S. HRG. 117–148

EMERGING TECHNOLOGIES AND THEIR IMPACT ON NATIONAL SECURITY

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

FEBRUARY 23, 2021

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46–695 PDF WASHINGTON : 2022

COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire	JAMES M. INHOFE, Oklahoma
KIRSTEN E. GILLIBRAND, New York	ROGER F. WICKER, Mississippi
RICHARD BLUMENTHAL, Connecticut	DEB FISCHER, Nebraska
MAZIE K. HIRONO, Hawaii	TOM COTTON, Arkansas
TIM KAINE, Virginia	MIKE ROUNDS, South Dakota
ANGUS S. KING, Jr., Maine	JONI ERNST, Iowa
ELIZABETH WARREN, Massachusetts	THOM TILLIS, North Carolina
GARY C. PETERS, Michigan	DAN SULLIVAN, Alaska
JOE MANCHIN III, West Virginia	KEVIN CRAMER, North Dakota
TAMMY DUCKWORTH, Illinois	RICK SCOTT, Florida
JACKY ROSEN, Nevada	MARSHA BLACKBURN, Tennessee
MARK KELLY, Arizona	JOSH HAWLEY, Missouri
	TOMMY TUBERVILLE, Alabama

ELIZABETH L. KING, *Staff Director*
JOHN D. WASON, *Minority Staff Director*

CONTENTS

FEBRUARY 23, 2021

EMERGING TECHNOLOGIES AND THEIR IMPACT ON NATIONAL SECURITY

TUESDAY, FEBRUARY 23, 2021

UNITED STATES SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m. in Room SD–106, Dirksen Senate Office Building, Senator Jack Reed (Chairman of the Committee) presiding.

Committee Members present: Senators Reed, Shaheen, Gillibrand, Blumenthal, Hirono, Kaine, King, Warren, Peters, Manchin, Duckworth, Rosen, Kelly, Inhofe, Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan, Cramer, Scott, Blackburn, Hawley, and Tuberville.

OPENING STATEMENT OF SENATOR JACK REED

Chairman REED. I will call the hearing to order, and good morning. And since this is the first open hearing since the Senate has organized I would like to begin by once more welcoming the new members of the committee, Senators Rosen, Kelly, and Tuberville. We all look forward to working with you this year, as we provide oversight to the Department of Defense and craft the Fiscal Year 2022 National Defense Authorization Act.

This morning the committee meets to examine the impact of emerging technologies on national security. I want to thank the three extremely well-qualified witnesses who are joining us today to help us better understand this issue. Dr. Eric Schmidt is the former Chief Executive Officer (CEO) of Google and chair of the Defense Innovation Board, and currently co-chairs the National Security Commission on Artificial Intelligence, which was established by this committee. Mr. Brad Smith is the president of Microsoft Corporation, and retired General "Hawk" Carlisle is the president and CEO of the National Defense Industrial Association.

Each of you has unique and extensive technical, commercial, and defense experience at the intersection of advanced technology and the military that will help inform our discussion. It is my hope that today we can begin to address a number of key questions relating to emerging technologies and national security, including what are the key emerging technology areas and trends that will shape national security and economic prosperity in the future; what actions could accelerate or slow the operational use of these technologies; how do you assess the standing of the United States in the global competition to develop and deploy these emerging technologies; and what specific recommendations do you have for actions in policy,

programs, or organizational reform that this committee or the Pentagon should pursue to improve our ability to deploy these technologies for national security.

The future national security environment will likely be shaped by emerging technologies such as quantum computing, biotechnology, hypersonics, 5G, and artificial intelligence. I am concerned that the Defense Department is not postured correctly to invest in the correct emerging technologies or to play the appropriate role of co-developer and early adopter of the advanced capabilities they will enable.

The technology development environment has become globalized and extremely fast moving. We need to make sure that we are looking at the right technologies, have the processes in place to take advantage of them, and deliver new capabilities to warfighters at the speed of technological change, and faster, much faster, than our peer adversaries. Overlaying this is the competition with China in both the national security and economic sectors and their aggressive attempts to undercut our current technological superiority.

We must also be concerned about the strength of our national research and innovation enterprise, including the workforce, the health of the manufacturing and industrial base, and the infrastructure that we need to support technology development.

Finally, all of this must be in light of budget constraints and competing challenges for the Department of Defense (DOD), namely balancing modernization with near-term readiness and force structure. We also want to make sure that we are making the best use of the great advantages that this nation possesses in the global competition. For example, we have the world's best innovators in defense industry and the commercial sector. Are there ways that we can help them work more closely together to produce next-generation defense systems.

We have the world's leading research universities, whose efforts have led to all the emerging technologies we are discussing today and also many of the technologies that we use in our current force and even our daily lives. Are we still making best use of their talents to support national security?

We are still the magnet for the world's best and brightest technical minds. Are we positioning ourselves to continue to attract that talent and to get them to work on the complex national security challenges of the future?

The technologies and systems that we take for granted for both national security, such as precision weapons, the nuclear deterrent GPS [global positioning system], and the internet, were all called emerging technologies at some point. It took focused investment of resources and the time and toil of countless scientific experts to solve the technical challenges that inevitably occurred, but it also took leaders that were willing to patiently protect those resources and people, encourage risk-taking, and to accept and drive the changes necessary to cut through the red tape and support these systems moving from the lab into our operations. With today's emerging technologies and changing world, we are faced with similar decisions and challenges, and we need to ensure that we have the same experts and leadership for success.

Again, I want to thank you all for your willingness to appear today, and I look forward to your testimony.

Senator Inhofe is delayed, and he indicated that he would prefer to have his statement submitted for the record. I ask that that be submitted, without objection. So ordered. Thank you very much.

[The prepared statement of Senator James Inhofe follows:]

PREPARED STATEMENT BY SENATOR JAMES INHOFE

Thank you, Mr. Chairman.

Dr. Schmidt, Mr. Smith and General Carlisle. Thank you for being here to talk about this important topic today.

As highlighted in the 2018 National Defense Strategy Commission report, the United States must stay ahead in several emerging technologies to maintain or regain a warfighting advantage against China and Russia.

Some of those key technologies are Artificial Intelligence (AI), 5G, Hypersonics, Emerging Biotechnologies and Quantum Computing, and Directed Energy.

The COVID–19 pandemic has shown that Department of Defense emerging biotechnology research, including that done over the last decade at the Defense Advanced Research Projects Agency (known as DARPA) has been critical in fostering new technologies that have been critical in vaccine and therapeutic development in this pandemic.

I am looking forward to hearing our witnesses talk today about what technologies are most important for us to adopt for our warfighters to be best prepared for the future.

Russia and China are aggressively developing these capabilities, and, in some cases, we are already behind or falling behind. Without action, the United States may find itself at a technological disadvantage in future conflicts.

However, the challenges facing the Department of Defense are not just about developing new technologies, but the Department must also reform its processes, policies and culture to be able to more quickly adopt and deploy new technologies-all while making sure that we are balancing the need to modernize our military capabilities with maintaining near-term readiness.

Thank you for appearing, and I look forward to your testimony.

Chairman REED. And now I will ask the witnesses to begin. Dr. Schmidt, please.

STATEMENT OF DR. ERIC E. SCHMIDT, CO–FOUNDER, SCHMIDT FUTURES

Dr. SCHMIDT. Thank Mr. Chairman, I think I can speak for all of us that we are incredibly proud to have been invited here, and it is a great honor and privilege to be part of your discussions.

I am one of these people who, like everyone in the room, believes very strongly that America is a great country and that our leadership is very, very important. I also believe that our national security in the United States is tied to both our economic security and our military security. And I am worried that we do not understand the competitive threat from China to what we are trying to do, and I want to take you through some of the things that are going on.

In each of the following strategic areas, China is pushing to meet or beat the work of the United States: semiconductors, where both countries are dependent on Taiwan and South Korea; artificial intelligence (AI), China catching up relatively soon, according to their doctrine; energy: they are way down the maturation curve, and we need to jump forward or lose that industry; quantum: they have a well-funded effort and there are important national security consequences from the use of quantum in a number of areas; communications: we are all familiar with the dominance of Huawei and the issues for national security that is provided. You can see that

the success of Huawei in the developing world will be a long-term problem for our country; and synthetic biology, the building of life. China is busy building a biobank and is trying to sort of come to global domination in a number of key areas.

