going to need leadership in OSTP at the White House to do things like look at whole-of-government investment in science and technology, particularly in some of these areas like quantum technology where government investment is really important, because it is not quite mature enough where the private sector is going to pick it up; on things like immigration policy, to make sure we are bringing in top talent and keeping them. I think one of the challenges on some of those topics, it does run counter to where the administration currently is.

Ms. SPEIER. Mr. Carter.

Mr. CARTER. I would agree with Mr. Scharre. And I would just add that a lot of what was done at the end of the Obama administration was to ask some very important questions to task people with gathering information, with finding answers to some of these tough policy challenges.

And I worry that, yes, at the working level people are continuing to pursue these initiatives. They are going to have no one to report to when they find answers. Those weren't just, you know, kind of black holes into which we were pitching our resources.

Those were important questions that we are going to need to answer not just for national security purposes but because we need to think about building these commercial markets for AI technolo-

gies and things like that. And leadership at the top level is going to be important.

Ms. SPEIER. I always worry that we are kind of late. The Office of Personnel Management [OPM] that was hacked into, we really didn't know about it for over a year. So China had access for a full year into some of the most sensitive information about Federal employees.

Kaspersky operated in this country for years and was actually hired by government entities as the purveyor of software or malware detection; and yet, it wasn't until 2 months ago that Kaspersky has been identified as not being a good actor.

What do we do about this? Are there other Kasperskies out there, from a Chinese perspective, that we should be concerned about or from other countries? Mr. Cheng.

Mr. CHENG. Absolutely, yes, there are other entities out there. It is interesting to note that while on the one hand we have tried to limit access for companies like Huawei, other Chinese companies have been able to sell products. I believe the Federal Government only recently recommended not acquiring Lenovo computers, which are another Chinese entity.

What can we do about it? I think one of the most important aspects here is recognizing we are in the competition. I think that for too long we have been focused, for good reason, on the ongoing conflicts in places like Afghanistan and Iraq. But these are countries that do not pose a technology challenge to us.

Recent events involving Russia, ongoing events involving China, I think, are providing a wakeup call. But I think that outside of perhaps this room and some quarters in the think tank and policy community, there is still this view that at the end of the day, China and Russia really are somehow distant threats and laggard competitors, rather than in some ways, increasingly our peers.

Ms. SPEIER. I have actually 20 seconds or I have expired. Maybe you could just finish the answer to that question.

Mr. SCHARRE. Yeah. I am sorry. I lost my train of thought.

Ms. SPEIER. Kaspersky, OPM.

Mr. SCHARRE. Yes. I think the fundamental problem here is that our cybersecurity architecture is just simply very porous and has a lot of vulnerabilities across the board. And part of this is about, you know, really we have incentivized efficiency over robustness and security as we have built up different kinds of computer architectures.

And so—and this is a place where finding ways to change the incentive structures on things like who pays when there is, you know, a hack at a company that releases, you know, vital personal data. To change the incentive structure so that companies are incentivized to take cybersecurity more seriously might be ways to address that problem.

Ms. STEFANIK. Quickly.

Mr. CARTER. I agree, and I would just add to that that when you look at Kaspersky in particular, for us to fully recognize what had happened and to kind of announce at a national level that, oh, my God, Kaspersky has done this to us took a while.

But I think a number of years ago if you had talked to folks in the cybersecurity community and asked them about Eugene Kas-

persky and some of the other folks in that company, they would have known full well what their background is and their relationship to the Russian state. So partly it is just about getting the right people to listen to the right people.

Ms. SPEIER. Thank you. I yield back.

Ms. STEFANIK. Mr. Lamborn.

Mr. LAMBORN. Thank you. Thanks for having this hearing. Thank you, all, for being here.

China's satellite manufacturing industry is growing at an alarming rate. In the past 2 years, Chinese factories have pumped out 40 satellites. I am concerned that China is using unfair trade practices, such as subsidizing launch costs, to prop up its state-owned entities.

This, in turn, places our own satellite manufacturers at a competitive disadvantage. So it is for this reason, as well as for the threat that they pose to our Nation's cybersecurity, that I included a provision in last year's Defense Authorization Act that bans the procurement of SATCOM [satellite communication] systems if such systems use satellites or components designed or manufactured by the Chinese.

So, Mr. Cheng, given your expertise in China's military and space sector, are you aware of this or any other trends that China is employing to prop up its satellite export industry?

Mr. CHENG. Sir, I am not sure that—with state-owned enterprises, almost by definition, it is subsidized. When you have a state-run banking system, you can also make very clear investment choices where profit motive is not an issue. However, our ITAR [International Traffic in Arms Regulations] regulations have, in a sense, really affected already China's ability to play in things like the satellite launch industry.

With regards to the satellite-specific aspect, where the Chinese seem to be going right now is two aspects: One, lower-end countries, countries that are new to space, Nigeria, Bolivia, Venezuela, where they can sell satellites, design, build the ground facilities all for a price that frankly no country can really compete with.

The other aspect here is that in the private sector, as there are talked about, thousands satellite—ten—4,000 satellite constellations of small sets. We expect to see the Chinese start moving into that arena. But that is dealing with private companies, not with the government.

These are areas that will potentially constitute revolutionary capabilities, and the Chinese recognize that it is important to play there. So therefore, it is also very likely that they won't care about, one, cost, and, two, punishment, unless it is truly meaningful and deep impacting, not on these companies themselves, which are probably invulnerable, but rather to a larger thing like access to western capital, listing on stock exchanges, et cetera.

Mr. LAMBORN. And as a follow-up to that, Mr. Cheng, as they continue to gain market share in satellite manufacturing, sometimes through the use of unfair trade practices, how does that impact our own manufacturers, and, more specifically, the price point that we pay for DOD and IC satellites?

Mr. CHENG. I am not aware that our DOD and intelligence community satellite programs are actually open to competition. I don't

think that the Chinese are likely to be able to step in to—at this point and persuade the National Reconnaissance Office——

Mr. LAMBORN. Don't you think there are indirect effects?

Mr. CHENG. Absolutely.

Mr. LAMBORN. That is what I am getting at.

Mr. CHENG. At the subsystem level it is certainly possible. Again, ITAR regulations, however, do limit the ability for launch and things like that. So that, I think, is a factor.

The ITAR has succeeded really in limiting and channeling Chinese access. Where this is much more of a problem will be in the truly commercial sectors, just as with other high-technology areas. The question is whether Intelsat and Eutelsat are going to necessarily buy a satellite from Boeing if the Chinese can offer a satellite of relatively comparable capability for a purely commercial purpose. Now, subsystems, solar panels, batteries, things like that, in the longer term in the supply chain, that is certainly a possibility.

I do also want to note here that the Chinese are almost certainly going to be offering data, not just the physical hardware, but more and more as they deploy constellations, we should expect to see them offering data at very competitive, potentially undercutting prices to a variety of users, which will then, of course, justify everything from imaging to SIGINT [signal intelligence] about a variety of targets.

Mr. LAMBORN. Mr. Carter or Mr. Scharre, is there more we should do to protect against China's unfair trade practices when it comes to satellite manufacturing or the selling of data?

Mr. CARTER. I would actually—looking at what is happening in the space industry now, there is actually a huge amount of innovation happening in the United States in the private sector, and a large part of that seems driven by the fact that U.S. companies know that they can't compete on price with the current technology. But there is also a clear free-market mechanism that is driving them to innovate and find ways to cut cost and deliver better capabilities.

So I think there may be room to do more to combat China's anti-competitive practices, but I would also say that there is probably more reason for optimism about the U.S. commercial space sector today than there has been in a while.

Mr. LAMBORN. Thank you.

Ms. STEFANIK. Mr. Khanna.

Mr. KHANNA. Thank you, Chairwoman Stefanik, for allowing me to participate on this subcommittee.

I read your testimony about China proposing almost \$150 billion in the next 5 years of funding on artificial intelligence. And I think Mr. Carter pointed out that our investment—total U.S. Government investment is about \$1 billion.

I wonder what you would recommend for the United States Government to be competitive going forward in the next 10 years on artificial intelligence?

Mr. CARTER. I would say two things in AI in particular. One is, China understands that certain technologies are building blocks that enable other technologies to develop. We should take the same approach, think about what are the most fundamental break-

throughs that need to happen and then allow the private sector to commercialize and develop applications based on those breakthroughs.

A second piece is they look at the technology ecosystem fundamentally differently than we do. So when they think about AI, they are thinking in the same breadth about the internet of things, about ubiquitous connectivity, miniaturization, material science, energy science. And when we think about our approach to R&D to support artificial intelligence, we also need to look at all of these enabling technologies.

And, finally, it is not just the R&D space. Another example that I would point to in this area is China's pursuit of basic resources. And I think that that is something that we haven't quite gotten to connecting to AI yet, but China's approach to controlling lithium supplies and rare earth minerals is entirely based on their view of the potential of autonomous vehicles and other devices that are going to be using batteries.

And they are pursuing diplomatic government and commercial relationships with countries like Bolivia that have lithium supplies, Chile. And it is not just lithium; it is a range of other minerals.

We need to take this approach. All these technologies are linked. All of these basic sciences feed into the development of AI. AI is a system of systems. That is the biggest thing that I would encourage. We should invest in the most fundamental building blocks across all of these areas on which people can then build really good AI.

Mr. SCHARRE. You know, artificial intelligence is an area where there is so much investment happening in the private sector that I don't know that dollars is what the government needs to bring to the table.

The U.S. Government is never going to bring as much money as Google and Facebook are throwing at AI right now. And those advances are already happening. The trick for the government is to be able to bring that technology into the national security space and make sure that the government is able to go out and access that, in particular because these are not companies that typically work with the government, right. They are not building normal weapons systems.

Project Maven, the algorithm warfare cross-functional team that Chairwoman Stefanik mentioned, is something that is happening right now with DOD. They are trying to break down some of these barriers, grab ahold of this technology.

I think we want to expand the scope of that so that we find these acquisition tools that are working, give them to other people across the Department and other parts of the government as well, so they can go ahead and bring this technology in and use it very rapidly for near-term applications. They can think in, you know, months instead of years is what they are going to have to do to bring this in.

I think there are also some unique policy challenges the government needs to confront when they do this. There are a lot of safety and control and vulnerability problems with current sort of cutting-edge AI systems.

They are not the same as cybersecurity vulnerabilities, but it is a good analogy that machine learning systems have their own kinds of weaknesses and vulnerabilities. And the government has got to be conscious of that when we use them in national security applications.

So that if, for example, we use object recognition to do scanning for luggage for TSA [Transportation Security Administration] that there is not some vulnerability, people can find a way to kind of trick the system to sneak a bomb through that.

Mr. KHANNA. A quick follow-up. What would you think of creating an artificial intelligence center in the Department of Defense to do the things you are talking about? Quickly, I guess, and Mr. Cheng too.

Mr. CHENG. I think that that would be less useful than something like replicating things like the XPRIZEs. When we look at the explosion in space technology—no pun intended—what we have seen is that that has incentivized the private sector to go into things.

Another one is we are relaxing a lot of regulations that are preemptively already strangling things. Antimonopoly rules to facilitate smaller companies interacting with each other without having to look over their shoulder about legal vulnerabilities, liability concerns, these are, I think, much more useful than setting up yet another bureaucracy within DOD that would probably operate still under the standard current acquisition regulations that are the problem that I think all of us have identified here as more an obstacle than a facilitator.

Mr. SCHARRE. I think a DOD AI innovation center makes sense. I do think you would want to think about how you structure it so that the primary function is tapping into what the private sector is already doing.

Mr. CARTER. I would just add that the Defense Innovation Board recommended exactly this, and I think that when you have industry leaders that they are calling for it saying they could work better with DOD if they had it, that is a sign in itself. But we should probably also get their input on how to structure it, how to operationalize it.

Mr. KHANNA. Thank you.

Ms. STEFANIK. Thank you. Your time is expired.

We will now go to the second round of questions. My question has to do with the broader data question.

Mr. Scharre, in your opening statement, you noted that internet users top 3.8 billion people, nearly 5 billion people using cell phones, nearly 3 billion people using social media, and more than 20 billion devices connected via the internet of things.

What does this mean with respect to the amount of data available and being generated, especially in my opening statement when I referenced the potential for China to control 30 percent of the world's data by 2030? How does this impact the intelligence community, for example, which is a community that is grappling with this pace of technological change?

Mr. SCHARRE. So right now, we have these oceans of digital data, and it is very hard to actually make sense of it and process it. Artificial intelligence is changing that. And, in fact, the current meth-

ods of machine learning, deep learning in particular, need large volumes of data.

And so you actually have this synergy between these two kinds of digital technologies, this proliferation of large amounts of data, this huge accumulation of it, and AI that needs this data and then can learn from it and then can learn very complex things that you can't teach people. It can learn to recognize faces, translate languages.

For a country like China, that means that having this, you know, indigenously within their own countries, having hundreds of millions of internet users, people doing banking over mobile devices, all of that is this pool of data that they can draw into to then feed into their AI sector and they can begin learning things about human behavior. And so that is a significant advantage. Then they can translate that to a whole variety of applications.

Ms. STEFANIK. Thank you.

Another topic that you touched upon in your opening statements but I don't think we have dived into is genomics and synthetic biology. With respect to health care, gene editing, and synthetic biology, we have seen China position itself with plentiful and very low-cost gene-editing technologies. You've referenced the genetic research center, China is home to the largest genetic research center.

China also has passed laws making it illegal to export healthcare and genomic data about the Chinese population, that combined with some of their recent hacks on U.S. healthcare systems that were attributed to China. Can you discuss what your concerns are in this area?

Mr. SCHARRE. Yes. So this is, I mean, an area that is—we are seeing these incredible fundamental breakthroughs because now computer costs have driven down the cost of sequencing the human genome. So it will accumulate not just individual genomes, but large dataset, and they are beginning to do analysis across them.

It is almost hard to overstate how significant this could be in the long term. We are talking about understanding human biology, changing the actual code of human biology. And so that is places where we want to be a dominant player, and we want to think about how do we protect that kind of genetic data.

You know, how do we protect—I think this is a broader policy question really involving both national competitiveness, but also privacy issues of the United States, things like who owns your genome, right, who owns your genetic data, who has access to that.

When you look at cybersecurity practices today, right, if we can't protect people's credit card numbers and OPM data and their Equifax data, the idea that we are building giant databases that have human genomes in them is a little bit actually scary, right? And so I think we need to think hard about how we begin to protect that data.

Ms. STEFANIK. Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair.

If we could just go back to—so I could clarify the investment that China is making in AI and what we are investing in AI, it is a little confusing. And I just want to understand when you talk about \$7 billion and that is just with the city—the two Chinese cities,

and then our R&D investment in AI is \$1.1 billion for the U.S. Government.

Are we comparing apples and apples in terms of the total investment of—in AI, both government and private sector on both, or is this—are you talking about just government to government?

Mr. CARTER. So that comparison is not strictly apples to apples. I think that the key point is that if you look at everything that the U.S. Government is doing, it amounts to a tiny amount of actual direct funding for research in AI. I think that statistic came from the report from a couple years ago, the NSIC [National Security Investment Consultant Institute] report.

And what you see in China is they have investment at all levels of government, so those municipal governments are investing. Beijing just announced that they are going to build a new AI center that is going to be kind of an off shot of Zhongguancun, which is an innovation center in the center of Beijing.

But if you look at the private sector, I do think that is an area where we have a huge advantage. Part of it is that U.S. companies are investing huge amounts of money in AI. Part of it is that U.S. investors are, I think, smarter technology investors than Chinese investors. They have got decades of experience doing it. People have been throwing money at all kinds of crazy ideas in Silicon Valley for, you know, 40-plus years.

So when you look at what is happening in China, they are putting a lot of money into companies and into technologies that I don't think will necessarily actually bear fruit. So on the private sector side, I think we are putting in a lot of money and we are making better investments. On the government side we are putting in essentially no money, and there is probably room for us to do more.

Mr. LANGEVIN. Yeah, I would agree to do both. And having that collaboration with the private sector, you know, purchasing commercial off-the-shelf also is something where we can leverage the amazing investments that the private sector is making as well. But I think it is important that the government invest in this R&D technology as well, without a doubt.

Let's also talk to something else. I know we have touched on this a bit, but to give you an opportunity to expand on it. You know, I believe a comprehensive whole-of-government approach is needed to maintain U.S. technological advantage. And it also—it must include investment in our future workforce and collaboration of all agencies.

I also believe the strategy should not be focused on countering activities of one country, but rather should force a culture of innovation. And so what are your thoughts on this issue? Again, I know we have touched on this, but further thoughts that you would like to share on this.

And also what are your recommendations for Congress for policies that maintain our technological edge in critical areas by appropriately addressing exploitations in activities of other nations while also fostering a culture of innovation in the U.S.?

And the other thing, if we don't get it, if you can maybe touch on it before the time runs out, China is a keen competitor in the international community in developing regulatory mechanisms and

addressing legal and ethical issues regarding the use of emerging technologies.

In your view, how can the U.S. remain the leader in the international community for developing regulatory policies, setting of international norms, and addressing ethical issues in adopting sound doctrine for emerging technologies?

You know, it was a real wakeup call for me when I heard Elon Musk talk about artificial intelligence being the biggest fundamental existential threat in the existence of mankind that we face today. So how do we make sure that other nations are using—developing and using these technologies responsibly and that we are leading in that area as well?

Mr. CHENG. Sir, one of the things that we can take away from the U.S. versus Chinese experience on the internet is that the Chinese very much want only nation-states to have a say in the establishing regulations. They have really hated ICANN [Internet Corporation for Assigned Names and Numbers] and wanted to move administration of the internet to the U.N.'s [United Nations] International Telecommunications Union.

I would suggest that that is not in our interest for multiple reasons, not least of which is that our private sector is vibrant and powerful. We should, therefore, be a strong advocate for a multi-stakeholder approach in the development of rules, norms, standards, including in the areas of artificial intelligence and genetic engineering.

Mr. SCHARRE. You know, when it comes to fostering U.S. competitiveness, I mentioned this before, what I really think the most essential thing is human capital. We have talked for example on CFIUS and the balance of, you know, constraining foreign-directed investment. But dollars are fungible; people are ultimately the most valuable asset in innovation.

And so I think things like investing in STEM [science, technology, engineering, and math] education in the United States and then encouraging immigration policies that look for bringing the best and brightest over and keeping them here are really essential so that we remain a place where people want to come, want to innovate, want to build new technologies and new companies.

Mr. CARTER. I would agree, and I would add that I think there is an overlap between the two themes that you talked about. So one of the greatest advantages of the U.S. private sector over the Chinese private sector is that our companies are global.

You talk about 30 percent of the data—the world's data is going to be in China. Well, we have a huge advantage on the other 70. U.S. companies—China has 1.4 billion people. China has—Facebook has over 2 billion users. The largest social media platforms, communications apps, email services are all based in the United States.

So much of the data that is being generated in other countries is our data. So that goes to your point, Mr. Langevin, that we need to establish relationships, build communities of like-minded nations in order to give ourselves an advantage of scale. That has always been China's greatest advantage.

Ms. STEFANIK. Time is expired.

Dr. Abraham.

Dr. ABRAHAM. Thank you, Madam Chair.

As much as AI gives me pause, synthetic biology gives me more. Because we are to the point with CRISPR/Cas9 [Clustered Regularly Interspaced Short Palindromic Repeats] where we can modify not only single genome or genes, but an entire sequence of genes.

But going back to the chairwoman's comment and Mr. Langevin's, yes, state players certainly want rules and regulations in place that control this because we know where this can lead. We have truly gone from science fiction to reality, and if not now, very soon.

But there are groups globally that are very, very well-funded that could take this technology and do very, very evil things with very limited resources as far as labs. We know CRISPR/Cas9 can be done in any normal molecular biology lab and then right now.

Just an opinion, because I understand it is that, is there anything we as Americans, we as Congress, we as a group of people with moral standards can do to limit our—you can't put the genie back in the bottle, literally. But is there anything that could be done to prevent some of the potential that is out there? And I know it is a very subjective question, but I would like your opinions.

Mr. SCHARRE. Yeah, I think on biotechnology threats, the most significant thing we can do is invest in things that might involve responses or defenses. So government organizations like Defense Threat Reduction Agency or CDC [Centers for Disease Control and Prevention] that will be thinking about how to respond to natural or artificial pathogens and ways to react to that.

In part because the nature of information technology is such that constraining it is so very difficult, because it is not something like stealth. The essence of it is information. It spreads very easily. These techniques are widely available, and so we are going to have think about how we prepare ourselves for a world where there may be potentially, in the long term, somewhat scarier threats on the horizon.

Dr. ABRAHAM. Mr. Cheng.

Mr. CHENG. I hope that this never comes to pass.

Dr. ABRAHAM. That is wishful thinking.

Mr. CHENG. Yes, sir. But if it does, I think it is also going to be very important that the response, not just the medical response but the law enforcement legal response, be swift and be punitive.

To make—if deterrence is going to work against nation-states, we have a—ironically, we have more options. But against non-state actors and things like that, we need to make very clear that you cannot hide, that you cannot get away with this, that there will not be some kind of excuse made, well, but they are an oppressed peoples, or, gee, you know, we can't, you know—it needs to be swift and it needs to be sure and it needs to be strong, because that is the only way you are going to deter—you may not deter the first incident, but hopefully you can deter the second or third.

Dr. ABRAHAM. Mr. Carter.

Mr. CARTER. I agree. I really hope this never comes to pass. I would just add that one of our great defenses is the ethical framework of the scientific community. I think that around the world you have people who have come through a certain set of institutions

that instill within them a certain set of values. In the short term, I hope that that is enough to keep us safe.

Longer term, the only thing that I would add to what my colleagues said is there will probably come a time when we need to think about how we can use these technologies to make ourselves stronger and more resilient against some of these threats.

Biotechnology is like AI or quantum in many ways, in that I think the technology presents the threat, but it can also present solutions to the threat and so we should look into that.

Dr. ABRAHAM. Thank you, Madam Chair.

Ms. STEFANIK. Ms. Speier.

Ms. SPEIER. Thank you.

Yeah, we have talked a number of times in this last hour about CFIUS and the reforms that CFIUS needs. You have spoken in generalities for the most part. Could you give us some specifics of the kinds of things that should be reforms that we undertake?

Mr. SCHARRE. Certainly. I think the things that would make sense would be expanding the scope of CFIUS so that it enables—

Ms. SPEIER. By scope—you said that before. Tell us what you mean by scope?

Mr. SCHARRE. Right. So in two particular ways. One, that it covers potentially more—that it is triggered by a wider variety of more commercial activities, so foreign investment at maybe a lower level, a percentage of investment in that company.

Ms. SPEIER. What is it now?

Mr. SCHARRE. I want to say it is 50. I have got it right here. Fifty percent, I want to say. So lower than that, like down by 25, and then looking at maybe other things like joint commercial ventures or other types of commercial activities that might cover.

I think the second thing would be expanding the type of technologies that you are doing. And I think probably the best approach there, because of the challenge of sort of some of these technologies be evolving, will be giving the executive some flexibility in creating a list of technologies that fall into the scope that might be reviewed periodically they would have to report back to Congress on.

Ms. SPEIER. Mr. Cheng.

Mr. CHENG. In this case, I think it may be not an issue of reform, but establishing a new entity, perhaps embedded within something like the Securities and Exchange Commission, Department of Treasury, Department of Commerce that would be overseeing and monitoring investments in new developing technologies, joint ventures, and things like that, not by outsiders, but by entities that may be influenced from abroad.

As I said earlier, a joint venture company, where did the capital come from? Who is sitting on that board? How are they going—what kind of access did a—newly developed intellectual property, possibly in technologies that we don't even recognize could be in the longer term strategically important.

That is not a CFIUS role right now because, again, it is not an outside investor, but this is something that I think especially, when we look at the Chinese and others, they recognize that it is start-ups, it is new technologies, especially cutting-edge, where the long-

term strategic consequences simply can't be predicted. So the Chinese and others invest in everything in the expectation that you may have longer-term payouts and payoffs.

Ms. SPEIER. Mr. Carter.

Mr. CARTER. I would say that—well, with what Mr. Scharre was referring to, I think it is the issue of noncontrolling investments. So control has always been a key principle for CFIUS. Does a foreign entity control a U.S. company?

And I think that that is where there is a lot of room to say we need to think about a broader issue than them controlling the company. It is them having access to the company, to its way of thinking, to its technology.

Also, I think I mentioned earlier, this idea of enabling commodities. Of thinking not just in terms of what are technologies we don't want other people to have but what are—what is a resource base that we want the United States to have and that we don't want other countries to have that feeds into technology, things like data. China will have 30 percent of the world's data. Do we need to give them our data as well?

And then the last thing that I would add is, I think CFIUS already has a mechanism. Often, instead of rejecting a deal they propose constraints, firewalls within companies, internal procedures which can be used to address some of the issues that can arise from foreign control of the company or foreign investment in the company.

I think we definitely need to keep that as an element of our CFIUS strategy because we want to make—we want to have an open investment environment. We want to be part of a global investment ecosystem. But there are other ways than blocking deals that we can ensure that companies aren't being used to transfer technology out of the United States.

Ms. SPEIER. Francis Collins, maybe 2 years ago, who was, in fact, one of the creators or the—one of the individuals who was able to decipher the genome, was invited to China. And he went to what was a shoe factory previously and was shown this lab, so to speak, with 3,000 Chinese working on the genome. For all intents and purposes, have they eclipsed us?

Mr. CARTER. It is not just a question of the number of people that are doing it. And in synthetic biology and artificial intelligence in particular, quantum as well actually, I think you would get pretty broad consensus from people in the field that there is a huge difference between the top 50 percent, the top 10 percent, the top 1 percent and the top 1 percent of the 1 percent.

They may have more people doing it, but I do think that the best people in many of these fields are still in U.S. institutions.

Ms. SPEIER. That is a little bit of good news. Thank you.

I yield back.

Ms. STEFANIK. Mr. Khanna.

Mr. KHANNA. Thank you, Madam Chair.

You had said that the key is for our military Department of Defense to harness the—what is going on in the private sector and to—in artificial intelligence. And so I had a two-part question. One, if we were to create a center like the Defense Innovation Board recommends, do you think it would be better to house that within the

Department of Defense, or would it be better to have something like that outside like we have at Los Alamos or Sandia? What would be better?

And second, what would you say is the importance of Google and some of these tech companies in Silicon Valley to our national security? The reason I ask that is, you know, Steve Bannon is very concerned about the threat of China, and yet, he also often refers to my district as the technology lords. And I wonder with too many agency [inaudible], I wonder what people would think of technology in Silicon Valley as critical to our national security.

Mr. SCHARRE. I do think an AI innovation center would make sense for the Department of Defense. It would be a different kind of entity than if you created a national-level one. I think it makes sense for DOD, because I see the central problem is DOD's ability to import this technology.

It is not that we need to create a government agency or government entity to create artificial intelligence. These companies are doing it. It is that we need something inside, really a strong and central organization inside DOD that can allow the import of these into the military kinds of space. And so I think that that is certainly valuable.

Mr. CARTER. I completely agree. And I think that it is not just a question of setting up an AI center. It is also addressing the perennial challenge of Federal acquisitions, particularly defense acquisitions.

If we acknowledge that the private sector is the main engine of innovation in a lot of these key fields, and if we acknowledge that these technologies are going to be the basis of military advantage going forward, we can't ask programs like DIUx and In-Q-Tel, which are a tiny part of Federal acquisitions, to provide the bulk of our capabilities going forward.

So we either need to make those kinds of programs a much bigger part of our overall acquisitions machine or we need to fix our overall acquisitions machine so that it can actually tap into these technologies effectively.

Mr. CHENG. I mean, the reality here is that for Google, for Facebook, for Microsoft, DOD is a relatively small piece of their market. The problem is, DOD still acts as though this is the 1950s and these companies should appreciate all the work and budgetary dollars and, therefore, should be more than happy to comply with a defense Federal acquisition system that I think many, many, many people would agree is badly broken.

So the other issue here is if you set up this center for artificial intelligence, you can lead the horse to AI. But getting services, et cetera, to accept it—when we look at, for example, the resistance that we see towards unmanned aerial vehicles and unmanned underwater vehicles in terms of their ability to be integrated into the current system—this is a relatively mature technology, comparatively speaking—there is a lot of bureaucratic opposition, I would suggest.

And I am not sure that a center like this—this is not an argument against it. But it is not—creating one is not going to somehow magically have everybody sort of say, oh, well, okay, then, you know, I will be happy to accept a model 700 in my command post.

Mr. KHANNA. And any quick comments on how important tech companies in Silicon Valley are to our national security?

Mr. SCHARRE. I think in principle they are vitally important, but we need to make sure that we are actually leveraging that also for national security purposes then.

Mr. CARTER. I would also add that our adversaries clearly see them as important, which is why, for example, they subject them to industrial espionage, cyber attacks every day.