These are contests of values as well as investments, and it is important that American values, the things that we hold and cherish so deep, are the winners in all of these technological areas. We need to do a whole bunch of things, including focus on advanced production, which covers manufacturing, architecture, and assembly, and intelligence-augmented infrastructure, everything from our roads and bridges to pipelines to electric networks. This is how America wins.

So what we need to do is recognize that China is a very significant competitor and that we need to respond to the sort of things they are doing and make sure we stay well ahead. So I will give you a set of examples, which will inform the discussion.

The United States national security apparatus, and in particular the DOD, treats software as a very low priority. It needs to be treated as a very high priority. Software is going to drive pretty much all of the interesting accomplishments in the national security sense in the next 10 or 20 years, and hiring and training and personnel policies that are similar to the software companies are important.

We need to build missiles the way we now build cars. It turns out that the modern car plan designs everything in a design studio, knows everything, presses a button, and boom, all that come out, and they work really, really well. The bespoke design approaches, where the contractors today and the primes operate, are completely counter to the way a Silicon Valley company would operate. You put a design team together, they figure it all out, they work very quickly, very much like the original Lockheed Skunk Works. We have lost that, and it is important to retain that.

We must make sure, for our economic strength, that the next generation of technologies in AI, semiconductors, and so forth, are successful not just for our commercial operations but our national security.

If I continue to give you a few more examples, we are going to have to have some kind of leadership out of the White House. I am the chairman of the National Security Commission on AI. Thank you. You all asked for it. It is coming out March 1. One of its many recommendations is that there be a technology competitiveness council at the White House, driven by the Vice President, to get the kind of right attention on all of these issues.

We are going to have to basically fund an AI research network, one of our recommendations. We are going to have fund biology labs, where you can order up the kind of biology that you need and it shows up the next day, so you can continue to be innovating. We are going to need to welcome high-skills immigrants into the U.S., and keep our foreign-born PhDs here in the country.

We are going to need a solution to the 5G problem. China will soon have 1 billion people connected to a 1 gigabit network on each of their phones. The United States strategy does not have enough bandwidth allocated for 5G, and the telecommunications companies just spent $80 billion to purchase frequency in the C-band. That

$80 billion went to the U.S. Government. In my view, instead of spending it, to the United States Government, it should have been used to spend to build the infrastructure to build the 5G infrastructure to compete with China and to provide leadership for us.

The important thing here, and I will finish up by saying, is that the private sector is America's great strength. We move faster and globally than any government could. Fast, iterative design and product cycles are the key to competitiveness, and we need global platforms or we will be forced to use the Chinese ones, which is a disaster. I propose the combination of what I said, adopt the AI Commission recommendations, which are coming out on March 1, target the military systems that can be accelerated by some of these new design approach—you are wasting money with the existing design cycles. It is not helping with preparedness. And then figure out a way to build agreements between American industry—and, Mr. Chairman, you already talked about this—and the military, and also build very tight relationships with our trusted strategic partners in other countries.

Thank you.

[The prepared statement of Dr. Schmidt follows:]

PREPARED STATEMENT BY DR. ERIC E. SCHMIDT

Chairman Reed, Ranking Member Inhofe, Members of the Committee, thank you for the opportunity to testify on the importance of emerging technologies for the future of our national security.

I will begin with a broad view of the state of U.S. technology leadership, then discuss the future defense landscape, and conclude with some recommendations for the Pentagon.

I offer these views in my personal capacity, but they are informed by my experience leading the National Security Commission on Artificial Intelligence (NSCAI) and the Defense Innovation Board (DIB), as well as my work in philanthropy, with Schmidt Futures, and in the private sector. Many of my points here preview the conclusions and recommendations in the AI Commission's forthcoming Final Report set to be released publicly on March 1.

My argument today is straightforward: When it comes to emerging technologies, our government needs to get the fundamentals right. I mean that in two ways. First, to preserve national competitiveness, we need to focus on the fundamental technologies that will have broad impacts on our economy, our society, and our security. Second, to shape the military we will need to defend the United States in the future, we have to put the fundamental building blocks into place as soon as possible. Those include the people, the research, the technology infrastructure, and other basic elements that I will describe.

The AI Commission's Final Report includes many critical recommendations to win the global technology competition and strengthen national defense. I urge the Committee to seriously consider adopting all of the recommendations that are relevant to your work, and also to encourage your colleagues on other committees to do the same.

The logic for action is compelling.

GLOBAL TECHNOLOGY LEADERSHIP AND NATIONAL SECURITY

Extending our global leadership position in technology is both an economic and a national security imperative. Innovation is the foundation of our economy, and the source of our military advantage. Leadership gives our government and military access to the most advanced available technologies. It puts us in the best position to secure them against vulnerabilities. And it enables us to set standards for their responsible use.

I am convinced that the threat of Chinese leadership in key technology areas is a national crisis and needs to be dealt with directly, now. The President had it exactly right in his speech in Munich: the United States is in a "long-term strategic competition with China."

China is pursuing technology leadership through strategic investments in a wide range of critical technology areas, including through the Made in China 2025 initiative. Consider artificial intelligence, which is the fulcrum of this broader technology competition. AI will be leveraged to advance all dimensions of national power—from healthcare to food production to environmental sustainability. The successful adoption of AI in adjacent fields and technologies will drive economies, shape societies, and determine which states exert influence and exercise power in the world. Many countries have national AI strategies. But only the United States and China have the resources, commercial might, talent pool, and innovation ecosystem to lead the world in AI. In some areas of research and applications, China is an AI peer, and it is already more technically advanced in certain applications. Within the next decade, China could surpass the United States as the world's AI superpower.

In addition to AI, China is seeking to lead the world in quantum computing, fifth generation (5G) networks, and synthetic biotechnology, among other areas. Beijing sees its national strategies in these areas as mutually reinforcing. The CCP has made clear which technologies it views as top national priorities. In each of these areas China is pushing to meet or beat our work.

If China takes the lead, the first-mover advantages in developing and deploying new technologies will make it difficult for the United States to catch up. In critical sectors with strong network effects like telecommunications, a winner-take-all dynamic raises the stakes for rapidly developing leading technology platforms. The United States Government must develop a unified strategy to advance and protect the technologies that will underpin national competitiveness in the middle decades of the 21st Century, even as we continue to cooperate with competitors like China in areas of mutual interest.

A WHITE HOUSE APPROACH TO NATIONAL COMPETITIVENESS IN CRITICAL TECHNOLOGIES

The United States needs an integrated approach to federal investments and policies across a range of emerging technologies. A comprehensive national strategy would set and reinforce priorities and would reconcile budget tradeoffs. The strategy should be led by the White House. I strongly endorse the AI Commission's recommendation to establish a new White House-led Technology Competitiveness Council. This would be chaired by the Vice President and overseen by a senior White House coordinator to ensure the President has the organization in place to develop, drive, and fund a real national technology strategy.

A national strategy should focus on fundamental technologies with broad impact on national competitiveness and security. A priority shortlist should include AI, 5G, microelectronics, biotechnology, and quantum computing. The importance of these areas is widely recognized. The shortlist should also include advanced production (which covers manufacture, agriculture, and assembly), as well as infrastructure augmented by machine intelligence (everything from roads to bridges to pipelines to electric networks).

Advanced production is essential to enable the country to produce the goods it needs in the face of supply chain shocks, natural disasters, epidemics, and so on. And it can permit leapfrogging through greater efficiencies and energy optimization while reducing decaying stockpiles of goods. The capacity to produce high-tech goods domestically is critical to national security, both to maintain access to finished goods and as a driver of innovation. The United States must strive for self-reliance in industries that are critical to national security or that would take too long to regenerate in the event of protracted conflict.

New infrastructure is essential to handle emergencies (for example, think of Texas's frozen gas supplies, or California's shifting wildfires), permit tradeoffs among different modalities (trains versus trucks versus pipelines), and reduce both environmental impact and total cost of ownership. U.S. physical infrastructure remains largely disconnected: no U.S. cities are ranked among the world's top 10 in smart city connectedness, and only one is in the top 30.[1] Maximizing citizens' access to the digital economy, and more closely connecting the physical and digital worlds, will be necessary to fuel future growth. This can add a significant boost to national GDP.