In some ways, I think we are asking them to actually be soldiers particularly in the information domain and fight on our behalf, but they are not really being compensated for that. And we don't have a strategy for how that is integrated with our national defense capabilities, and we probably need to address that.

Mr. KHANNA. Thank you.

Ms. STEFANIK. Thank you to our witnesses, and thank you to our members for their excellent questions and the excellent testimony.

As I mentioned in my opening statement, this is a critically important topic that we will continue to focus on in future hearings and as we continue to develop the NDAA [National Defense Authorization Act], specifically the science and technology budget.

Thank you very much. And with that, this meeting is adjourned. [Whereupon, at 3:40 p.m., the subcommittee was adjourned.]

A P P E N D I X

JANUARY 9, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JANUARY 9, 2018

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee
China's Pursuit of Emerging and Exponential Technologies
Jan. 9, 2018

The subcommittee will come to order.

I would like to welcome everyone to our first Subcommittee event for 2018. Today we will examine China's Pursuit of Emerging and Exponential Technologies and the resultant impact on U.S. national security.

This is a critically important topic and will inform our future events, including the Science and Technology budget for the Department of Defense, and the continuation of the reform and Innovation efforts this committee has promoted over the past several years. Our committee, and ETC in particular, has most recently reviewed in detail China's advances in cyber capabilities and information warfare, and also monitored their development of advanced weapons systems such as hypersonics and directed energy. But this hearing will take a broader focus and touch on many of the newer technologies that China is investing in to support their national objectives.

China continues to increase their research and development investments at an alarming pace, and is rapidly closing many of their technology gaps. More and more, we see China using only domestic Chinese firms and creating high market-access barriers to support domestic capacity. The effect is to replace any and all dependency on foreign companies, investments, and technologies. Aside from the obvious economic benefit of China being able to create millions of high-paying, high-skill jobs – there are also obvious national security implications should they corner the market on advanced technologies critical to national security. We also see them aggressively moving to acquire enabling commodities such as data – and current trajectories have China on track to have roughly 30% of the world's data by 2030.

Many of China's published National-level plans, such as achieving dominance in Artificial Intelligence by 2030, indicate a top-down, government-driven agenda that provides a road-map for strategic collaboration between industry, academia, and their civil society. These plans, when combined with resourcing, effort, and patience, may propel China to leap ahead in many of the technology sectors we will talk about today.

Most notably, China's leadership appears to recognize the connection between the development of many of these advanced technologies and economic growth. This is something we should remind ourselves of as we continue to examine this important topic; perhaps it is a lesson we need to re-learn amidst our debates on Sequestration and Continuing Resolutions.

But China's dominance in many of the technology sectors we will discuss today is not a forgone conclusion. What we learn today and in future hearings must

be translated into action – to inform and reform the Department of Defense in support of national level efforts, so that the United States remains home to the world’s leading experts, researchers, and technological breakthroughs.

Today’s hearing is also timely because of the organizational changes currently underway in the Pentagon, namely the re-establishment of the Under Secretary of Defense for Research and Engineering.

I firmly believe that the Under Secretary for R&E needs to be the prime mover to drive change and foster innovation within the Department. A primary mission of this office should be to provide distinct direction and leadership to energize the Defense Industrial Base, the military services, the Department of Defense labs, and to guide even newer initiatives such as the Strategic Capabilities Office, the Defense Innovation Unit – Experimental (or DIUx), the Defense Digital Service, and the Algorithmic Warfare Working Group. And while many of these newer initiatives have created tremendous momentum and energized a conversation about changing “the culture” of the Department of Defense, much more needs to be done to make these more than one-off quick gains.

If properly empowered and resourced, I also believe that the Under Secretary for R&E will be in a unique position to drive a national level dialogue for Science and Technology policy that will – in addition to helping maintain a battlefield advantage – energize our domestic Industrial Base and provide technology jobs and opportunities across many of the sectors we will talk about today.

We have significant expectations of Dr. Mike Griffin – the nominee to be the Under Secretary for Research & Engineering – but we do so while also offering him our support and confidence – because the threats we face from China and others demand that we energize and organize our government to ensure that Policy keeps pace with Technology in order to define a National Science & Technology strategy, and to close the gap with China.

To guide us through this important topic of China’s pursuit of emerging and exponential technologies we have before us a panel of experts:

- Mr. Dean Cheng, Senior Research Fellow with the Asia Studies Center at the Heritage Foundation.
- Mr. Paul Scharre, Director and Senior Fellow with the Technology and National Security Program at the Center for a New American Security
- And –
- Mr. William Carter, Deputy Director and Fellow with the Technology Policy Program at the Center for Strategic and International Studies.

Welcome to all three of our witnesses and we look forward to your testimony.

Thank you again to our witnesses for being here today. Mr. Cheng, we will begin with you.



CONGRESSIONAL TESTIMONY

China's S&T and Innovation Efforts
Testimony before the
Armed Services Committee
Emerging Threats and Capabilities Subcommittee
U.S. House of Representatives
[January 9, 2018]

Dean Cheng
 Senior Research Fellow, Asian Studies Center
 The Heritage Foundation

My name is Dean Cheng. I am a Senior Research Fellow in the Asian Studies Center at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Over the past forty years, since Deng Xiaoping began his policy of “Reform and Opening,” the People’s Republic of China (PRC) has evolved from a less developed country to the second largest gross domestic product (GDP) in the world. Over the past 25 years, it has also steadily transformed the People’s Liberation Army (PLA) into a force that is capable of influencing regional, and increasingly global, security environments.

An essential element of this growth, both in terms of China’s economy and military, rests upon its ongoing investments and support for science and technology, including in critical technology areas.

A Long-standing Emphasis on Science and Technology (S&T)

Chinese leaders have long viewed science and technology as an essential part of China’s “comprehensive national power (*zonghe guojia liliang*; 综合国家力量).” Comprehensive national power reflects the various factors that influence a nation’s capabilities and international standing. It includes national military and economic strength, political unity, and diplomatic standing. An essential element of comprehensive national power is the nation’s level of scientific and technological development.

By Beijing’s Chinese calculations, a capable scientific and technological base is essential in order to achieve economic autonomy. A state that has substantial capabilities in this regard, they believe, can chart its own course, determining what kinds of industries it will develop. Moreover, it can reap significantly better returns on its investments, by moving higher up the value chain. By contrast, a nation with a weak scientific and technological base will likely be relegated to subcontracting to other states, and will find it hard to break into those areas with better returns on investment.

CONGRESSIONAL TESTIMONY

At the same time, science and technology are increasingly linked to military capacity. While militaries in the Industrial Age could rely on mass to overwhelm an adversary, in the Information Age, it is quality, as well as quantity, that matters. Chinese military and political leaders, analyzing the conflicts since the first Gulf War (1990–1991), have clearly concluded that the PLA can no longer rely on barely trained militia equipped with “rifles and millet” as they did during the Mao Zedong era. Instead, they have focused on developing ever more sophisticated weapons in order to “fight and win future informationized local wars.”

To this end, Chinese leaders have consistently supported programs that promote the PRC’s scientific and technological capacity and support innovation.

Deng Xiaoping put in place “Plan 863,” also known as the Program for High-Technology Research and Development. In March 1986, four leading Chinese scientists (who were also part of the military industrial complex) approached Deng, and urged him to support investments in high technology. Only by increasing China’s scientific base, they argued, could the PRC hope to compete in the long term with the Soviet Union and the West. Deng authorized the creation of Plan 863, which directed investments of human, physical, and financial capital towards seven key high-technology areas:

- 1) Automation,
- 2) Biological sciences and genetic engineering,
- 3) Energy,
- 4) Information technology,
- 5) Lasers,
- 6) Advanced materials, and
- 7) Aerospace technology.¹

Thirty years later, Plan 863 continues to support advanced research in these areas, as well as telecommunications and marine sciences (which were added to Plan 863’s purview in the 1990s).

Under *Jiang Zemin*, who became Party General Secretary and national leader in 1992, the PRC began to push investments in interdisciplinary research under “Plan 973,” also known as the National Basic Research Program of China. While oriented more towards basic (rather than applied) research, it supported a variety of efforts. Jiang also put in place two major programs (“Plan 985” and “Plan 211”) to improve China’s universities to world-class standards. As China produces tens of thousands of engineers and scientists every year, many of these are likely to have benefited from the additional resources allocated to these universities.

Hu Jintao made “indigenous innovation” one of his signature catch phrases. During Hu Jintao’s administration (2002–2012), the PRC issued the “National Medium to Long-Term Plan for the Development of Science and Technology.” This called for China to become a major source of global innovation by 2020, allocating 2.5 percent of GDP to research and development. The Medium to Long-Term Plan includes an array of engineering and scientific megaprojects, as well as “frontier technologies” which align with those previously enumerated as part of Plan 863.

¹Micah Springut, Stephen Schlaikjer, and David Chen, *China’s Program for Science and Technology Modernization: Implications for American Competitiveness* (Washington, DC: Government Printing Office, 2011), p. 27, http://sites.utexas.edu/chinaecon/files/2015/06/USCC_Chinas-Program-for-ST.pdf (accessed January 5, 2018).

Table I-1 Key Areas, Technologies, and Programs Identified in China's Medium- and Long-Term Plan for Development of Science and Technology*

Key Areas (11): • Agriculture • Energy • Environment • Information technology industry and modern services • Manufacturing • National defense • Population and health • Public securities • Transportation • Urbanization and urban development • Water and mineral resources	Frontier Technologies (8): • Advanced energy • Advanced manufacturing • Aerospace and aeronautics • Biotechnology • Information • Laser • New materials • Ocean
Engineering Megaprojects (16): • Advanced numeric-controlled machinery and basic manufacturing technology • Control and treatment of AIDS, hepatitis, and other major diseases • Core electronic components, high-end generic chips, and basic software • Drug innovation and development • Extra-large-scale integrated circuit manufacturing and technique • Genetically modified new-organism variety breeding • High-definition Earth observation systems • Large advanced nuclear reactors • Large aircraft • Large-scale oil and gas exploration • Manned aerospace and Moon exploration • New-generation broadband wireless mobile telecommunications • Water pollution control and treatment	Science Megaprojects (4): • Development and reproductive biology • Nanotechnology • Protein science • Quantum research

During Hu's administration, the Chinese Academy of Sciences, a key part of China's research and scientific organizational infrastructure, also released a massive series of reports highlighting key Chinese technology targets by 2050. These included energy, aerospace technologies, advanced manufacturing, advanced materials, information technology, and oceanographic research.² Hu also encouraged foreign direct investment—and also often required high-technology industries to open research campuses in China as part of those investments.

Under *Xi Jinping*, this emphasis on science and technology and innovation has continued unabated. In February 2016, a new key high-technologies program was announced. This would merge several ongoing programs, including Plan 863 and Plan 973, and reorganize them into five lines of effort.³

1) Natural sciences,

*From U.S. National Research Council, *The New Global Ecosystem in Advanced Computing: Implications for U.S. Competitiveness and National Security* (Washington, DC: The National Academies Press, 2012), p. 102.

²China Academy of Sciences, *Innovation 2050: Science, Technology, and China's Future* (Beijing, PRC: Science Publishing House, 2009).

³"China Inaugurates National R&D Plan," *Xinhua*, February 16, 2016, http://news.xinhuanet.com/english/2016-02/16/c_135104108.htm (accessed January 5, 2018).

CONGRESSIONAL TESTIMONY

- 2) Major science and technology projects,
- 3) Key technologies R&D plan,
- 4) Technical innovation, and
- 5) Human resources for science and technology.

China's S&T and Innovation Players

These various programs have supported efforts by an extensive cross-section of Chinese institutions, reflecting not simply a *whole-of-government* approach to promoting science and technology, but a *whole-of-society* approach. The Chinese have employed all the various tools at their disposal, from their own substantial human capital to business deals to economic espionage, to foster and improve their scientific and technological prowess. Most important, arguably, has been the massive array of domestic research institutes and entities. These include:⁴

The Chinese Academy of Sciences. With a staff of some 50,000 and an array of 100 subordinate institutions, this is the leading institution of Chinese scientific endeavors.

Government Research Institutes. The various governmental ministries have their own research institutes, which provide more focused research on topics related to their areas of specialization.

Institutions of Higher Education. As noted earlier, Jiang Zemin began a program to improve China's universities and elevate them to world-class status as research institutions. This has been concomitant with a major expansion of China's scientific human capital. One research report concludes that China is the world's foremost producer of undergraduates with degrees in science and engineering, representing one-quarter of the global annual output. The report also concludes that the PRC produces more doctorates in natural sciences and engineering than any other nation.⁵

Industrial Enterprise Research Entities. This includes both research at state-owned enterprises (SOEs) and that at privately run corporations. For certain key sectors, such as aerospace, the supporting industries are still SOEs. One example is the Chinese Aerospace Science and Technology Corporation (CASC), which is one of the two main conglomerates in China's space industrial complex. CASC is a massive entity, with 90,000–120,000 employees and eight subordinate academies. Each of these academies, in turn, has an array of research laboratories and institutes, and some even have their own universities.

Not all Chinese research is conducted through state-owned or state-directed enterprises, however. Chinese *private companies* are increasingly part of the landscape of Chinese science and technology. In October 2017, Jack Ma, perhaps China's wealthiest man and head of the private company Alibaba, announced that his company would be investing **\$15 billion** over the next three years in a massive R&D push. This would include "projects in areas such as data intelligence, financial technologies, quantum computing, and machine learning."⁶

The Alibaba research initiative reflects China's growing economic clout. Chinese authorities recognize that many companies desire to be part of the Chinese market, and have therefore taken advantage of this to access key

⁴This section draws from Micah Springut, Stephen Schlaikjer, and David Chen, *China's Program for Science and Technology Modernization: Implications for American Competitiveness* (Washington, DC: Government Printing Office, 2011), pp. 18–22, http://sites.utexas.edu/chinaecon/files/2015/06/USCC_Chinas-Program-for-ST.pdf (accessed January 8, 2018).

⁵Reinhilde Veugelers, *The Challenge of China's Rise as a Science and Technology Powerhouse*, Bruegel Policy Contribution No. 19, July 2017, <http://bruegel.org/wp-content/uploads/2017/07/PC-19-2017.pdf> (accessed January 5, 2018).

⁶Saheli Choudhury, "Alibaba Says It Will Invest Over \$15 Billion Over Three Years in Global Research Program," CNBC, October 11, 2017, <https://www.cnbc.com/2017/10/11/alibaba-says-will-pour-15-billion-into-global-research-program.html> (accessed January 5, 2018).

CONGRESSIONAL TESTIMONY

technologies. Chinese authorities have welcomed foreign direct investment in the PRC—but foreign companies are generally required to form joint ventures with Chinese partners, who in turn will have access to key processes and intellectual property. The ability even to form a joint venture is often predicated upon the willingness to transfer technology, processes, or patents to the PRC.

Augmenting these various open efforts has been an extensive economic espionage program. This has included the use of PLA assets to acquire information and technology. The indictment of five Chinese military officers in 2014 by the U.S. Department of Justice was not for military spying, but for “computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries.” The officers were specifically accused of stealing information “that would be useful to their competitors in China, including state-owned enterprises.”⁷

Expanding Payoffs

These various efforts have already begun to bear significant fruit. From being primarily reliant on foreign technology, Chinese scientists have scored a number of major innovations and successes in recent years. These include achievements in:

Genetic Engineering. Chinese scientists have been the first to conduct human trials involving cells modified through Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) gene-editing technology. This includes a case involving aggressive lung cancer,⁸ and another involving editing cloned human embryos with genetic diseases.⁹

Space Systems. China will launch a lunar lander to the far side of the Moon in 2018, something neither Russia nor the United States have done before (despite much more extensive lunar exploration programs). In order to support this mission, the Chinese are also deploying a data-relay satellite to Lagrange Point-2, one of the five points in the Earth-Moon-Sun system where the various gravitational fields create “parking spots.” While a number of nations have deployed scientific satellites to various Lagrange points, China will launch the first data-relay satellite to such a location in 2018, in support of its pioneering far-side lander mission.¹⁰

China has also deployed the first quantum computer on a satellite, launching Micius in August 2016. In August 2017, they used the quantum satellite to transmit data 1200 kilometers, an unprecedented distance.¹¹ This was followed in September 2017 with a videophone call from Beijing to Vienna, which was encrypted using keys generated on the satellite.¹²

⁷News release, “US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and Labor Organization for Commercial Advantage,” U.S. Department of Justice, May 19, 2014, <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (accessed January 5, 2018).

⁸David Cyranoski, “CRISPR Gene-Editing Tested in a Person for the First Time,” *Nature*, November 15, 2016, <https://www.nature.com/news/crispr-gene-editing-tested-in-a-person-for-the-first-time-1.20988> (accessed January 5, 2018).

⁹David Cyranoski, “Chinese Scientists Fix Genetic Disorder in Cloned Human Embryos,” *Nature*, October 2, 2017, <https://www.nature.com/news/chinese-scientists-fix-genetic-disorder-in-cloned-human-embryos-1.22694> (accessed January 5, 2018).

¹⁰Leonard David, “China Launching Lander, Rover to Moon’s Far Side This Year,” *Space.com*, January 4, 2018, <https://www.space.com/39275-china-change-4-moon-mission-launch-2018.html> (accessed January 5, 2018).

¹¹Arjun Kharpal, “China Uses a Quantum Satellite to Transmit Potentially Unhackable Data,” *CNBC*, August 10, 2017, <https://www.cnbc.com/2017/08/10/china-uses-quantum-satellite-to-transmit-potentially-unhackable-data.html> (accessed January 5, 2018).

¹²Amy Nordrum, “China Demonstrates Quantum Encryption By Hosting a Video Call,” *IEEE Spectrum*, October 3, 2017, <https://spectrum.ieee.org/tech-talk/telecom/security/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call> (accessed January 5, 2018).

Information Technology. China's advances in quantum computing are part of a larger effort that has seen China rise to the top in certain key areas of information technology. China, for example, has the world's fastest and second fastest super-computers (Sunway TaihuLight and Tianhe-2, respectively); the fastest U.S. supercomputer ranks fifth.¹³ It should also be noted that the Sunway TaihuLight uses *only* Chinese-manufactured microprocessors, reflecting the maturing of China's microprocessor industry.¹⁴

Chinese leaders have meanwhile echoed Vladimir Putin in emphasizing the need to develop artificial intelligence (AI). In July 2017, Beijing issued the "New Generation Artificial Intelligence Plan," outlining China's goal to become a major center for artificial intelligence research and applications by 2030. Alibaba and Baidu, the Chinese search engine, are meanwhile pushing development of AI.¹⁵ In this regard, the massive Chinese censorship infrastructure they have put in place, including the Great Firewall of China, is likely to be a major facilitator in this effort. To some extent, Chinese censors already rely on AI as an initial filter to screen messages for acceptability. This trend will likely accelerate, as China puts in place the "social credit score" which will take even more factors into account—and require even more monitoring.

Drone Technology. Chinese drones span the gamut of sophistication and capability. At one end are dedicated military drones such as the CH-3, CH-4, and CH-5. These resemble American unmanned combat aerial vehicles (UCAVs) such as the Reaper and Predator. In this area, Chinese engineers have deployed an experimental drone to 82,000 feet, substantially higher than the U.S. military's RQ-4 Global Hawk, which had been the previous high flyer at 60,000 feet.¹⁶

At the other end, Dajiang Innovation Technology Corporation (DJI) dominates the consumer drone market. It apparently also collected audio, visual, and telemetry data from its hundreds of thousands of drones used around the world. This has become such a concern that the U.S. Army banned the further use of DJI drones in August 2017.¹⁷

These various advances highlight the increasing synergies among Chinese high-technology efforts. Advances in artificial intelligence help improve drone performance, while the drones themselves provide potential access to tens of thousands of data feeds. Advances in information technology are at the heart of the recent advances in genetic engineering.

The Growing Challenge from Chinese Science, Technology, and Innovation

This brief survey of Chinese technological advances provides a glimpse to the extent of the growing challenge the PRC poses to U.S. technological and scientific preeminence. Indeed, in some areas such as super-computing, it is

¹³Top500 List, November 2017, <https://www.top500.org/list/2017/11/> (accessed January 5, 2018).

¹⁴Patrick Thibodeau, "China Builds World's Fastest Supercomputer Without US Chips," *Computerworld*, June 20, 2016, <https://www.computerworld.com/article/3085483/high-performance-computing/china-builds-world-s-fastest-supercomputer-without-u-s-chips.html> (accessed January 5, 2018).

¹⁵Louise Lucas, "Chinese Tech Groups Look for Edge in Using Artificial Intelligence," *Financial Times*, December 18, 2017, <https://www.ft.com/content/e8bba054-d02f-11e7-b781-794ce08b24dc> (accessed January 5, 2018), and Anthony Kuhn, "Chinese Advances in Artificial Intelligence," NPR, January 1, 2018, <https://www.npr.org/2018/01/01/574985930/chinese-advances-in-artificial-intelligence> (accessed January 5, 2018).

¹⁶Stephen Chen, "China Tests New Spy Drones in Near Space 'Death Zone,'" *South China Morning Post*, October 31, 2017, http://www.scmp.com/news/china/society/article/2117709/china-tests-new-spy-drones-near-space-death-zone?utm_source=edm&utm_medium=edm&utm_content=20171031&utm_campaign=scmp_china&emarsys=1&sc_src=email_2060322&sc_lid=1157&sc_lid=146777614&sc_uid=CdSb7QujVI (accessed January 5, 2018).

¹⁷Bart Jansen, "Army Bans DJI Drones Because of Concerns about Cyber Vulnerabilities," *USAToday*, August 4, 2017, <https://www.usatoday.com/story/news/2017/08/04/report-army-bans-dji-drones-because-concerns-cyber-vulnerabilities/540720001/> (accessed January 5, 2018).

CONGRESSIONAL TESTIMONY

China, not the United States, that is the leader. It is therefore essential that the United States government, including Congress, recognize the nature of the challenge posed by Beijing's science and technology juggernaut.

First, *the PRC is not reliant on stealing technology; it is increasingly an innovator*. China may benefit from reduced R&D costs by engaging in economic and scientific espionage, but the growing number of "firsts" that it has scored, whether in deploying a lander to the far side of the Moon or a quantum communications satellite that can support video telephone calls across continents, should dispel the belief that it is wholly dependent upon exploiting others' innovations. Indeed, the Chinese themselves have emphasized that they do not want to rely on outside technology—as seen with the Sunlight TaihuLight super-computer.

Second, *China is competing with its entire society*. That the PRC has employed its military cyber forces to engage in espionage is already well known. But China's actions go beyond having the military help its economic competitiveness. It is also important to recognize that civilian and nongovernmental entities, in turn, are likely to help military and security efforts. This apparent integration of civilian and military efforts, at least in the realm of computer network operations, is supported by the observation in the 2013 edition of *The Science of Military Strategy* that there are three broad categories of Chinese computer network warfare forces. These are comprised of:

- 1) Specialized military units, specifically tasked for implementing network offensive and defensive operations;
- 2) Specialist units organized with military permission, drawn from local capabilities (e.g., from within a military region or war zone), including the Ministry of State Security and the Ministry of Public Security, and other relevant government departments; and
- 3) Civilian strength, comprised of voluntary civilian participants who can conduct network operations after being mobilized and organized.¹⁸

The PRC government is also likely to *draw upon the resources and personnel of Chinese private companies*. As a Council on Foreign Relations conference report warned, U.S. policymakers should view many Chinese private-sector firms as essentially operating at the behest of the PRC government. "There is little functional distinction between private firms and...[state-owned enterprises], one participant noted; another underscored the role that Chinese state financing plays in lending a political overtone to what might otherwise appear to be private-sector investment decisions."¹⁹

Finally, it is important to recognize that *the PRC's efforts at promoting science and technology, and innovation more broadly, encompasses a variety of approaches*. The American focus is typically on technological innovation; what new widgets might be on the horizon? But there are other forms of innovation. During the 1980s, when there was great concern about Japan's challenge to the United States, it was recognized that companies like Sony and Honda were competing, not by making entirely new things, but by improving how things were made. While the VCR was invented in the United States, it was Japanese companies that manufactured them by the commercial container-load cheaply yet reliably. Japanese production techniques were the innovation.

Similarly, there can be doctrinal and organizational innovation. In 1940, Great Britain and France both fielded more tanks than Nazi Germany. Moreover, many of the Allies' tanks were arguably superior to their German counterparts, on a 1:1 basis. But the Germans had developed the doctrine of *blitzkrieg*, and organized their forces accordingly, whereas the Allies remained wedded to a doctrine that largely saw tanks as subordinate to the infantry, to be dispersed across the front.

¹⁸Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

¹⁹Council on Foreign Relations, "Chinese Investment in Critical US Technology: Risks to US Security Interests," October 16, 2017, <https://www.cfr.org/report/chinese-investment-critical-us-technology-risks-us-security-interests> (accessed January 5, 2018).

CONGRESSIONAL TESTIMONY

Taken together, technological, production, doctrinal, and organizational innovation presents the potential of synergistic, reinforcing developments that can potentially leave an adversary far behind. In the case of the PRC, and especially the PLA, the development of the PLA Strategic Support Force (PLASSF) may well be this kind of fundamental, devastating breakthrough.

The PLASSF brings together China's electronic warfare, network (including cyber) warfare, and space warfare forces. It is noteworthy that no other military has brought these kinds of capabilities into a single force. China has concentrated within a single service forces familiar with a variety of cutting edge technologies, from hacking to space warfare to advanced electronic operations. Not only is PLASSF therefore most likely to benefit from advances in Chinese technologies, but it is organized to develop suitable doctrines to exploit those same advances.

For the United States, then, the challenge from China is likely to be increasingly from a combination of both new technologies that China itself has developed, and old and new technologies organized and employed innovatively. An effective response cannot simply be focused on one or another technological development (although emerging and exponential technologies *can* be game-changers). Instead, it must involve both the U.S. government and the broader American society. It must include flexibility in our approach to organizations, roles, and missions, as well as openness to new technologies. Only in this manner can we effectively meet the Chinese challenge.

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2016, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2016 income came from the following sources:

- Individuals 75.3%
- Foundations 20.3%
- Corporations 1.8%
- Program revenue and other income 2.6%

The top five corporate givers provided The Heritage Foundation with 1.0% of its 2016 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Dean Cheng

Dean Cheng brings detailed knowledge of China's military and space capabilities to bear as The Heritage Foundation's research fellow on Chinese political and security affairs.

He specializes in China's military and foreign policy, in particular its relationship with the rest of Asia and with the United States.

Cheng has written extensively on China's military doctrine, technological implications of its space program and "dual use" issues associated with the communist nation's industrial and scientific infrastructure.

He previously worked for 13 years as a senior analyst, first with Science Applications International Corp. (SAIC), the Fortune 500 specialist in defense and homeland security, and then with the China Studies division of the Center for Naval Analyses, the federally funded research institute.

Before entering the private sector, Cheng studied China's defense-industrial complex for a congressional agency, the Office of Technology Assessment, as an analyst in the International Security and Space Program.

Cheng has appeared on public affairs shows such as John McLaughlin's One on One and programs on National Public Radio, CNN International, BBC World Service and International Television News (ITN). He has been interviewed by or provided commentary for publications such as Time magazine, The Washington Post, Financial Times, Bloomberg News, Jane's Defense Weekly, South Korea's Chosun Ilbo and Hong Kong's South China Morning Post.

Cheng has spoken at the National Space Symposium, National Defense University, the Air Force Academy, Massachusetts Institute of Technology (MIT) and Eisenhower Center for Space and Defense Studies.

Cheng earned a bachelor's degree in politics from Princeton University in 1986 and studied for a doctorate at MIT. He and his wife reside in Vienna, Va.

**DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES**

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Dear Cheng

Capacity in which appearing: (check one)

☒ Individual

☐ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: _____

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

None applicable.

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

January 9, 2018

Testimony before the House Armed Services Subcommittee on Emerging
Threats and Capabilities

China's Pursuit of Emerging and Exponential Technologies

Paul Scharre, Senior Fellow and Director
Technology and National Security
Center for a New American Security

Chairwoman Stefanik, Ranking Member Langevin, and distinguished members, thank you for inviting me to testify today.

We live in a time of dizzying technological change. The information revolution, which has now been underway for several decades, continues to unfold in surprising ways. The United States was a first-mover in information technology. By leveraging advances in the microprocessor revolution in the 1970s and 1980s, the United States led the world in the development of personal computers, the internet, the Global Positioning System (GPS), and other information-based technologies. Today, information technology has spread to nearly every corner of our lives. It has also spread around the world. While the United States is still the global leader in information technology, other nations are now also significant players. China, in particular, is a major and fast-growing player in information technology.¹

As the world's third largest economy behind the United States and the European Union and as the most populous nation in the world, China has major structural advantages that make it a key competitor in information technology. China's population, in particular, is a key source of strength because it is a potential source of data on human behavior and genomics. Combined with a more lax cultural attitude towards data protection and personal privacy, this data can help fuel advances artificial intelligence and synthetic biology.²

The Information Revolution

There are three broad trends underlying the information revolution: the datafication of our world, increasing networking and connectivity, and increasingly intelligent machines. These trends intersect and reinforce each other in powerful ways, and understanding these trends can help in understanding some of China's structural advantages.