---

[1] *Smart City Index*, IMD, 8 (Oct. 2019), *https://www.imd.org/research-knowledge/reports/imd-smart-city-index-2019/#:~:text=The%20Top%2010%20smartest%20cities,and%20Dusseldorf%20(10th).*

A MORE ASSERTIVE GOVERNMENT ROLE

On a level playing field, the United States is capable of out innovating any competitor. However, today, there is a fundamental difference in approaches to innovation between the United States and China that puts American leadership in peril. For decades, the United States innovation model has been the envy of the world. The open exchange of ideas and free markets, with targeted government involvement to support basic research, are pillars of the American way of innovation and reflect American values. In America, tech firms compete for market share; they are not instruments of state power.

Most technology advances in the United States will be driven by the private sector and universities. We must not lose an innovation culture that is bottom-up, and infused with a garage startup mentality. However, keeping things exactly the same as we have in the past is not a winning strategy. Large tech firms cannot be expected to compete with the resources of China or make the big, nation-wide investments the United States will need to stay ahead. We will need a hybrid approach that more tightly aligns government and private sector efforts to win.

The private sector is America's great strength; companies move faster and more globally than any government could. However, given the changing landscape, the U.S. Government must take a hands-on approach to national technology competitiveness. Promoting a diverse and resilient research and development (R&D) ecosystem and commercial sector is a government responsibility. Expanding talent pipelines, more quickly reforming immigration and visa authorities like H–1B to attract the world's best, and improving our education system are all public policy choices. Protecting critical intellectual property and thwarting the systemic campaign of illicit knowledge transfer being conducted by competitors is a government obligation. Protecting hardware advantages and building resiliency into supply chains necessitates legislation and federal incentives. Bringing together like-minded allies and partners requires U.S.-led diplomacy.

DEMOCRATIZING AI RESEARCH: A NATIONAL RESEARCH RESOURCE

Here is one concrete example of government action that could spur nation-wide technology advances with benefits for overall national competitiveness. Today, I worry that only a few big companies and powerful states will have the resources to make the biggest AI breakthroughs. Despite the diffusion of open source tools, the needs for computing power and troves of data to improve algorithms are soaring at the cutting edge of innovation. The government should democratize access to compute environments, data, and testing facilities in order to provide researchers beyond leading industry players and elite universities the ability to pursue progress on the cutting edge of AI. It can do this by creating a National AI Research Resource (NAIRR), which would provide verified researchers and students subsidized access to scalable compute resources, co-located with AI-ready government and non-government data sets, educational tools, and user support.[2] It should be created as a public-private partnership, leveraging a federation of cloud platforms.[3] The AI Commission has detailed plans to implement this recommendation.

DIGITAL INFRASTRUCTURE: GETTING 5G RIGHT

Promoting the rapid buildout of 5G network infrastructure is a national security imperative. Future military preparedness will rely on it, and fostering technologically competitive U.S. companies of all sizes depends on it. Moreover, as the pandemic has made clear, strong digital infrastructure bolsters our resilience to systemic shocks, allowing Americans to access telehealth, education, and other services they need in times of crisis. 5G networks will be the connective tissue between all advanced mobile systems, and particularly in conjunction with advances in AI and

[2] Acting on a recommendation NSCAI issued in our *First Quarter Recommendations,* Congress has taken the first step to establish the NAIRR in the Fiscal Year 2021 National Defense Authorization Act, creating a task force to develop a roadmap for a future NAIRR. The result of this effort will be due to Congress 18 months after appointment of task force members. See Pub. L. 116–283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021); see also First Quarter Recommendations, NSCAI at 2 (Mar. 2020), *https://www.nscai.gov/previous-reports/*.

[3] This approach could build on successful models such as the COVID–19 High Performance Computing Consortium, *(https://covid19-hpc-consortium.org/)* and NSF's CloudBank, *(https://www.cloudbank.org/)*.

[4] See Testimony of Elsa Kania before the United States-China Economic and Security Review Commission, Hearing on Technology, Trade, and Military-Civil Fusion (June 7, 2019), *https://*

computing power, will enable profound new technological capabilities directly in user devices. China has treated this as a strategic priority and invested heavily in a Gigabit nationwide mobile network, which it will soon achieve. In the United States, however, 5G network development has proceeded slowly—only delivering incremental increases in data speeds and coverage. We should act now and decisively to improve the U.S. position. I have three ideas.

First, we should *reinvest spectrum auction proceeds into network infrastructure.* I suggest we examine ways to recycle the $81 billion in revenue from the Federal Communication Commission's (FCC) Auction 107 of "C-band" spectrum, and any future auctions, into funding designated for network infrastructure, with an allocation mechanism designed to promote rapid and equitable buildout by the private sector. Second, we should *explore spectrum sharing and other auction alternatives.* For example, DOD has invited public input into how it could share spectrum it controls with industry. I have suggested a model wherein DOD retains control of the spectrum but allows industry to share it in exchange for industry building the required infrastructure quickly, and at its own cost. To be clear, this is not "nationalized 5G," as some critics have claimed. This would be a privately built, operated, and maintained network that prioritizes DOD use. In any case, I believe DOD should be applauded for examining innovative solutions to this urgent problem. Third, we should *modify auction terms.* For any future auctions, particularly in the C-band spectrum that is ideally suited for 5G, the FCC should impose strict buildout requirements for auction winners that ensure that the necessary network infrastructure gets built quickly and equitably. We can't just wait for 6G or 7G to arrive. Competitive advantage surrendered now is likely lost forever. I see this as an untenable national security risk.

HARDWARE VULNERABILITIES: MICROELECTRONICS

After decades leading the microelectronics industry, the United States is now almost entirely reliant on foreign sources for production of the cutting-edge semiconductors that power all of the AI algorithms that are critical for defense systems and everything else. The dependency on semiconductor imports, particularly from Taiwan, creates a strategic vulnerability from adverse foreign government action, natural disaster, and other events that can disrupt the supply chains for electronics—as we have seen in the auto industry recently. Although American universities and firms remain global leaders in the key areas of semiconductor R&D and chip design, the semiconductor industry is now highly globalized and competitive. Taiwan Semiconductor Manufacturing Corporation (TSMC) leads the world in semiconductor contract manufacturing and Samsung in South Korea is also producing state-of-the-art logic chips. Simultaneously, in a bid to catch up and achieve chip self-sufficiency, China is pursuing unprecedented state-funded efforts to forge a world-leading semiconductor industry by 2030. If a potential adversary bests the United States in semiconductors, it could gain the upper hand in every domain of warfare.

The United States should commit to a strategy to stay at least two generations ahead of China in state-of-the-art microelectronics and commit the funding and incentives to maintain multiple sources of cutting-edge microelectronics fabrication in the United States. I would recommend:

(1) the Executive Branch should finalize and implement a national microelectronics leadership strategy; (2) Congress should offer a 40 percent refundable tax credit and grants for domestic fabrication investments by firms from the United States and its allies; and (3) Congress should appropriate an additional $12 billion over the next five years for microelectronics research, development, and infrastructure in key areas such as advanced packaging. These investments should help accelerate the transition of ideas from university prototypes to commercial-scale production domestically.

Together, these efforts will enable the U.S. Government, private sector, and academia to rise to the challenge of rebuilding U.S. semiconductor superiority. Focusing our efforts to develop domestic microelectronics fabrication facilities will reduce dependence on imports, preserve leadership in technological innovation, support job creation, improve national security and balance of trade, and enhance the technological superiority and readiness of the military—an important consumer of advanced microelectronics.

IMPLICATIONS OF THE EMERGING TECHNOLOGY COMPETITION FOR DEFENSE

Emerging technologies are creating new whole-of-society threats. This is not just, or even primarily, a traditional battlefield challenge in the near term. AI-enabled capabilities will be tools of first resort in a new era of conflict. State and non-state

actors determined to challenge the United States, but avoid direct military confrontation, will use AI to amplify existing tools and develop new ones. Adversaries are exploiting our digital openness through AI-accelerated information operations and cyber attacks. "Ad-Tech" will become "NatSec-Tech" as adversaries recognize what advertising and technology firms have recognized for years—that machine learning is a powerful tool for harvesting and analyzing data. Using espionage and publicly available data, adversaries will gather information and use AI to identify vulnerabilities in individuals, society, and critical infrastructure.

Looking more narrowly at military issues, key technology areas have important and wide-ranging defense applications. Fundamentally, the sources of battlefield advantage will shift from traditional factors like force size and levels of armaments, to factors like superior data collection and assimilation, connectivity, computing power, algorithms, and system security.