Datafication of our world: The modern information economy produces over 2.5 exabytes of data daily (an exabyte is one quintillion bytes, or 10^{18} bytes).³ In the past few years the information revolution has generated more data than existed in the entire 5,000 years of recorded human history. This data comes in a variety of forms: mapping data showing patterns of human activity and the locations of people and things; human communications data showing people's networks and the content of their interactions; search, shopping, and entertainment data showing people's preferences and interests; and as gene sequencing becomes cheaper, the digitization of human genetic data. This trend in the datafication of our world is digitizing and quantifying the world around us: our lives, our bodies, and our likes and desires. Much of this data is unstructured and unlabeled, making it a sea of potential information, if one can sort and organize this data to yield useful insights.

Networking and connectivity: The world is increasingly networked, making it possible to transmit and share this new ocean of digital data. In 2017, global internet users topped 3.8 billion people, more than half of the world's population. Nearly 5 billion people use cell phones – roughly two-thirds of the world. Nearly 3 billion people are active social media users. And global connectivity continues to grow at a breakneck pace. Every day more than a million new people join social media.⁴ As more people come online, their data comes online as well. They, too, become digitized. People and companies are also sharing this data, sending it over networks that are growing in scale and bandwidth. The number of connected devices is growing even faster than internet users. An estimated 20 billion devices will be connected to this sprawling global network in 2018. Internet of Things (IoT) devices, which include smart meters, medical devices, home appliances, and industrial applications, are growing at the fastest rate and by 2021 are expected to account for over half of all connected devices.⁵ These devices create data and share it across a global network that will traffic over 150 exabytes of data per month in 2018. Global internet traffic is growing even faster than connectivity, at a rate of 24% per year. Broadband speeds are increasing to account for this data and are expected to roughly double over the next 5 years.⁶ It is not just the amount of connected people, devices, and data that is increasing, but the volume and speed at which they are communicating.

More intelligent machines: These trends have been made possible because of exponential growth in computer processing power, which enables ever-smaller and more powerful computers, tablets, smartphones, and devices. For the past fifty years, this trend has been encapsulated in a maxim known as Moore's Law, named for Intel co-founder Gordon Moore, which has observed that chip performance has doubled roughly every two years.⁷ The rate of advancement of CPU (central processing unit) performance has slowed in recent years. While still improving exponentially, it has been at a markedly slower pace as chips have approached the nanometer scale.⁸ At the same time, in the past few years there has been an explosion in deep learning, a powerful machine learning technique used to enable artificial intelligence (AI). This has yielded tremendous progress on long-standing AI problems such as object recognition and natural language processing. Deep learning draws on large amounts of parallel computer processing, made possible because of advances in graphics processing units (GPUs) driven by the gaming industry; as well as large amounts of data. In deep learning, deep neural networks train on millions of pieces of data to learn how to recognize objects, translate between languages, or perform many other cognitive tasks. Deep learning systems can even learn from unlabeled data, a process known as unsupervised learning.⁹ Thus, advances in increasingly powerful computer processors have enabled the production of myriad devices that collect vast quantities of data, which in turn have fueled learning machines that can process and make sense of this data.

China's population is a major structural advantage in this information revolution, as it allows the pooling of large amounts of data. China already has 730 million internet users, a figure that will grow as the country becomes increasingly urbanized and connected. Chinese users also appear more comfortable sharing their data than Western counterparts, which companies can use to train more sophisticated algorithms to understand human behavior.¹⁰

China also combines a dynamic private sector with a government that plans and executes long-term strategies to increase China's competitiveness in key technology areas. China has used this in recent years to execute plans to leap forward on artificial intelligence, synthetic biology, and quantum computing, all key technologies tied to the information revolution.

Artificial Intelligence

China is a global leader in artificial intelligence, second only to the United States. Baidu, Tencent, and Alibaba – all Chinese firms – are top-tier AI companies, and China also has a vibrant AI startup scene.¹¹ Since 2014, China has surpassed the United States in the total number of publications and cited publications in deep learning, an important sub-field of AI.¹² The United States still leads the world in AI patents, but China is growing at a faster rate.¹³ While the quantity of publications does not necessarily equate to quality, Chinese AI researchers perform well in international competitions.¹⁴ Chinese teams “dominated” the ImageNet visual image recognition competition for the past two years and a Chinese start-up won the Facial Recognition Prize Challenge hosted by the Intelligence Advanced Projects Agency (IARPA).¹⁵ Overall, Chinese AI researchers are not as experienced as U.S. counterparts, but they are improving.¹⁶ In the 2017 meeting of the Association of the Advancement of Artificial Intelligence (AAAI), there were roughly as many papers accepted from China as there were from the United States.¹⁷

In July 2017, China published a national strategy for artificial intelligence, the “New Generation AI Development Plan.”¹⁸ Under this plan, China's goal is to be the “premier global AI innovation center” by 2030.¹⁹ To achieve this goal, China's plan includes improving in areas where China is currently weak, such as human capital, by focusing on the education and recruitment of top AI talent. As one example, Chinese-born and American-educated AI researcher Qi Lu recently left an executive vice president role at Microsoft to become the Chief Operating Officer at Baidu.²⁰ News reports indicate Chinese firms see the Trump Administration's anti-immigrant policies as an opportunity to draw away top U.S. technology talent, as immigrants are responsible for one-quarter of startups in the United States.²¹

China also has significant advantages in translating private sector advances in AI into national security applications because of its model of military-civil fusion.²² In the United States, the Department of Defense (DoD) has struggled to break down largely self-imposed barriers to working with non-traditional defense companies that lock the DoD out of crucial innovation in places like Silicon Valley. China has a closer relationship between the public and private sector and is able to more easily “spin in” private sector innovations into the military through their strategy of military-civil fusion. This means that not only is China a significant global player in artificial intelligence – with a plan to be the global leader by 2030 – but that China has major advantages in translating these private-sector gains into national security applications.

Synthetic Biology and Genomics

The information revolution has opened up new opportunities in biotechnology as computers have made genome sequencing increasingly affordable. The cost of sequencing the human genome has been falling exponentially at a rate faster than Moore's Law.²³ In turn, the acquisition of large datasets of human genomes has significant research potential, as these datasets can be mined by data analytics and AI for correlations between genes and health outcomes. A Chinese company, Beijing Genomics Institute (BGI), is the world's largest genetic research center. BGI has a U.S.-based center headquartered in Cambridge and has sequenced the genomes of millions of Americans. BGI has robust support from the Chinese government and partnerships with Chinese military research institutes such as the Academy of Military Medical Sciences.²⁴

At the national level, the Chinese government is proactively engaged in developing its biotech sector and has created multiple national-level biotechnology development plans. One of the strategies China uses to advance its biotechnology industry, as in other areas, is "going out" and "bringing in" foreign innovation by investing in foreign companies.²⁵ For example, in 2013 BGI acquired next-generation genome sequencing technologies by purchasing the U.S. company Complete Genomics.²⁶

The importance of genomics is likely to increase as the cost of gene sequencing continues to fall and larger datasets of human genomes are established, making possible large-scale analysis of human genes. Given that the ultimate aim is modifying life itself, it is nearly impossible to overstate the long-term potential of synthetic biology and genomics. As this field matures, China is well-positioned to be a global leader.

Quantum Computing

Quantum computing is another important area of information-related technologies and one in which China has shown striking recent advances. Quantum computing is an entirely different method of computing from current approaches and relies on the unusual properties of quantum physics. Quantum technology has many potential national security applications, including cryptography, remote sensing, and secure communications.²⁷ Chinese researchers have made recent strides in quantum technology, demonstrating a 10-qubit quantum processor and a quantum communications satellite in 2017.²⁸ China is following up on these advances with national-level investments in quantum technologies. China recently launched the Jinan Project, a plan to build a secure quantum computer network, and is building a \$10 billion National Laboratory for Quantum Information Sciences.²⁹

Conclusion

As the world's third-largest economy and most populous nation, China has many inherent structural advantages in competing in high-technology areas. China has a dynamic private sector, with both large established firms and dynamic start-ups, and a large pool of potential talent to draw upon. In places where China has weaknesses, such as the quality of human capital in some fields, China is actively working to improve by recruiting top talent from abroad. China's population, increasingly networked and digitized, is a major source of potential data, which is a critical resource for

information-enabled innovation. One of China's biggest strengths relative to the United States, however, is the government's willingness to develop and follow through on large-scale long-term investment plans in key technology areas. China has repeatedly demonstrated an ability, in multiple technology areas, to acquire foreign expertise by investing in foreign companies and then using that to improve Chinese indigenous capabilities. China's capacity for executing long-term strategies for technology development should not be underestimated, and Chinese plans to become the global leader in critical technology areas such as artificial intelligence should be taken seriously.

Further Reading

For further reading, see:

Michael J. Biercuk and Richard Fontaine, "The Leap Into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks*, November 17, 2017, <https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/>.

Elsa Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, Washington, DC, November 2017, <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.

CNAS Funding

CNAS is a national security research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity. The Center retains sole editorial control over its ideas, projects, and productions, and the content of its publications reflects only the views of their authors. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. Accordingly, CNAS will not engage in any representation or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from foreign sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. A full list of CNAS supporters and the center's funding guidelines can be found here: <https://www.cnas.org/support-cnas>.

Consistent with Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress, a detailed list of CNAS federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years has been provided to this committee as an attachment.

Notes

¹ Chris Dong, "China ICT Market: Trends, Complexity, Potential," presentation, IDC Web Conference, July 6, 2017.

² "The Algorithm Kingdom: China May Match or Beat American in AI," *The Economist*, July 15, 2017, <https://www.economist.com/news/business/21725018-its-deep-pool-data-may-let-it-lead-artificial-intelligence-china-may-match-or-beat-america>. Dong, "China ICT Market," slide 7.

³ IBM, "10 Key Marketing Trends for 2017," 3, <https://public.dhe.ibm.com/common/ssi/ecm/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reports-wrl12345usen-20170719.pdf>.

⁴ Simon Kemp, "The Global State of the Internet in April 2017," *TheNextWeb*, https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/#.tnw_iUhkTTm1.

⁵ CISCO, "The Zettabyte Era: Trends and Analysis," June 7, 2017, <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni-hyperconnectivity-wp.html>.

⁶ Ibid.

⁷ For several decades, computing power doubled roughly every 20 months. Over the past decade, this pace has slowed to every 2 to 2.5 years. Michael Kanellos, "Moore's Law to roll on for another decade," *CNet*, February 11, 2003, <https://www.cnet.com/news/moores-law-to-roll-on-for-another-decade/>; Don Clark, "Intel Rechisels the Tablet on Moore's Law," July 16, 2015, <https://blogs.wsj.com/digits/2015/07/16/intel-rechisels-the-tablet-on-moores-law/?mg=prod/accounts-wsj>. Actual data on transistor count per chip is available at "Transistor Count," OMICS International, http://research.omicsgroup.org/index.php/Transistor_count.

⁸ Top500, "Highlights of the 50th Top500 List," presentation, slides 6-8, <https://www.top500.org/lists/2017/11/slides/>. Tom Simonite, "Moore's Law is Dead. Now What?," *MIT Technology Review*, May 13, 2016, <https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/>.

⁹ Robert D. Hof, "Deep Learning: With massive amounts of computational power, machines can now recognize objects and translate speech in real time. Artificial intelligence is finally getting smart," *MIT Technology Review*, <https://www.technologyreview.com/s/513696/deep-learning/>.

¹⁰ "The Algorithm Kingdom."

¹¹ Elsa Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, Washington, DC, November 2017, <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.

¹² U.S. National Science and Technology Council, "The National Artificial Intelligence Research and Development Strategic Plan," October 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

¹³ "The Algorithm Kingdom."

¹⁴ Kania, "Battlefield Singularity," 8.

¹⁵ Aaron Tilley, "China's Rise In The Global AI Race Emerges As It Takes Over The Final ImageNet Competition," July 31, 2017, <https://www.forbes.com/sites/aarontilley/2017/07/31/china-ai-imagenet/#4bef5f25170a>. "Yitu Tech Wins the 1st Place in Identification Accuracy In Face Recognition Prize Challenge 2017," *PRNewswire*, November 03, 2017, <https://www.prnewswire.com/news-releases/yitu-tech-wins-the-1st-place-in-identification-accuracy-in-face-recognition-prize-challenge-2017-300549292.html>.

¹⁶ Kania, "Battlefield Singularity," 8.

¹⁷ "AAAI-17 Accepted Papers," <http://www.aaai.org/Conferences/AAAI/2017/aaai17accepted-papers.pdf> or Sarah Zhang, "China's Artificial-Intelligence Boom," *The Atlantic*, February 16, 2017, <https://www.theatlantic.com/technology/archive/2017/02/china-artificial-intelligence/516615/>.

¹⁸ "State Council Notice on the Issuance of the New Generation AI Development Plan," August 20, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

¹⁹ Kania, "Battlefield Singularity," 9.

²⁰ "The Algorithm Kingdom."

²¹ Meng Jing, "Chinese firms fight to lure top artificial intelligence talent from Silicon Valley," *South China Morning Post*, April 2, 2017, <http://www.scmp.com/tech/china-tech/article/2084171/chinese-firms-fight-lure-top-artificial-intelligence-talent-silicon>. Adam Bluestein, "The Most Entrepreneurial Group in America Wasn't Born in America," Inc., <https://www.inc.com/magazine/201502/adam-bluestein/the-most-entrepreneurial-group-in-america-wasnt-born-in-america.html>. Nick Wingfield, "In Blow to Tech Industry, Trump Shelves Start-Up Immigrant Rule," *The New York Times*, July 10, 2017, https://www.nytimes.com/2017/07/10/technology/in-blow-to-tech-industry-trump-shelves-start-up-immigrant-rule.html?_r=0. Sara Ashley O'Brien, "Trump administration loses bid to delay Obama's 'startup visa,'" CNN.com, December 2, 2017, <http://money.cnn.com/2017/12/02/technology/international-entrepreneur-rule-delay/index.html>. U.S. Citizenship and Immigration Service, "USCIS to Begin Accepting Applications under the International Entrepreneur Rule," December 14, 2017, <https://www.uscis.gov/news/news-releases/uscis-begin-accepting-applications-under-international-entrepreneur-rule>.

²² Kania, "Battlefield Singularity," 12.