The advantages to be gained are well understood by our competitors. Russia has plans to automate a substantial portion of its military systems. China's military has embraced "intelligentized war"—investing, for example, in swarming drones to contest United States naval supremacy.[4] China is testing and training AI algorithms in military games designed around real-world scenarios. The recent use by Azerbaijan of drones and loitering munitions to defeat air-defense systems and mechanized forces in Nagorno-Karabakh is a harbinger of the kind the future American forces will soon face.

Defending against AI-capable adversaries without employing AI is an invitation to disaster. AI will compress decision time frames from minutes to seconds, expand the scale of attacks, and demand responses that will tax the limits of human cognition. Human operators will not be able to defend against AI-enabled cyber or disinformation attacks, drone swarms, or missile attacks without the assistance of AI-enabled machines. The best human operator cannot defend against multiple machines making thousands of maneuvers per second potentially moving at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can.

The Pentagon is developing many operational concepts to fight these future wars. But I am concerned that at the Department's current pace of technology integration, the military will not be capable of carrying them out in time. To fight as the military intends to fight in 2030 or 2035, the Department needs to get the fundamentals in place well before then.

THE COMMERCIAL MODEL

DOD needs to revise how it builds things. Silicon Valley has shown a way to do this: form smart teams, drive hard deliverables, and move quickly. The government does not allow any of that: procurement is separate from design and design feedback, software is an afterthought, and the big systems are siloed so they can't be integrated together. We should build missiles the way we now build cars: use a design studio to develop and simulate in software. Return to the skunkworks model of fast iteration. The long design cycles are killing our competitiveness. Fast iterative design and product cycles are the key to competitiveness. DOD should target military systems that can be accelerated by a new design studio and digital twinning approach and change procurement rules to allow for it. At the very least DOD should pick a few programs and agree collectively to run them very differently.

GETTING THE FUNDAMENTALS RIGHT AT THE PENTAGON

I recognize I cannot wave a magic wand over the Pentagon, so below are some important concrete things DOD should do now at a bare minimum. Again, the NSCAI has detailed recommendations that I endorse for getting the technical backbone right. These focus mainly on AI but most have broad applicability for new technology integration and development in DOD.

1. INTEGRATE EXISTING DIGITAL TECHNOLOGIES NOW

The Pentagon's byzantine processes can sometimes obscure a basic point. Much of the new technology the military needs is already available on the commercial

[4] See Testimony of Elsa Kania before the United States-China Economic and Security Review Commission, Hearing on Technology, Trade, and Military-Civil Fusion (June 7, 2019), *https://www.uscc.gov/sites/default/files/June%207%20Hearing—Panel%201—Elsa%20Kania—Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence—0.pdf;* Elsa Kania, "AI Weapons" in China's Military Innovation, Brookings at 1 (April 20, 2020), *https://www. brookings.edu/wp-content/uploads/2020/04/FP—20200427—ai—weapons—kania—v2.pdf.*

market. Buy more of it. Doing so would create market incentives to produce more and more useful defense technologies. The Department should:

- *Prioritize existing technologies that can augment intelligence functions*—especially applications of AI. There are significant opportunities to better leverage commercially available technologies to improve situational awareness and indications and warnings. Automation and human-machine teaming can enhance the effectiveness of a range of ISR platforms and improve the full cycle of intelligence collection and analysis.
- *Network DOD's digital innovation initiatives to scale impact.* A number of the Department's innovation organizations have delivered results.[5] But they are uncoordinated and under-resourced. DOD signaling of technology priorities is ad hoc and is not supported by a track record of significant DOD investments in digital technology with non-traditional vendors. As a result, national security AI applications attract less private-market investment. The Department should harmonize its innovation initiatives to carry out a coordinated strategy for commercial technology solutions. The Under Secretary of Defense for Research and Engineering should direct this effort.
- *Establish AI delivery teams at each Combatant Command.* AI delivery teams should be embedded at each Combatant Command and should be capable of supporting the full lifecycle of AI development and fielding—including data science, engineering, testing, and production. Teams should include forward-deployable components to act as the local interface with operational units.

2. IMPROVE THE DEPARTMENT'S DIGITAL INFRASTRUCTURE

DOD took a promising first step in 2020 with the issuance of a Data Strategy.[6] However, the Department lacks the modern digital ecosystem, collaborative tools and environments, and broad on-demand access to shared AI resources it needs to integrate AI across the organization. The Secretary of Defense should direct the establishment of a DOD-wide digital ecosystem. The Secretary should require that all new joint and service programs adhere to the design of this ecosystem, and that, wherever possible, existing programs become interoperable with it by 2025. This technical foundation should: 1) provide access to leading cloud technologies and services for scalable computing; 2) enable the sharing of data, software, and capabilities through well-documented and hardened application programming interfaces with proper access controls; and 3) give all DOD developers and scientists access to the tools and resources they need to drive new AI capabilities.

At the same time, the Department should define a joint warfighting network architecture by the end of this year. The goal should be to create a secure, open-standards systems network that supports the integration of AI applications at operational levels and across domains.[7] It should be accessible by all of the military services and encompass several elements, including command and control networks; data transport, storage, and secure processing; and weapon system integration.

3. REFORM LEADERSHIP STRUCTURES

Leadership is the critical variable. Driving innovation requires organizational change, not just technical capacity. Senior civilian and military officials should set clear priorities and direction, empower subordinates, and accept higher uncertainty and risk in pursuing new technologies. Specifically, DOD should:

- Establish a high-level Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence.[8]

---

[5] DOD innovation initiatives include various entities across the military services and the Office of the Secretary of Defense that are focused on bridging the gap with the commercial sector, especially with start-ups and non-traditional vendors. These include the Defense Innovation Unit, AFWERX, NavalX, and the Army Applications Laboratory, among others.

[6] See Executive Summary: DOD Data Strategy, U.S. Department of Defense (Sept. 30, 2020), *https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF*.

[7] The network envisioned is well-aligned with ongoing DOD efforts to embrace standards-driven interoperability, system adaptability, and data-sharing. See *Memorandum for Service Acquisition Executives and Program Officers,* U.S. Department of Defense (Jan. 7, 2019), *https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular—Open—Systems——Approach.pdf*.

[8] Section 236 of the Fiscal Year 2021 National Defense Authorization Act allows the Secretary of Defense to establish a steering committee on emerging technology and national security threats. However, the structure described in Sec. 236 does not include leadership from the Intelligence Community, which is critical to ensuring a coordinated approach between DOD and the IC. See Pub. L. 116–283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

- Ensure the JAIC Director remains a three-star general or flag officer with significant operational experience who reports directly to the Secretary or Deputy Secretary. [9]
- Appoint the Under Secretary of Defense for Research and Engineering as the co-chair and chief science advisor to the Joint Requirements Oversight Council.

4. BUILD NEW TALENT PIPELINES

There is no conceivable program, pilot, internship or pathway for tech talent that will close the DOD talent deficit, and the same problem exists across all national security agencies. I cannot stress enough the need for a radical rethinking of talent pipelines. The NSCAI has exactly the right idea. This is not a time to add a few new positions in national security departments and agencies for Silicon Valley technologists and call it a day. We need to build entirely new talent pipelines from scratch. We should establish a new Digital Service Academy and civilian National Reserve to grow tech talent with the same seriousness of purpose that we grow military officers. The digital age demands a digital corps. Just as importantly, the United States needs to win the international talent competition by improving STEM education and our highly skilled immigration system.

Technology experts need better ways to spend a career in government focused on their fields. Current talent management practices often put experts in positions that are unrelated to their areas of expertise. Many leave the government or military as a result. DOD should create civilian and military career fields in software development, data science, and AI. My philanthropy, Schmidt Futures, is sponsoring a small pilot, called the Center for Digital Talent, that aspires to open new recruiting pathways for technologists into the Department, but much more work needs to be done.

Senior leader education is also very important. Leaders who do not understand new technologies are less likely to pursue programs that will add value. They will not be able to incorporate new technologies into operational concepts or organizational processes. DOD should create emerging technology critical billets and an emerging technology certification process that is analogous to the current joint qualification process.

DOD also needs to integrate computational thinking and AI basics into junior leader training. NCOs and junior officers need a baseline level of knowledge to responsibly field new capabilities. DOD needs to integrate digital skills and computational thinking into pre-commissioning requirements, initial officer training, and NCO education. I recommend focusing on problem curation, data collection and management, the AI lifecycle, probabilistic reasoning and data visualization, and data-informed decision making.

5. INVEST MORE IN S&T AND ALIGN INVESTMENTS WITH STRATEGY

The Department should commit to spending at least 3.4 percent of its budget on science and technology, with a focus on emerging and disruptive technologies. [10] This would be a significant increase from the current level of 2.3 percent, and would follow longstanding recommendations by the Defense Science Board and others, which are echoed in the forthcoming NSCAI report. For AI in particular, the Department should increase R&D spending from around $1.5 billion to at least $8 billion by 2025. [11]

To align investments with strategy, DOD should produce a Technology Annex in the next National Defense Strategy document. This annex would prioritize technology investments and development in relation to the military capabilities needed to carry out future operational concepts. And it would clearly signal which technologies are Department priorities.

---

[9] The Senate confirmed Lt. Gen. Michael Groen to lead the JAIC in September 2020. NSCAI's has recommended that the three-star requirement be statutorily mandated.

[10] This would encompass DOD budget activities 1 through 3, which can help produce the advancements that will drive the next generation of capabilities.

[11] This should encompass investments in pushing the boundary of AI technology towards new capabilities, and developing AI-enabled elements to build into existing systems and platforms. The AI Commission has identified a number of critical areas to be supported: human-AI teaming; advanced scene understanding; intelligent edge devices, computing, and networking; robust and resilient AI; AI test and evaluation, verification and validation; integrated AI; modeling and simulation for decision support; autonomous AI systems; advances toward more general artificial intelligence.

6. REFORM DOD'S OUTDATED BUDGET PROCESS

I've stated before that the DOD's problem is not innovation, but innovation adoption. Its outdated, industrial-age budgeting process creates a valley of death for new technology, allowing basic research funding and also procurement of weapons systems, but preventing the flexible investment needed in prototypes, concepts, and experimentation of new concepts and technologies like AI.

Although we have had 50 years of acquisition reform, we have not meaningfully changed the PPBE (Planning, Programming, Budget and Execution) process developed in the 1960s. Congress and the Defense Department need to work together to immediately authorize and fund pilots, and set the stage for more sweeping reform. [12]

7. ENSURE RESPONSIBLE DEVELOPMENT, TESTING, AND USE OF AI-ENABLED AND AUTONOMOUS SYSTEMS

I see a consensus emerging on how to use AI responsibly for defense. The DIB produced a set of AI ethics principles. The AI Commission followed with more granular, operational-level guidance. These efforts have been well received by DOD leadership.

If an AI-powered system does not work as designed with predictability and guided by clear principles, then operators will not use it, the military services will not embrace it, and the American people will not support it. Rushing to integrate AI would be counterproductive if it caused service members to lose confidence in its benefits. All military systems require rigorous testing, safeguards, and an understanding of how they might operate differently in the real world than in a testbed. AI-enabled autonomous weapon systems could be more precise, and as a result, reduce civilian casualties. But they also raise important ethical questions about the role of human judgment in employing lethal force. If improperly designed or used, they could also increase the risk of military escalation.

An entirely new approach to testing, evaluation, validation and verification (TEVV) will be needed. DOD should tailor and develop TEVV policies and capabilities to meet the changes needed for AI as its AI-enabled systems grow in number, scope, and complexity. This should include establishing a TEVV framework and culture that integrates continuous testing; making TEVV tools and capabilities more readily available across DOD; updating or creating live, virtual, and constructive test ranges for AI-enabled systems; and restructuring the processes that underlie requirements for system design, development, and testing.

CONCLUSION

It has been a great privilege to have worked at the leading edge of the American technology industry for over 30 years. That work began, for me, with grants from the Federal Government.

My graduate work in computer science in the 1970s and 1980s was funded in part by the National Science Foundation and the Defense Advanced Research Projects Agency. These and other investments fueled a renaissance of technology that made America and its technology sector the envy of the world and our military the most capable fighting force in history.

But right now, the United States is not playing to win. It is the Chinese who are competing to become the world's leading innovators. Never before in my lifetime have I been more worried that we will soon be displaced by a rival or more aware of what second place means for our economy, our security, and the future of our nation.

A bold, bipartisan initiative can extend our country's technology advantage but only if we act now. Success matters for more than our companies' bottom lines and our military's battlefield edge. Because our technology and that of our closest allies and partners embodies our values, advancing individual liberty and strengthening free societies are also on the line. I leave you with the urgent message that for the American model to win, the American Government must lead. To that end, I urge Congress again to adopt all of our AI Commission recommendations, which provide a clear blueprint to win a technology competition that is centered around AI.

---

[12] I am encouraged that the Fiscal Year 2021 NDAA included support for the Department's Budget Activity 8 pilot program, which seeks to overcome the barrier that DOD spending categories pose to the development and sustainment of digital technologies. Congress and DOD could build on this pilot to establish needed flexibility more broadly by creating a single source of funding that could support the full lifecycle of development, delivery, and continuous update for AI and other digital technologies.

Chairman REED. Thank you very much. Mr. Smith, please.

STATEMENT OF MR. BRAD L. SMITH, PRESIDENT, MICROSOFT CORPORATION

Mr. SMITH. Well, thank you, Mr. Chairman and members of the committee, and let me join Eric in saying thank you for having this hearing and giving us the opportunity to share our ideas with you.

Let me build on what Eric has said, because I think he covered a lot of things extremely well. Clearly technology is changing every aspect of society, including the nation's national security needs. It starts with the cloud and the edge and it goes to 5G and AI and a future based on quantum computing. And I think the first question for all of us is really to ask, how should we, as a nation, think about what this means for the defense of the country in the future?

I think the answer is really with a combination of confidence and concern. I think there are many reasons to be confident, and, Mr. Chairman, you referred to some of them. We have the world's best research universities. We have an enormously creative and dynamic commercial technology sector. We have a military that both quantitatively and qualitatively, on a person-by-person basis, is the best in the world. And perhaps most importantly, we stand for democratic principles and values that most of the world, quite rightly, wants to follow.

That is a formidable combination, and yet I do believe there are causes for concern, really two. Eric covered the first well. We are competing with a formidable competitor. China is investing, and it is investing heavily in every area of technology we are here to talk about this morning.

But I think there is a second dimension as well. Over time, technology either favors offensive weaponry in attacks or defensive protection against attacks. And if you think about American history, geography has always been our friend. We could look not to one large ocean but two to keep our adversaries at a distance. But the truth is the internet has changed all of that. It has made everybody each other's next-door neighbor.

And I think we should draw a lesson, even from the events of the last week. Think about what happened when the electrical grid went down in Texas. Think about the danger to American civilians if there is a disruption of the water supply. And then think about a future where a nation need not send missiles or planes but can simply send code to do its fighting for it. This is changing the threat landscape, and unfortunately favors offensive attacks against a very broad defensive horizon that must be secured.

So what do we do? Well, Eric has already touched on a number of important ideas. I would mention four. Number one, we need to strengthen the nation's digital infrastructure and digital defenses, and that touches every part of the public sector and every part of the private sector as well. Number two, we need to think about and decide how we can harness these advances in technology to equip our warfighters in the nation's military it can move faster and continue to be at the technological edge.

Certainly at Microsoft we have had the opportunity to do that in recent years. We have had the opportunity to work with the Department of the Army on the Integrated Visual Augmentation Sys-

tem goggles that provide not only night vision and thermal vision but lots of other data as well. And we have seen the Army benefit from the procurement reforms that this committee has advanced, and believe it, it changes everything, in my view, about how we can innovate faster.

Number three, we need to think not just about military applications but the health of our technology base as a whole—the education of our people, the investment in higher education and research, our immigration system, and how we advance the areas of technology where we risk most falling behind.

And finally, we need to work more closely with our allies than ever before, and we need to lead with moral authority and not the strength of technology alone. We need to remember every day that there will never be perhaps another day when we will be competing with an adversary that has a smaller population than ours. But we do, in fact, have a set of human rights protections and democratic values that can pull the world together. And when we succeed in doing that, both to harness the power of our technology and to build an alliance of partners and friends, I think we put this country on the course that it needs, that should give us all more confidence than concern.

Thank you very much.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT BY BRAD SMITH

Chairman Reed, Ranking Member Inhofe, and Members of the Committee, thank you for the opportunity to offer some perspectives on issues that are vital to U.S. national security.

Digital technology plays an increasingly critical role in the defense of the nation. Emerging technologies are redefining the way we secure the peace, maintain our defense, and when necessary, fight wars.