²³ U.S. National Human Genome Research Institute, "The Cost of Sequencing a Human Genome," <https://www.genome.gov/27565109/the-cost-of-sequencing-a-human-genome/>.

²⁴ Elsa Kania, unpublished manuscript.

²⁵ Ibid.

²⁶ Complete Genomics, "About Us," <http://www.completegenomics.com/>.

²⁷ Michael J. Biercuk and Richard Fontaine, "The Leap Into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks*, November 17, 2017, <https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/>.

²⁸ Chao Song et al., "10-qubit entanglement and parallel logic operations with a superconducting circuit," *Physical Review Letters* 119 (2017), <https://arxiv.org/pdf/1703.10302.pdf>. Gabriel Popkin, "China's quantum satellite achieves 'spooky action' at record distance," *Science*, June 15, 2017, <http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance>.

²⁹ Tom Ward, "China Set to Launch the World's First Quantum Communication Network," *Futurism*, July 16, 2017, <https://futurism.com/china-set-to-launch-the-worlds-first-quantum-communication-network/>. Jeffrey Lin and P.W. Singer, "China is opening a new quantum research supercenter," *Australian Popular Science*, October 12, 2017, <http://www.popsoci.com.au/tech/computing/china-is-opening-a-new-quantum-research-supercenter.475275>.

Paul Scharre

Paul Scharre is a Senior Fellow and Director of the Technology and National Security Program at the Center for a New American Security. He is author of the forthcoming book, *Army of None: Autonomous Weapons and the Future of War*, to be published in April 2018.

From 2008-2013, Mr. Scharre worked in the Office of the Secretary of Defense (OSD) where he played a leading role in establishing policies on unmanned and autonomous systems and emerging weapons technologies. Mr. Scharre led the DoD working group that drafted DoD Directive 3000.09, establishing the Department's policies on autonomy in weapon systems. Mr. Scharre also led DoD efforts to establish policies on intelligence, surveillance, and reconnaissance (ISR) programs and directed energy technologies. Mr. Scharre was involved in the drafting of policy guidance in the *2012 Defense Strategic Guidance*, *2010 Quadrennial Defense Review*, and Secretary-level planning guidance. His most recent position was Special Assistant to the Under Secretary of Defense for Policy.

Prior to joining OSD, Mr. Scharre served as a special operations reconnaissance team leader in the Army's 3rd Ranger Battalion and completed multiple tours to Iraq and Afghanistan. He is a graduate of the Army's Airborne, Ranger, and Sniper Schools and Honor Graduate of the 75th Ranger Regiment's Ranger Indoctrination Program.

Mr. Scharre has published articles in *The New York Times*, *Foreign Policy*, *Politico*, *Proceedings*, *Armed Forces Journal*, *Joint Force Quarterly*, *Military Review*, and in academic technical journals. He has presented at the United Nations, NATO Defence College, Chatham House, National Defense University and numerous other defense-related conferences on robotics and autonomous systems, defense institution building, ISR, hybrid warfare, and the Iraq war. He has appeared as a commentator on CNN, MSNBC, NPR, the BBC, and Swiss and Canadian television. Mr. Scharre is a term member of the Council on Foreign Relations. He holds an M.A. in Political Economy and Public Policy and a B.S. in Physics, cum laude, both from Washington University in St. Louis.

**DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES**

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Paul Scharre

Capacity in which appearing: (check one)

☐ Individual

☒ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: Center for a New American Security

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
See attachment			

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
See attachment			

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

**CNAS Federal Contract or Grant Information****2017**

Federal Grant/Contract	Federal Agency	Dollar Value	Subject of Contract or Grant
HQ0034-16-C-0079	DOD, OSD Net Assessment	\$99,608	Long-term Security Risks of Artificial Intelligence
HQ0034-16-C-0085	DOD, OSD Net Assessment	\$155,079	The Return of Marco Polo's World and the U.S. Military Response
Intragovernmental Personnel Act of 1970 Agreement	DOD Policy	\$99,592	IPA forKelley Saylor
H92222-16-D-0013	Gemini Industries Inc.	\$25,000	Sovereign Challenge Conference Study Support
N00244-15-1-0056	PASCC/DOD, NAVSUP Fleet Logistics Center San Diego to CNAS	\$149,645	Managing Escalation and Limiting War in a Conflict in the Western Pacific
Subcontract Number: P010220314; Prime Contract Number: GS00F002CA	Science Applications International Corporation	\$594,214	Quick Reaction Capability Battle Space Awareness Intelligence, Surveillance, and Reconnaissance (QRCBAISR) Support
FA3300-13-G-0014	United States Air Force	\$27,500	USAF Military Senior Fellow
TRNGRA-09Y0902BROW	United States Army	\$27,500	USA Military Senior Fellow
W91QF0-16-P-0031	United States Army War College	\$4,908	2016 Strategy Conference
30-11-G81DCS134-000	United States Coast Guard	\$26,250	USCG Military Senior Fellow
MOU	United States Marine Corps	\$27,500	USMC Military Senior Fellow
MOU Between Deputy Chief of Naval Operations (Information, Plans and Strategy) Strategy and Policy Division (OPNAV N51) and CNAS	United States Navy	\$27,500	USN Military Senior Fellow

2016

Federal Grant/Contract	Federal Agency	Dollar Value	Subject of Contract or Grant
HQ0034-16-C-0079	DOD, OSD Net Assessment	\$99,608	Long-term Security Risks of Artificial Intelligence
HQ0034-16-C-0085	DOD, OSD Net Assessment	\$155,079	The Return of Marco Polo's World and the U.S. Military Response
Intragovernmental Personnel Act of 1970 Agreement	DOD Policy	\$99,592	IPA forKelley Saylor
Subcontract Number: 136968; Prime Contract Number: N00024-13-D-6300	John Hopkins University	\$39,161	Strategic Capabilities Office (SCO) Wargame
N00244-15-1-0056	PASCC/DOD, NAVSUP Fleet Logistics Center San Diego to CNAS	\$149,645	Managing Escalation and Limiting War in a Conflict in the Western Pacific
Subcontract Number: P010220314; Prime Contract Number: GS00F002CA	Science Applications International Corporation	\$594,214	Quick Reaction Capability Battle Space Awareness Intelligence, Surveillance, and Reconnaissance (QRCBAISR) Support
FA3300-13-G-0014	United States Air Force	\$27,500	USAF Military Senior Fellow
TRNGRA-09Y0902BROW	United States Army	\$27,500	USA Military Senior Fellow
30-11-G81DCS134-000	United States Coast Guard	\$26,250	USCG Military Senior Fellow
MOU	United States Marine Corps	\$27,500	USMC Military Senior Fellow
MOU Between Deputy Chief of Naval Operations (Information, Plans and Strategy) Strategy and Policy Division (OPNAV N51) and CNAS	United States Navy	\$27,500	USN Military Senior Fellow

2015			
Federal Grant/Contract	Federal Agency	Dollar Value	Subject of Contract or Grant
HQ0034-15-C-0048	DOD, OSD Net Assessment	\$320,298	Maturing Precision Strike
HQ0034-15-C-0101	DOD, OSD Net Assessment	\$99,900	Leveraging History
Intragovernmental Personnel Act of 1970 Agreement	DOD Policy	\$99,592	IPA for Zachary Hosford
Order Number XDATA-SUB01-PO01; Prime Contract Number: FA8750-12-C-0301 for DOD, DARPA	Giant Oak	\$74,856	Open Source Software for National Security (Disruptive Defense paper)
Prime Contract Number: NNM15AAQ2C; Task Order # NNM16AA34T	Johns Hopkins University	\$250,000	JANNAF Ultra-low cost access to Space (ULCATS) Study
2010-0718815-000	Office of the Director of National Intelligence	\$5,000	ODNI Braintrust Indefinite Delivery Indefinite Quantity (IDIQ)
N00244-15-1-0056	PASCC/DOD, NAVSUP Fleet Logistics Center San Diego to CNAS	\$149,645	Managing Escalation and Limiting War in a Conflict in the Western Pacific
Subcontract Number: 085001.011.0220.2105.3; Prime Contract Number: FA8075-14-D-0001 DSIAC, Task Order 0011 for Air Force AFICA and DTIC	SURVICE Engineering	\$91,337	Beyond Armor: New Force Protection Concepts for U.S. Mounted Troops
FA3300-13-G-0014	United States Air Force	\$27,500	USAF Military Senior Fellow
TRNGRA-09Y0902BROW	United States Army	\$27,500	USA Military Senior Fellow
30-11-G81DCS134-000	United States Coast Guard	\$26,250	USCG Military Senior Fellow
MOU	United States Marine Corps	\$27,500	USMC Military Senior Fellow
MOU Between Deputy Chief of Naval Operations (Information, Plans and Strategy) Strategy and Policy Division (OPNAV N51) and CNAS	United States Navy	\$27,500	USN Military Senior Fellow



CNAS Foreign Government Contract or Payment Information

2017			
Foreign Contract / Payment	Foreign Government	Dollar Value	Subject of Contract or Payment
Memorandum of Understanding between the Center for a New American Security and the Government of France signed 23 December 2016	Government of France	\$30,000	Testing Possible Challenges to the Greenland, Iceland, UK (GIUK) Gap: A Table Top Exercise
Agreement dated 8 May 2017	Embassy of Japan	\$36,000	Quarterly briefings and counsel sessions
Agreement dated 1 August 2017	Government of Japan	\$181,819	Building Capabilities for the US-Japan Alliance in the East China Sea
Memorandum of Understanding between the Center for a New American Security and the Government of Norway signed 27 January 2017	Royal Norwegian Ministry of Defence	\$39,960	Testing Possible Challenges to the Greenland, Iceland, UK (GIUK) Gap: A Table Top Exercise
Accepted proposal for "U.S.-Taiwan Strategic Partnership"	Taiwan Economic and Cultural Representative Office (TECRO)	\$210,000	CNAS-TECRO Partnership
Memorandum of Understanding between the Center for a New American Security and the Government of the United Kingdom signed 16 November 2016	Government of the United Kingdom	\$25,000	Testing Possible Challenges to the Greenland, Iceland, UK (GIUK) Gap: A Table Top Exercise
2016			
Foreign Contract / Payment	Foreign Government	Dollar Value	Subject of Contract or Payment
Memorandum of Understanding between the Center for a New American Security and the Government of France signed 23 December 2016	Ministry of Defence of the French Republic	\$30,000	Testing Possible Challenges to the Greenland, Iceland, UK (GIUK) Gap: A Table Top Exercise
Agreement dated 23 May 2016	Embassy of Japan	\$36,000	Quarterly briefings and counsel sessions
Agreement dated 26 July 2016	Government of Japan	\$252,500	Beyond the San Hai: Implications of China's Emerging Bluewater Maritime Strategy
Accepted proposal for "U.S.-Taiwan Strategic Partnership"	Taiwan Economic and Cultural Representative Office (TECRO)	\$230,000	CNAS-TECRO Partnership
Accepted proposal for "UAE Missile Technology Control Regime (MTCR) Study"	United Arab Emirates	\$250,000	UAE Missile Technology Control Regime (MTCR) Study
Memorandum of Understanding between the Center for a New American Security and the Government of the United Kingdom signed 16 November 2016	Government of the United Kingdom	\$25,000	Testing Possible Challenges to the Greenland, Iceland, UK (GIUK) Gap: A Table Top Exercise
2015			
Foreign Contract / Payment	Foreign Government	Dollar Value	Subject of Contract or Payment
Agreement dated 11 May 2015	Embassy of Japan	\$36,000	Quarterly briefings and counsel sessions
Purchase and Sale Agreement between the Center for a New American Security and the Embassy of the Republic of Lithuania to the United States	Embassy of the Republic of Lithuania	\$75,000	Assured Resolve: Testing Possible Challenges to Baltic Security

MOU between the Center for a New American Security and the Government of Finland Represented by the Ministry of Foreign Affairs and the Ministry of Defense	Government of Finland	\$75,000	Assured Resolve: Testing Possible Challenges to Baltic Security
Agreement dated 26 May 2015	Government of Japan	\$252,500	Staying Ahead of the Curve: Alliance Requirements for Managing China's Maritime Might
Agreement between the Kingdom of Denmark and the Center for a New American Security dated 4 December 2014	Kingdom of Denmark	\$91,953	Climate Change in the Developing World
MOU between the Center for a New American Security and the Ministry of Defence of Estonia	Ministry of Defence, Estonia	\$20,000	Assured Resolve: Testing Possible Challenges to Baltic Security
Grant Letter for USA-15/0001 Assured Resolve: Testing Possible Challenges to Baltic Security	Norwegian Ministry of Foreign Affairs	\$38,220	Assured Resolve: Testing Possible Challenges to Baltic Security
Agreement between the Ministry of Defence of the Republic of Latvia and the Center for a New American Security on Co-operation	Republic of Latvia	\$75,000	Assured Resolve: Testing Possible Challenges to Baltic Security
Grant Letter for USA-15/Exercise Assured Resolve: Testing Possible Challenges to Baltic Security	Royal Norwegian Ministry of Defence	\$36,780	Assured Resolve: Testing Possible Challenges to Baltic Security
Accepted proposal for "U.S.-Taiwan Strategic Partnership"	Taiwan Economic and Cultural Representative Office (TECRO)	\$200,000	CNAS-TECRO Partnership
Swedish Contribution to Center for a New American Security (CNAS) - the project "Assured Resolve - challenges to Baltic Security"	Sweden, Ministry of Foreign Affairs	\$75,000	Assured Resolve: Testing Possible Challenges to Baltic Security



**Statement Before the
House Armed Services Committee
Subcommittee on Emerging Threats and Capabilities
*“Chinese Advances in Emerging Technologies
and their Implications for U.S. National Security”***

A Testimony by:

William Carter

Deputy Director and Fellow, Technology Policy Program

January 9, 2018

2118 Rayburn House Office Building

Introduction and Main Points

Chairman Stefanik, Ranking Member Langevin, thank you for the opportunity to participate in today's hearing on this important topic. China's significant progress in key emerging technologies like [artificial intelligence, cyber, space-based capabilities and antisatellite weapons, electronic warfare and quantum computing] have transformed the global security environment in recent years, and require a rethink of the way that we approach securing our nation.

Asia is a critical part of America's future, economically and strategically, and we are in a new era of strategic competition with China, one defined by our competing progress in advanced technologies. Our response to China's progress in technology is essential to our future. The goal of my testimony is to amplify some of these issues and to propose potential solutions for how we can implement an effective strategy to deal with this challenge.