Innovations in cloud and edge services, artificial intelligence, and 5G are already having a direct and practical impact on the nation's defense. As the decade progresses, we should look to the potential importance of quantum computing as well. These technologies will redefine the requirements for military operations at mission speed, based on their ability to harness massive amounts of data and computational power. They will also be interconnected: future computational capabilities will be defined by an ability to accelerate applications across the cloud, using AI and advanced silicon. They will reshape the security needs for the nation's critical infrastructure and affect training requirements for our military personnel. In short, new technology will have a pervasive impact on our national security.

Yet one would be hard-pressed to say that the country currently has a comprehensive strategy to harness these technologies for the country's defense. A more cohesive approach is needed.

This strategy needs to be grounded in a clear-eyed assessment of where digital technology is going and the nature of global competition in technology markets. Speed matters. The United States must move more quickly to advance broad-based technology innovation and pursue new approaches to use, secure, and adapt commercial advances for military applications. This requires a holistic approach to government-sponsored basic research, commercial technology development, and investments in new military uses. It will require an even closer partnership between the government and the tech sector.

An essential starting point is to ask: What are we trying to accomplish? To be sure, the protection of American lives and the peace and prosperity of our country are the primary considerations. But so is the country's unique role in providing global leadership. When we think about the role of technology in the context of the country's defense and national power, our ability to lead the world and to establish and defend the most important connective tissue of the international order—in areas such as finance, cybersecurity, healthcare, and transportation—marks one of the deepest roots of American power and security.

For the last 70 years, the United States has provided what we might think of as the global public operating system in every essential area of life. The next 70 years will witness this not as a metaphor, but as real software power. Any successful national security strategy therefore must also find ways for us to continue to offer the best options for nations around the world as they transition every part of their national lives to a digital age. As in the past, there is no substitute for technology the world can trust, based on the United States' commitment to human rights and democratic values.

Based on this vision, the country should pursue a digital defense strategy with seven objectives:

1. Focus on where digital technology is going and where advantage will lie.
2. Strengthen the nation's technology leadership by investing in talent and research.
3. Enhance American competitiveness and security by modernizing technology-related trade and investment policy.
4. Accelerate the adaptation of commercial digital technology for defense applications.
5. Continue to strengthen the defense of the nation's digital infrastructure.
6. Pursue a strong and renewed commitment to technology collaboration with our allies.
7. Lead with moral authority and not the strength of technology alone.

All this is described in greater detail below.

1. FOCUS ON WHERE DIGITAL TECHNOLOGY IS GOING AND WHERE ADVANTAGE WILL LIE.

Almost all the digital technology we rely on today was made possible because of Gordon Moore's simple rule: processing speeds of silicon chips double every two years. For more than a half century, this principle has defined the explosive advancement of hardware, software, and connectivity. While Moore's Law is reaching the physical limits of fabricated chips, computing will continue to advance at a rapid rate. Today's focus on algorithms, software, new materials, integration technologies, and even subatomic research will redefine computing. And while the computer revolution took root on American soil, it is now a worldwide endeavor with global powers, including China, competing and sometimes leading the race.

The rise of the cloud and the transition to distributed intelligence at the cloud and the edge.

Cloud services have become the lifeblood of most modern enterprises. They make large amounts of computational power and storage available without capital investments in hardware by the end user. This is reshaping military technology in the same way it is impacting every other field. DOD has embraced these trends through projects like the Joint Enterprise Defense Initiative ("JEDI").

JEDI lays the foundation for DOD to embrace a full array of transformative technologies. For the first time, DOD will be able to fully leverage billions of dollars of annual private sector investment in cloud security, reliability, infrastructure, and governance. It will replace investments in single-purpose systems that are out of date by the time they come into service, using instead a modern compute environment that evolves with changing technology. Investment in hybrid solutions will further enable these core capabilities to extend from the data center to the field with new devices that enable data insights and analysis in rugged environments with poor or no connection to the network.

As the cloud extends its reach beyond data centers to what has been coined the "intelligent edge," cloud computing is becoming geographically distributed through an ever-expanding Internet of Things (IoT). Whether in a home, vehicle, or factory, the edge is considered one of the last bastions of Moore's Law as embedded sensors and devices become more efficient and less expensive. By 2030, 50 billion IoT devices will reside on the edge of the world's computing network. Just two years from now, in 2023, International Data Corporation (IDC) projects that more than 50 percent of new enterprise IT infrastructure will be at the intelligent edge rather than corporate data centers, up from less than 10 percent in 2020. By 2024, the number of applications deployed in the cloud and at the edge will increase 800 percent. [1]

This means the future of computing for everything, including military applications, is about the combination of computing power in the cloud and at the edge, with robust connectivity between them. As Microsoft CEO Satya Nadella has noted,

[1] Macy Bayern, "IDC: Top 10 Worldwide IT Predictions for 2020," TechRepublic, October 29, 2019, *https://www.techrepublic.com/article/idc-top-10-worldwide-it-predictions-for-2020/*.

the acceleration of this type of "tech intensity" is essential for any institution to thrive going forward. One has to be both world class at adopting the latest digital technology and building its own proprietary digital technology. This is going to be true for our defense institutions as well. [2]

As the world's intelligent edge explodes, so will the amount of data gathered by the tiny sensors and devices located where the digital and physical worlds intersect. Paired with Artificial Intelligence (AI) and its use of Machine Learning (ML), edge devices will have the power to see, listen, reason, and predict real-world developments around them. Perhaps more importantly, new intelligent edge applications will be able to interact with their physical environments to perform increasingly complex tasks with increasing degrees of autonomy. And as intelligent devices at the edge proliferate, so too will the surface area for cyberattacks as the vulnerabilities of these soft access points are exploited.

This distributed paradigm will bridge the physical and digital worlds by enabling previously difficult or impossible scenarios, like digital twins and rich real-time analytics to support our military on the most remote battlefields. Microsoft and the U.S. Army have already moved forward on this digital frontier by working together on the Integrated Visual Augmentation System (IVAS), based on the HoloLens 2 augmented reality (AR) system. For example, before warfighters seek to rescue hostages in a building, they can plan their mission based on a digital twin of the building and train for the operation using the rapid construction of a physical mock-up of it. The same technology enables warfighters to execute the operation with real-time visual data that integrates everything from the building's digital layout to local thermal images to facial recognition of the hostages and the identification of friendly forces.

Connectivity—from broadband to 5G, Low-Earth Orbit Satellites, and beyond.

As the computing canvas stretches from the edge to the cloud, reliable connectivity will become essential to provide the bandwidth and speed needed to maximize smart and connected devices. Fifth-generation, or 5G, networks will deliver data flows 10 to 100 times faster than 4G and support many more devices. They will offer the precision and speed needed to realize the power of edge computing with immersive, real-time, and intelligent experiences, much like electricity powers the world today.

Countries that rapidly deploy 5G stand to gain in revenue, job creation, and leadership in technology innovation. As we have seen with other technology transformations, software will play an important role in advancing 5G to deliver new solutions that increase speed, reduce costs, and boost security. With 5G more so than previous generations of wireless technology, software—from signal processing to radio area networks to complex traffic management—is at least as critical as spectrum and radio frequency infrastructure.

There is a significant opportunity for both traditional leaders and new players across the industry to innovate, collaborate, and create new markets, serving the world's networking and edge computing needs and the coming software ecosystem that will depend on these technologies. As with previous technology ecosystems, global standards and interoperability in our networking and computing infrastructure across the edge and cloud will be critical to unlocking the full creativity and productivity of the scientists, engineers, entrepreneurs, and innovators who will help shape our future.

As nations look to overhaul their broadband infrastructure, governments are rightly focusing on the cyber risks associated with 5G's supply chain integrity where they currently rely exclusively on a handful of foreign suppliers. While some nations are breaking this dependency by adopting modularized software-defined systems, some are concerned that these systems create a broader and multidimensional vulnerability. 5G's inherently modular nature and use of software-defined networking, however, also create opportunities to increase security and resiliency. This can foster a more diverse supplier ecosystem and enable the application of leading-edge security techniques and technologies, such as AI and containerization to identify, isolate, contain, and protect against malicious attacks on the network.

But 5G is not the only connectivity technology that is advancing. Existing solutions like fiber, satellites, Wi-Fi, and short-range technologies continue to progress.

---

[2] Satya Nadella, "The Necessity of Tech Intensity in Today's Digital World," LinkedIn, January 18, 2019, *https://www.linkedin.com/pulse/necessity-tech-intensity-todays-digital-world-satya-nadella/;* see also Dr. Tianyi (TJ) Jiang, "#TechIntensity Explained: 4 Ways It Shifts Business Strategy Forever," *AvePoint Blog,* October 10, 2018, *https://www.avepoint.com/blog/office-365/tech-intensity-explained/#:~:text=%E2%80%9CTech%20intensity%E2%80%9D%20is%20a%20phrase%20coined%20by%20Microsoft,its%20ability%20to%20build%20its%20own%20digital%20capability.*

For example, we can leverage satellite broadband to connect modular data centers to bring high-intensity, secure cloud computing to some of the most challenging environments, where critical prerequisites like power, connectivity, and building infrastructure are unreliable. And well before we reach the year 2030, we'll be discussing 6G and how to extend the networks' global reach through thousands of Low-Earth Orbiting Satellites.

Software combined with the explosion of data and infused with AI.

For most of the 179 years since Lady Ada Lovelace wrote the first program for a computing device—Charles Babbage's Analytical Engine—software programming has required a skilled individual to translate a human's understanding of a problem to a program that instructs a machine how to solve it. AI, particularly with the stunning progress computer scientists and engineers have made in ML over the past two decades, has allowed us to think about harnessing computers in a fundamentally different way.

ML systems learn from data without being programmed. They can reason about complex phenomena in both the digital and physical world, understand these phenomena, and make predictions or draw inferences that can support human decision making or be employed in automated ways. Using ML techniques, we have built AI systems that can both see and understand what they are seeing. We have built speech recognition systems that can hear and understand what is being said. We have built systems that can seamlessly and in real time translate between spoken human languages. We have even built AI systems that have achieved superhuman performance on tasks we once thought were high watermarks of human cognition, like beating the best human players in the world at games like Chess and Go.

The power of machine learning systems is growing rapidly, both in terms of improved performance on existing ML tasks (like speech recognition, computer vision and machine translation), and perhaps more interestingly, on the rapid expansion of new tasks that ML systems can undertake.

AI and machine learning workloads that run side by side with more traditional, hand-coded software will continue to grow at an exponential rate, driven by developers utilizing new AI algorithms and customers' ambitions to incorporate AI into new tasks. According to IDC, by 2024, more than 50 percent of user interface interactions will use AI-enabled computer vision, speech, natural language processing (NLP), and augmented and virtual reality (AR/VR).[3] And by 2025, at least 90 percent of new enterprise applications will embed artificial intelligence.

Recent ML breakthroughs, particularly the family of methods jointly referred to as deep learning, have allowed ML systems to approach or exceed human capabilities on a wide range of tasks. These breakthroughs enable us to teach AI systems to accomplish a very broad range of cognitive tasks by training on unlabeled data, such as Wikipedia texts and YouTube videos. Given the extremely large volumes of unlabeled data available on the internet, as well as data that can be produced in simulation environments and will be coming in growing volumes from sensors on the intelligent edge, we increasingly are bound more by the amount of computing power than the amount of data that we can bring to bear to train ever-larger models. Researchers anticipate that this trend will continue to yield results even as models grow to be 100 to 1,000 times larger than they are today.

The need to train models this large has unleashed a new race to create "AI supercomputers," with a primary competitive race unfolding between Google, based in part on its acquisition of DeepMind, and Open AI, which works with a substantial investment from and in partnership with Microsoft. As this race has progressed, Google, Open AI, and Microsoft have achieved new landmark results in natural language processing with AI models that now have hundreds of billions of machine-learning parameters. It has also led to additional breakthroughs in computer vision, speech recognition, content understanding and recommendations, and other areas of machine learning.

The implications for defense applications are expanding rapidly. For example, Microsoft is leveraging commercial AI technology to accelerate innovation for DOD through the creation of computer-generated, three-dimensional models of objects and environments. Until recently, Pentagon planning often was constrained by the availability of imagery from the theater of operations. Leveraging technology developed by our Xbox team, we combine gaming and rendering technology developed for consumer markets over the last 20 years to build lifelike models depicting objects in any environment, at any time of day, in any weather condition, and from any angle

[3] International Data Corporation, "IDC FutureScape Outlines the Impact 'Digital Supremacy' Will Have on Enterprise Transformation and the IT Industry," October 29, 2019, *https://www.idc.com/getdoc.jsp?containerId=prUS45613519.*

or perspective. (This technology is also being used in civilian scenarios to train Unmanned Aerial Vehicles to recognize the state of crops to enhance productivity for farming.) DOD can use these models to train personnel and plan operations.

Semiconductor Chips—from faster processing speeds to a quantum future.

While the first generation of AI supercomputers are being built with today's most powerful semiconductor chips and networks, the building blocks for these systems were not originally designed to support AI at scale. The next generation of AI supercomputers will require a surge in innovation in silicon, computer architecture, memory, and networking technology. Tomorrow's AI supercomputers will need to be orders of magnitude more powerful than the most powerful machines in existence today to meet the nearly unbounded demand for compute from modern AI programs.

As our need for compute continues to expand, the physical limitations of silicon are becoming apparent, spurring research and development on materials with enhanced capabilities to support new forms of computation, including quantum computing. Classical computers powered by silicon think in terms of binary bits of ones and zeroes. Quantum computers, by contrast, harness modern physics and the quantum mechanical behavior of nature to perform a computation using quantum bits—or qubits—the quantum version of a classic binary bit that represents multiple values simultaneously.

The promise of quantum computers lies in their ability to solve problems requiring "big compute"—challenges in cryptanalysis, chemistry, and materials science—in months, weeks, or days, where current and even the next generations of silicon-based chips and networks would still take billions of years. Once scaled up, quantum computing could lead to rapid advances across society and industry, including identifying an efficient catalyst to reduce carbon dioxide in the atmosphere and materials that could enable lossless power transmission or better battery technologies.

Unlocking the full potential of quantum computing will require more than simply building quantum computers, however. Quantum applications will require advanced classical computers working in conjunction with quantum computers. These applications on an industrial scale will require advances in semiconductor chips, cloud infrastructure, network connectivity, and more.

It is important to both national security and the American economy to secure a domestic quantum future. The National Quantum Initiative Act signed in 2018 was a critical first step. It bolstered the nation's leadership by investing in quantum research and development by government, industry, and academia. Industrial-scale quantum computing will require even more, including a physical infrastructure to support the quantum supply chain that encompasses manufacturing, materials development, system-level validation and verification, and nanoscale fabrication.

Looking to the future, Congress should consider funding a quantum equivalent of Operation Warp Speed. The U.S. Government could seek to combine federal resources with private sector capital and expertise. Federal funding could come in the form of milestone-based pre-payments for access to the capabilities that firms are developing, direct funding for scalable quantum solutions, and other means of accelerating and de-risking quantum efforts. Congress should also consider ways to increase cooperation and knowledge sharing between government quantum researchers and their private sector counterparts.

The conceptual threads that tie American technology together.

The foregoing areas reflect an enormous range of scientific and technological advances. Yet two conceptual threads run throughout all these critical fields. First, advances and adoption of technology at a global level require more than world-class technology itself. They also turn on the ability to persuade other governments and international markets to adopt standards and endorse technology protocols that reflect American inventions. The United States has excelled in these fields through decades of international collaboration and outreach. It will need to continue to do so for decades into the future.

Second, and perhaps more important, all these innovative technologies require and run on trust. As digital technology becomes an ever more ubiquitous part of our lives, it has increasingly profound impacts on our privacy, safety, security, and other fundamental freedoms. This too has deep implications for American leadership and values. Global technology competition is not only about the latest technical invention. It is also about products that reflect values the world can trust.

2. STRENGTHEN THE NATION'S TECHNOLOGY LEADERSHIP BY INVESTING IN TALENT AND RESEARCH.

National policy for digital defense technology also needs to be grounded in a clear-eyed assessment of the state of global technology markets and the nature of global technology competition. There are two factors that deserve special attention.

American digital defense technology increasingly starts with the development of commercial technology and then moves to military and intelligence adaptations, rather than the other way around.

Since the 1800s, military technology has fallen into two categories. The first is illustrated by the jeep, a classic example of commercial technology that the military adapted for use in World War II. Henry Ford debuted the Model T in 1908 as the world's most practical and inexpensive automobile. Ford and other American automakers improved on this design for decades. In 1940, the U.S. Army recognized that the approaching war would require a new and inexpensive four-wheel drive motor vehicle. It turned to the nation's manufacturers, who adapted off-the-shelf automotive parts and designed the first prototype in just two days.