Since the Cold War, U.S. national security has been built upon the unparalleled strength of American technology. In the 1950s, the Department of Defense successfully "offset" the Soviet Union's conventional military superiority by strengthening our nuclear deterrent, and in the 1970s we again cemented our military dominance through innovation in precision munitions, stealth, and a new generation of space based ISR and communications technologies, the so-called "second offset." Today, this offset dynamic is being reversed. China is pursuing an "offset strategy" of its own to overcome our conventional superiority by winning the race to dominate the next generation of technology.

In 2014, the Department of Defense (DoD) announced a "third offset," developing the next generation of technological dominance based on artificial intelligence and robotics, miniaturization and ubiquitous connectivity, and quantum computing, but this technological race is very different than the others. The success of previous offsets was based on investing in winning a race our adversaries didn't even know they were in while allowing them to focus their resources on an area of advantage that we could overcome through innovation. But today, even as we are pursuing our "third offset," China is pursuing a "first offset" of its own, and is investing in the same technologies to challenge us that we are investing in to maintain our strategic edge. They have developed a national strategic plan – in fact many of them – to overtake us in the race to dominate these new technologies, and are rapidly closing the gap in innovation, deployment, and militarization of these new systems with the U.S.

China's Technology is Catching up with, and Perhaps Surpassing Our Own

China sees offensive cyber capabilities, anti-satellite weapons, electronic warfare tools, hypersonic weapons, artificial intelligence, and quantum technologies as key to enabling the PLA to win wars in future, high-tech conditions and offset the advantages of the U.S. military, and has made significant strides in all of these areas. These technologies can be divided into two broad buckets: technologies to disrupt and degrade our military capabilities by exploiting our vulnerabilities in the information domain, and technologies that will determine the future global balance of both economic and strategic power.

The PLA correctly views the U.S. military as highly vulnerable to a first strike in the “information domain,” and is developing capabilities in this domain that will overcome their conventional disadvantages. We may have more and better aircraft carriers, tanks, and missiles than the PLA, but without access to data and connectivity many of these systems are ineffective or even inoperable. Chinese military thinkers describe the U.S. military’s Achilles heel simply: “No satellites, no fight.”

China has demonstrated the ability to significantly disrupt, degrade, and even destroy the ICT infrastructure on which our military depends. The PLA has tested a range of anti-satellite weapons, including conventional ground-based kinetic kill vehicles,¹ directed energy weapons,² jamming and spoofing capabilities,³ and “kill-satellites” designed to disable or destroy other satellites on orbit.⁴ They have expanded their electronic warfare capabilities, testing their capabilities to jam radar and communications and spoof GPS systems.⁵ China has also developed some of the most sophisticated offensive cyber capabilities in the world.

China is also investing heavily in building its technological base to dominate the technologies of the future. In particular, China sees artificial intelligence (AI) and quantum as foundational to both economic and military competitiveness in the long term, and has become not just a copycat or adopter of these technologies, but an innovator in its own right.

Competition in AI between the U.S. and China has become neck-and-neck. Chinese researchers now publish more papers on AI than any other country in the world, although U.S. papers are still more widely cited, suggesting that they are more impactful and highly respected in the field.⁶ Chinese companies have also made significant breakthroughs in AI applications including

¹ Shirley Kan, “China’s Anti-Satellite Weapon Test,” CRS Report for Congress, RS22652, April 23, 2007

² Richard D. Fisher, Jr., “China’s Progress with Directed Energy Weapons,” Testimony before the U.S.-China Economic and Security Review Commission hearing, “China’s Advanced Weapons,” February 23, 2017

³ U.S.-China Economic and Security Review Commission, “2015 Annual Report to Congress,” November 17, 2015, p. 297

⁴ U.S.-China Economic and Security Review Commission, “2015 Annual Report to Congress,” November 17, 2015, p. 294

⁵ Bill Gertz, “Ship collisions raise specter of Chinese electronic warfare,” Asia Times, August 29, 2017

⁶ Simon Baker, “Which countries and universities are leading on AI research?” Times Higher Education, May 22, 2017

natural language processing,⁷ real-time translation,⁸ imagery analysis,⁹ and autonomous driving.¹⁰

In quantum, China may already be well ahead. China has launched a quantum communications satellite called Micius,¹¹ established a quantum fiber link between Beijing and Shanghai,¹² has invested billions of dollars into research on quantum computing, and even claims to have tested functioning quantum radar that can detect stealth aircraft.¹³ Some of China's claimed advances in quantum technology are likely embellished, but we have seen enough of China's capabilities in this field that we must take them seriously. Where the U.S. stands in quantum research is murky, as much of the research is classified. However, a number of US researchers have recently noted that the US seems to be lagging, owing primarily to the comparative willingness of the Chinese government to aggressively fund new quantum initiatives.¹⁴

Investing in Resiliency and Avoiding Conflict

Going forward, the U.S. must adopt a national strategy to counter China's offset in the short and long term. China's short-term strategy is to exploit the U.S. military's weaknesses and exert constant pressure to undermine us. In 2015, the PLA created the Strategic Support Force (SSF) to centralize information warfare units within the PLA. Notably, the SSF includes not only cyber, but also space and electronic warfare operations. The Chinese do not view information warfare as limited to computer networks, but rather as a domain spanning intelligence, communications, and the entire electromagnetic spectrum.

China's offensive cyber capabilities should be of greatest concern to us in the short term because they are being used against us every day to strengthen China's strategic position in incremental ways. There is much debate about whether we are in a "cyber war" with China. My answer to that is simple: no. "War" implies an all or nothing conflict against an enemy, one where we must do what it takes to defeat them. China is a "frenemy" of the United States, not an enemy, and we

⁷ Yiting Sun, "Why 500 Million People in China Are Talking to This AI," MIT Technology Review, September 14, 2017

⁸ Chen Na, "Baidu's Newest Gadget Translates Speech in Near-Real Time" Sixth Tone, September 21, 2017

⁹ Tom Simonite, "Baidu's Artificial-Intelligence Supercomputer Beats Google at Image Recognition," MIT Technology Review, May 13, 2015

¹⁰ Charles Clover, Emily Feng, and Sherry Fei Ju, "Baidu launches public road tests of autonomous cars in China," Financial Times, November 23, 2017

¹¹ Gabriel Popkin, "China's quantum satellite achieves 'spooky action' at record distance," Science Magazine, June 15, 2017

¹² Zhang Zihao, "Beijing-Shanghai quantum link a 'new era'," China Daily, September 30, 2017

¹³ Jeffrey Lin and P.W. Singer, "China Says It Has Quantum Radar: What Does That Mean?," Popular Science, September 27, 2016

¹⁴ Tim Johnson, "China speeds ahead of U.S. as quantum race escalates, worrying scientists," McClatchy DC, October 23, 2017

are not prepared to do whatever it takes to defeat them in response to the low-level espionage and network reconnaissance activities that both sides engage in every day.

We are in a new era of strategic competition with China in the information domain, a form of low-level, protracted back and forth in which both sides constantly prepare for possible conflict and seek to develop asymmetric capabilities that would allow them to dominate in a potential conflict. In China, this stance is referred to by PLA strategists as “active defense.”¹⁵ By conducting peacetime network operations, PLA officers aim to identify vulnerabilities in US systems that could be exploited for active disruption if an attack were ever launched against China. The PLA see such network reconnaissance as unlikely to lead to escalation or retaliation, but taken together they allow China to slowly improve its strategic position.

Though the active defense doctrine is ostensibly concerned with self-defense and post-emptive strike, the Chinese view cyber warfare as being highly effective for a first strike, and assume that very quickly afterwards vulnerabilities will be mitigated, defenses erected, and the advantage of surprise taken away. If the PLA were ever to attain a level of network penetration sufficient for them to feel confident in their ability to cripple US military forces long enough to attain a conventional or nuclear advantage, the US strategic position would be irreparably compromised.

It is important to note that, while we often talk of “technological parity,” when it comes to these technologies, in many ways it is less important whether their technology is “as good as ours” than whether it is good enough to render our capabilities ineffective. Our most important goal should be to invest in resiliency so that China is never confident enough to launch a preemptive strike. This means both hardening our networks and infrastructure, particularly in cyberspace and outer space, and developing and demonstrating our ability to operate in denied environments.

We must re-train our military to operate in analog mode without access to data and technology. We must ensure that any new system or platform DoD buys has at least some basic level of functionality without access to space-based capabilities, instead of buying systems that are extremely effective when connected but cannot operate at all in denied environments. We must build a secure supply chain and develop new ways to test and ensure the security of the chips that we use in our weapons systems. We must develop new space architectures that do not rely on a small number of exquisitely capable, but also vulnerable, government satellites, leveraging commercial satellite capabilities, international partnerships, and constellations of smaller, cheaper satellites that are individually less capable, but are more survivable and replaceable. And we must develop ground-based backups and redundant capabilities so that we are not entirely reliant on space. These are not new answers to new questions. We know what needs to be done, but we need to get serious about implementing these solutions.

¹⁵ Note: This is different from the “active defense” debate in the U.S., which refers to the discussion around allowing private companies to engage in cyber operations outside their own networks to counter cyber threats.

Leveraging Our Unique Strengths to Maintain a Long-Term Technological Edge

Ultimately, however, simply countering China's immediate efforts to exploit our vulnerabilities will not be enough to confront the emerging threat of China's growing technological capabilities. In the long term, China's strategy is not just to exploit the weaknesses in our military technology but to develop their own innovative, dynamic high technology sector to dominate the next generation of civilian and military technologies, particularly AI. They seek to leverage both commercial and military innovation in ways that complement each other and build both military and economic power. Their national strategies anticipate a shift from today's "informatized warfare" to "intelligentized warfare,"¹⁶ and their strategy to dominate in intelligentized warfare is to dominate key commercial industries in AI, quantum technology, augmented and virtual reality (AR/VR) and robotics.

We Need a National Strategy to Maintain Our Technological Dominance

China has a strategic plan—in fact many of them—to develop a technological edge over the United States. National policies like the New Generation AI Development Plan, the 13th Five Year National Science and Technology and Innovation Plan, and the Made in China 2025 Plan represent a concerted effort to leverage the full resources available to China in order to cultivate indigenous technological innovation. China recognizes that military technology does not exist in a vacuum. It is a part of an ecosystem that spans the public and private sector, and has dependencies ranging from access to basic materials to massive quantities of data. In the digital age, virtually all technological breakthroughs are fundamentally dual-use.

The Chinese system of industrial planning offers advantages in its ability to coordinate the activities of myriad groups and direct them all towards a single aim. An example of this is the case of high-end computer chips, a critical enabler for strategically-significant technologies like artificial intelligence. Realizing the significance of a robust integrated chip (IC) industry in China, the central government released its 2014 National Guidelines for the Development and Promotion of the IC Industry, established a national IC investment fund, which has provided over \$20 billion so far to support the industry, and introduced new financing tools, insurance products, and tax policies introduced by the central government to encourage innovation.¹⁷

The result of these policies has been a dramatic expansion of China's IC industry, with revenues increasing by almost 20% for the sector in 2017 compared to just 3.4% for the rest of the world.¹⁸ Further, 2017 represented the first year that chip design brought in more revenues than

¹⁶ Elsa B. Kania, "[Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power](#)," Center for a New American Security, November 2017

¹⁷ Dominic Barton, Jonathan Woetzel, Jeongmin Seong, Qinzhen Tian, "[Artificial Intelligence: Implications for China](#)," McKinsey Global Institute, April 2017

¹⁸ "[Total Revenue of China's IC Industry to Grow Above Global Average at Annual Rate of 19.86% for 2018, Says TrendForce](#)," BusinessWire, November 9, 2017

chip packaging and testing, indicating that China's policies have been effective not only at expanding the industry, but at promoting the development of technologically sophisticated enterprises with high strategic value.

That said, there are enormous bureaucratic inefficiencies involved in China's centrally-planned approach to industrial policy, which can waste resources and create severe market distortions. We should not try to replicate China's approach, but instead strive to formulate a cohesive, whole-of-government strategy based not on central planning, costly oversight procedures and elaborate coordination mechanisms, but on a common understanding of the strategic goals of the nation and how all of the levers of government can be used to support them.

Invest in Long-Term Fundamental Research and Development

An important component of this strategy should be government investment in R&D and innovation. China has realized the essential role that both public and private R&D investments play in technologies like AI, but the U.S. increasingly depends on commercial R&D alone. Corporate research has a major role to play in advancing our nation's technological capacity, but the developers in these groups are often only focused on projects with immediate and guaranteed commercial applications. There is little incentive for most companies to fund sustained work on exploratory projects with long incubation periods and uncertain prospects for returns like fundamental research into quantum computing. The federal government is in a unique position to be able to support basic research which may not pay off for 20-30 years, but, like the internet, may prove revolutionary.

Unfortunately, U.S. commitment to support public sector R&D is flagging. After the July 2017 announcement of China's new AI development plan, local and provincial governments announced billions of dollars of support to the industry, with the cities of Xiangtan and Tianjin alone pledging a collective \$7 billion to AI projects.¹⁹ In comparison, total U.S. government R&D investment in AI was \$1.1 billion in 2015,²⁰ and the Trump administration's proposed budget would have cut the NSF's AI research funding by 10%. The U.S. government should be expanding, not curtailing, R&D funding for technologies like AI, leveraging research vehicles like DARPA, IARPA, and the national labs to advance our nation's technological capacity and ensure we are investing in the capabilities our defense and intelligence communities will need to manage emerging threats in the future.

Leverage the World-Leading Innovation of the U.S. Private Sector

¹⁹ Paul Mozur and John Markoff, "Is China Outsmarting America in A.I.?" New York Times, May 27, 2017 and Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," New York Times, July 20, 2017

²⁰ Executive Office of the President, "Preparing for the Future of Artificial Intelligence," National Science and Technology Council Committee on Technology, October 2016

In addition, the U.S. must continue to support private sector innovation, which represents our greatest competitive advantage as a nation. In the past, major defense innovations took place in government labs, giving the military easy and monopolized access to strategically-significant innovations. Today, this is no longer the case. The private sector is now the source for most new strategic technologies, and our military's future effectiveness will depend on leveraging commercial advances more effectively than our opponents.

There are two key things we can do to better leverage private sector innovation. First, we must support and enable the development of commercial markets for transformative new technologies. Technology has gotten decades ahead of our laws, policies, and regulations. Innovations like artificial intelligence, ubiquitous sensors, big data, and virtual reality raise significant questions about safety, security, privacy, and liability, and commercial markets for these technologies cannot thrive without a clear roadmap of how we will approach governing their development and use.

Second, we must fundamentally rethink our approach to bringing private sector innovations into the national security world. The Chinese government has recently taken a number of steps to promote what they call "military-civil fusion" by creating opportunities for government and military researchers to partner with leading technology companies in the development of new products.²¹ China's approach is based off of similar efforts in the U.S., notably through programs like DoD's Defense Innovation Unit Experimental (DIUx) and In-Q-Tel, which offer the security establishment a way to bypass cumbersome contract processes and accelerate the deployment of cutting-edge technologies within our military.

But these programs are tiny compared to the behemoth of traditional federal acquisitions, and we cannot expect a tiny part of the federal acquisitions process to produce the bulk of our next generation of military capabilities. As the share of transformative innovation continues to shift toward the commercial sector, these lean, agile acquisition programs cannot remain the exception, they must become the norm, and we must expect and tolerate stumbles and problems as we learn to leverage these approaches at scale.

We also need to have a deeper conversation about how we can maintain a technological edge in national security in a world in which technology is fast-moving, ubiquitous, and develops outside of the government and outside our own borders. Our way of thinking about the relationship between technology and national security dates back to the Cold War, and is based on the concept of controlling access to technologies that have military applications. Most of today's most popular technologies have at least a theoretical military application, whether FitBits, quadcopters, Google Maps or Shazam, and the military is barely able to keep up its awareness of the latest developments in the commercial sector, much less try to control cutting edge technologies.

²¹ Elsa B. Kania, "[Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power](#)," Center for a New American Security, November 2017

It is no longer plausible or useful to base our national security strategy on the assumption that our military will have sole access to the best technology. As China becomes more innovative, they will develop their own cutting-edge military technologies that we will not be able to control. Trying to control our own commercial technologies as “dual use” only deters private companies from working with DoD to protect their freedom to market their products internationally, and paying defense contractors to re-invent the wheel by building bespoke versions of commercial technologies for a DoD client has proven ineffective and wasteful, draining our resources and causing the military to fall dramatically behind the private sector in even simple day-to-day technologies. Perhaps it is time for a new way of thinking about maintaining a technological edge for the military. We may not be the only ones who have access to the cutting-edge technologies of the future, but we can try to adapt faster and make better use of new technologies than our adversaries.

Counter Chinese Efforts to Exploit the U.S. Education System and Innovation Economy in Ways that Work for Us

That does not mean we should be blind to our adversaries’ efforts to acquire our technology and exploit U.S. innovation. In February 2017, DIUx released a report on China’s technology transfer strategy which identified more than ten major strategies employed by China to acquire U.S. technologies, including early stage investments in U.S. tech startups, industrial espionage and cyber theft of intellectual property, and attracting talented engineers and students back to China along with all of their knowledge and experience of what U.S. companies and researchers are working on in their fields.²²

The current debate in the U.S. around Chinese tech transfer is focused on preventing them from exploiting our education and investment environment by keeping China out, but this is misguided. If China wants to send their best and brightest students to be educated in our universities and graduate programs, and invest billions of dollars in startups and R&D in the United States, so much the better for us. We should instead focus on keeping them here, allowing the talented researchers and engineers that we educate to innovate and build businesses that employ Americans and add to the U.S. economy. We must ensure that the next generation of innovators, wherever they are born, build the technology of the future here in the United States.

The DIUx report recommends that we look at ways to restrict Chinese investment in U.S. technology companies, particularly those with potential military applications. This is unlikely to work – it is easier to disguise the source of investment capital than to investigate it – and will not stop China from acquiring our technology through its other tech transfer strategies. Such an effort could also quickly become impossibly broad. Thousands of entrepreneurs seek capital in

²² Michael Brown and Pavneet Singh, “China’s Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation,” Defense Innovation Unit Experimental, February 2017

the U.S. each year to build businesses in AI, AR and VR, robotics, and IoT devices, and attempting to anticipate all those technologies which might one day have military applications is impractical, if not impossible. Furthermore, if anything, restricting China's access to U.S. technologies through investment could cause them to redouble their efforts to acquire our technology through more damaging means like industrial espionage and cyber theft, and to invest more of their money in domestic innovation.

That said, Congressional efforts to reform the CFIUS process are essential. The proposed legislation modernizes the process and makes it more flexible, which is important not just in our technological competition with China, but to ensure our continuing security against a range of global threats. In particular, expanding the Committee's oversight of joint ventures and non-controlling investments is important. We should do more to identify and prevent deals that truly threaten our nation's strategic industries, but our goal should not be to cut off Chinese investment in U.S. companies. If China wants to pour their money into U.S. companies instead of their own domestic entrepreneurs, we should not turn the money away, but instead push back against anti-competitive practices and IP theft that exploit the companies that take their capital. Instead of restricting investment, policymakers should focus on ways to support companies that take Chinese investment, such as pressuring China to open up market access to U.S. companies.

Invest in the Workforce of the Future

In the long term, we need to build in a workforce capable of leading the next generation of technological developments. Establishing new education and training resources for talent development was included as one of the main pillars of China's New Generation Artificial Intelligence Development Plan, and the country has followed through by creating several new graduate programs in AI at Chinese universities to support need for trained researchers. China has also set its sights on attracting foreign talent, investing through its Thousand Talents Program to entice outside academics to relocate to China.

The U.S. must also invest in cultivating domestic talent, expanding computer science education initiatives in schools and increasing funding for universities to support the next generation of researchers and slow the brain drain that is threatening the U.S.' ability to train successive generations of talent.²³ Universities are under financial pressure as the government retrenches, making it even more difficult to compete with the huge salaries commanded by people with specialized skills in cutting edge fields like machine learning and artificial intelligence. This is imperiling our ability to train the next generation of talent in these crucial fields.

As we think about where to focus our resources in education, we must move away from thinking in terms of the "STEM" disciplines, science, technology, engineering and math. STEM is both too broad and too narrow a category. On one hand, while the U.S. faces significant workforce

²³ Cade Metz, "[Tech Giants are Paying Huge Salaries for Scarce A.I. Talent](#)," New York Times, October 22, 2017

shortages in some STEM fields like artificial intelligence, materials science and data science, there are significant surpluses in other STEM fields like chemistry and biotechnology.²⁴ On the other hand, as automation plays an increasingly important role in the economy, the hard skills that STEM advocates so highly value will be the first to be automated, and the skills that we will need most from human beings will be soft skills like critical thinking, empathy and communication that are emphasized in the liberal arts. Our education strategy should focus on a two-pronged approach: develop a strong pool of technical talent that can build and operate the technology of the future, and build a broad workforce of quick thinking, adaptable people with basic digital literacy and the soft skills to complement and work with machines.

Build an Open Data Ecosystem and Leverage International Partnerships to Combat China's Advantage of Scale

China's scale is one of its greatest advantages over the United States. China has 1.4 billion people; the U.S. has less than 330 million.²⁵ The Chinese economy is the second largest in the world, and is projected to overtake the U.S. in 15 to 20 years. China will be home to 20% of the world's data by 2020 and 30% by 2030,²⁶ a huge advantage in the development of AI, which depends on massive volumes of data on which to train learning algorithms. The size of the Chinese market also attracts innovators and entrepreneurs and allows China to lure talent and IP from overseas.

But U.S. innovators also have advantages. China may have a huge consumer market but U.S. companies have larger global market share. Chinese companies dominate the domestic market, but have struggled to compete globally. China may have over 1 billion people, but Facebook has more than 2 billion users worldwide. Google has more Gmail users than any Chinese email service, and Facebook Messenger and WhatsApp have more users than any Chinese messaging service. As a result, while China may have 30% of the world's data, U.S. companies have a tremendous head start on cornering the other 70% of the global data market. These users are also more diverse and more global than users of Chinese services like WeChat and QQ. China's data is almost entirely on Chinese consumers, whereas U.S. companies like Facebook and Google have users around the world. This is an important advantage.

But U.S. tech companies' position in foreign markets is under threat from policies that make it more difficult for foreign companies to compete. Privacy advocates in the U.S. are also pushing for greater protections for data. Even close allies like the EU are developing policies like the General Data Protection Regulation (GDPR) that target U.S. companies' ability to compete. The

²⁴ Yi Xue and Richard Larson, "STEM crisis or STEM surplus? Yes and yes," *Monthly Labor Review*, U.S. Bureau of Labor Statistics, May 2015

²⁵ World Bank Global Development Indicators. Retrieved January 7, 2018.

<https://data.worldbank.org/indicator/SP.POP.TOTL>

²⁶ Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, November 2017

U.S. government must develop a strategy to combat protectionism, data localization and privacy policies that harm our global tech companies. Doing this effectively will require balancing legitimate concerns around privacy and consumer protection both in the U.S. and abroad with the need for an open, flexible data ecosystem that supports innovation and experimentation in AI. We can also use trade agreements and establish bilateral and multilateral partnerships to promote the free flow of data and support collaboration in R&D for emerging technologies.

Avoid Dogmatic Views of New Technologies like Autonomous Weapons

As we plan for the future, particularly in the military context, we cannot afford to adopt dogmatic views of new technologies that prevent us from exploring their potential. China looks at our strategies and policies, identifies their gaps and flaws, and seeks to exploit them for their own advantage. If we disavow potentially transformative technologies, we open a door to China to leapfrog our capabilities.

A prime example is autonomous weapons. In the US, lethal autonomous weapons systems (LAWS) often dominate conversations around AI, and discussions around AI policy too often revolve around the dangers of the military developing “killer robots” that could become available to malicious actors like criminals and terrorists. This conversation is both premature and behind the times. Fully autonomous weapon systems remain far from combat-ready, and human soldiers are not going anywhere anytime soon. At the same time, the technology for private individuals to build simple autonomous killing machines at little cost already exists, as a professor from UC Berkeley ironically demonstrated while advocating against the development of autonomous weapons.²⁷

In 2016, the Secretary of Defense said, “whenever it comes to the application of force, there will never be true autonomy, because there’ll be humans (in the loop).”²⁸ This argument makes sense for today’s AI technology. Human-machine partnerships are far more effective and reliable than fully autonomous systems in complex and dynamic combat environments, and are likely to remain so for a while. But if we rule out the possibility of fully autonomous combat systems, DoD risks missing out on a class of technologies that could fundamentally transform warfare.

Other countries like Russia and China are unlikely to exercise the same restraint when it comes to fully autonomous weapons systems, which they view as an opportunity to leapfrog US military dominance.²⁹ If these countries were to field fully autonomous weapons systems that could analyze and adapt to our tactics and strategies at machine speed, it could render our defenses ineffective if we do not do the same. DoD should invest in the next generation of

²⁷ Stuart Russell, “[Slaughterbots](#),” YouTube, November 12, 2017

²⁸ Sydney J. Freedbert Jr. And Colin Clark, “[Killer Robots? ‘Never,’ Defense Secretary Carter Says](#),” Breaking Defense, September 15, 2016

²⁹ Elsa B. Kania, “[Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power](#),” Center for a New American Security, November 2017

combat systems that leverage the full potential of AI, including the potential future development of lethal AI systems that can operate without humans in the loop. Instead of LAWS “never,” our policy should be “not until they can outperform human/MI collaboration,” including making ethically acceptable choices about when to pull the trigger.

Responding to Chinese Technological Progress and Maintaining our Technological Leadership in the Short and Long Term

China has taken a page out of the U.S. playbook, pursuing an offset strategy to overcome our conventional superiority by beating us in the race to the next generation of transformative technology. They are evaluating our military technology and our future strategy and doctrine, looking for the gaps and weaknesses of our approach so that they can exploit them for their own advantage. We must develop a new national security strategy of our own to win the race and overcome China’s efforts to undermine our global position.

In the short term, we must counter China’s efforts to exploit our military’s dependencies on ICT technologies by investing in resiliency and ensuring that China never develops enough confidence in their ability to compromise our systems to justify a first strike. In the long term, we must ensure that our world-leading education system and business environment work for us. We should rethink the relationship between private sector innovation and our military’s technological edge to better leverage our greatest strength, our private technology industry, to secure our nation. We should push back against China’s efforts to acquire our technology and the fruits of our innovation, but not push away China’s brightest minds and innovation capital if they want to send them to the United States. We should invest in fundamental R&D that will form the basis of the next generation of technologies, not by replicating or subsidizing the private sector’s efforts but by supporting the kind of long-term moonshot research that private companies are less willing to support. And we should build a strong base on which our private sector innovators can thrive by reinvesting in education, creating strong commercial markets for transformative technologies, and protecting our companies’ ability to compete in global markets.

Finally, we must remember that China is not the only threat we need to worry about. Russia, Iran and North Korea, among others, see the same weaknesses and vulnerabilities in our approach to national security that the Chinese do. To appropriately manage the range of threats the U.S. faces, we must focus not just on “beating China,” but on increasing our strength and agility across the technological domain. We are no longer the disruptor offsetting an adversary with a conventional advantage by sprinting to disruptive technologies, we are the conventional hegemon and we must be prepared to face any challenger. Policymakers must wake up to the threat faced by all of these countries, and ensure that our country is investing in the technologies and systems that will define the next era of warfare.

I thank the Committee for the opportunity to testify and will be happy to answer any questions.

William A. Carter
Deputy Director and Fellow, Technology Policy Program

William A. Carter is deputy director of the Technology Policy Program at CSIS. His research focuses on international cyber and technology policy issues, including artificial intelligence, surveillance and privacy, data localization, cyber conflict and deterrence, financial sector cybersecurity, and law enforcement and technology, including encryption. He has spoken at events and conferences around the world and participated in Track 2 dialogues on cyber and technology policy issues with China, Russia, and Australia. Before joining CSIS, he worked in the Goldman Sachs Investment Strategy Group, where he performed research and analysis on geopolitics and the macro economy and produced reports and presentations on international affairs and current events and their impact on markets. He previously worked at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University with a B.A. in economics.

**DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES**

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: William A. Carter

Capacity in which appearing: (check one)

☐ Individual

☒ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: Center for Strategic and International Studies (CSIS)

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
State Department	State Department	\$284,237.10	International Security Cyber Issues Workshop
Department of Defense	Department of Defense	\$824,684.39	NDAA 2015 Independent Study on PACOM AOR

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Contract	Japan, Japan External Trade Organization (JETRO)	\$20,000	China Innovation Policy Series
Contract	United Nations (Germany, The Netherlands)	\$160,000	International Security Cyber Issues Workshop

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Contract	Japan, Japan External Trade Organization (JETRO)	\$40,000	China Innovation Policy Series
Contract	The Netherlands	\$3,480	Cyber Workshop Co-Chair

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Payment	Japan, Japan Aerospace Exploration Agency (JAXA)	\$33,000	US-Japan space cooperation
Contract	Japan, Japan External Trade Organization (JETRO)	40,000	China's 13th 5 Year Plan