The other category is technology that is invented first for military use and subsequently adapted for commercial applications. A good example is the jet aircraft. America's first jet plane was the Bell P–59 Airacomet, also created during World War II. It was designed in secret and its invention wasn't shared with the public until 1943, after it had completed 100 flights. It would take 15 additional years before the jet engine would be attached to civilian aircraft and transform the world of commercial aviation.

The Cold War and the race to the moon were won principally by technology developed first for the government and later put to commercial use. But today the sequence often is reversed. Developing digital defense technology is often more like designing jeeps than inventing jets. This phenomenon, in turn, creates a need for American leadership in two areas—world-leading technology research and development capability in both the governmental and private sectors and the ability to quickly adapt civilian technology for military use.

The country must continue to refresh its capacity for digital innovation by investing in talent and research.

The United States is the world's technology leader today because of decades of investment in education and research. When the nation confronted the Sputnik launch by the Soviet Union in 1957, President Eisenhower and a bipartisan Congress recognized that sustained national progress required not just federal investment in a new generation of rockets, but in stronger math and science education for a new generation of people.[4] Just 11 months after Sputnik's launch, Eisenhower signed the National Defense Education Act (NDEA) into law, saying "this emergency program stems from national need, and its fruits will bear directly on national security."[5]

Federal investment in education and basic research created a powerful infrastructure for innovation, but like our roads and bridges, that infrastructure is showing its age. Last month, the National Security Commission on Artificial Intelligence (NSCAI), chaired by my co-panelist Eric Schmidt, said in its Draft Final Report that "the time is right for a second NDEA, one that mirrors the first legislation, but with important distinctions."[6] This frames the issue well and rightly sets a high bar for the bold ambition the country needs to refresh its innovation infrastructure. A new federal initiative should include the following elements, among others:

- *Expand support for STEM education.* Today, less than a third of American high schools offers an advanced placement course in computer science.[7] The number of young people taking such a course in 2020 was lower than for eleven other subjects. One challenge is the high cost of training teachers to teach computer science. Philanthropic groups such as code.org and tech companies such as Microsoft, Google, and Amazon have all launched important initiatives to help

[4] Wayne Urban, *More than Science and Sputnik: The National Defense Education Act of 1958* (Tuscaloosa: University of Alabama Press, 2010); Yanek Mieczowski, *Eisenhower's Sputnik Moment: The Race for Space and World Prestige* (Ithaca, NY: Cornell University Press, 2013).

[5] Dana Adrienne Ponte, *The First Line of Defense: Higher Education in Wartime and the Development of National Defense Education, 1939–1959* (Seattle: University of Washington Unpublished PhD Dissertation, 2016), 89.

[6] National Security Commission on Artificial Intelligence, *Draft Final Report,* January, 2021, 82, *https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Draft-Final-Report-1.19.21.pdf.*

[7] College Board, "AP Program Participation and Performance Data 2020," *https://secure-media.collegeboard.org/digitalServices/pdf/research/2020/Program-Summary-Report-2020.pdf.*

address this need, but more federal leadership and funding is needed, especially to support teacher training.

- *Invest in post-secondary education for critical disciplines.* Federal support under the NDEA targeted disciplines such as math and science (and especially physics) that Congress believed would be critical to winning the space race. A similar effort is needed today, and it should start by cataloguing the fields where there is a current or expected shortage of skilled personnel in the United States. This should address the need for a compute-savvy workforce skilled in key areas like AI, quantum, and cybersecurity. Like the NDEA itself, this effort should include a focus on career and technical education, leveraging the nation's community colleges and vocational schools as well as four-year colleges and graduate degree programs.
- *Modernize immigration laws to address technology needs.* The country's last major immigration overhaul took place in 1986, when Ronald Reagan was President and Tip O'Neil was Speaker of the House. It was closer in time to Sputnik's launch in 1957 than the technology challenges of 2021. The NSCAI's Draft Final Report captures well the types of immigration changes that are needed to ensure the United States attracts the best and brightest talent needed to advance technology's frontier. These include broadening the visa category for extraordinary talent, enabling better job portability for highly skilled visa holders, and enacting measures to clear the current green card backlog and provide a more stable path to green cards in the future.[8] In addition, we should not forget that the Nation's Dreamers include a substantial number of extraordinarily talented individuals with advanced technology skills, something we witness every day among DACA registrants who are Microsoft employees.
- *Increase federal support for basic research related to critical technologies.* The United States retains an unmatched capability for basic research through the country's research universities. Yet United States Government spending on research and development and our share of global spending have dramatically declined,[9] and within the next few years China is expected to surpass us.[10] As in the past, the country needs to bolster our research capability for the next generation of technology needs, including AI, quantum computing, and other critical technologies. Here too, the NSCAI gets it right in its Draft Final Report, recommending an increase in AI R&D at compounding levels, doubling annually to reach $32 billion per year by fiscal year 2026.[11]
- *Support DOD efforts to recruit tech talent and develop digital skills among DOD personnel.* Finally, the decade ahead will require that every American employer, including the nation's military, do more to invest in digital skills for its own personnel. While the country's employers increased their investments in digital skilling between 1980 and 2000, these investments have fallen and then stagnated since the year 2000.[12] Part of what is needed for the future will involve heightened DOD recruiting of tech talent. Virtually every job, including virtually every position in our military, will require more digital skills a decade from now that it does today. And conversely, as servicemembers exit the military, we need to support them to move into technology-enabled roles so their national security experience can help drive private sector applications and innovation. A successful example of a public-private partnership in this area is the Microsoft Software and Services Academy (MSSA).[13] It has enabled thousands of service members, veterans, and spouses to secure technology jobs with more than 600 employers across the country.

---

[8] National Security Commission on Artificial Intelligence, *Draft Final Report, 82–86.*

[9] Congressional Research Service, *The Global Research and Development Landscape and Implications for the Department of Defense,* November 8, 2018, *https://crsreports.congress.gov/product/pdf/R/R45403.*

[10] Paul Scharre and Ainikki Rikkonen, *Defense Technology Strategy,* Center for a New American Security, November 2020, CNAS—Defense Technology Strategy (s3.us-east-1.amazonaws.com)

[11] *NSCAI Draft Final Report, 90.*

[12] Brad Smith, "Microsoft Launches Initiative To Help 25 Million People Worldwide Acquire the Digital Skills Needed in a COVID–19 Economy," *Microsoft on the Issues* (blog), June 30, 2020, *https://blogs.microsoft.com/blog/2020/06/30/microsoft-launches-initiative-to-help-25-million-people-worldwide-acquire-the-digital-skills-needed-in-a-covid-19-economy/.*

[13] Microsoft Corporation, "Microsoft Software and Services Academy", *https://military.microsoft.com/programs/microsoft-software-systems-academy/.*

3. ENHANCE AMERICAN COMPETITIVENESS AND SECURITY BY MODERNIZING TECHNOLOGY-RELATED TRADE AND INVESTMENT POLICY.

The United States has been a global leader in digital technology since the field's inception, but this leadership will be more challenging to maintain in the decade ahead. While this conversation often begins by comparing the tech sectors in the United States and China, it is helpful to start by identifying the factors that influence this competition more broadly.

American success in the development of commercial technology typically requires success on a broad international scale.

This is true for three reasons. First, digital technology often involves high fixed costs and low marginal costs. The fixed costs are for engineering involved in software development and capital costs such as the construction of chip fabrication or data center facilities. To charge low prices and gain market share, companies must spread these high fixed costs across a large customer base that can only come from growth in foreign markets.

Two other factors are at work as well. Most technology markets have strong network effects, which enable strong returns to scale once a company has established market leadership. And finally, services that are dependent on large quantities of data for product improvement, including through ML, are likely to gain an additional advantage by being the first to reach a market leading position. All this explains why LinkedIn founder and Microsoft board member Reid Hoffman talks about the critical need in tech markets for blitzscaling, meaning a "lightning-fast path" to develop market leadership on a global scale. [14]

This has implications for competition between the American and Chinese commercial technology sectors. With a population of 1.4 billion people, China is in a unique position to develop technology markets at an unmatched domestic scale. The rapid growth of ByteDance's TikTok service illustrates this well. As of last year, the company's service inside China, named Douyin, had 600 million daily active users, while its international TikTok counterpart had another 689 million monthly active users, giving it almost 1.3 billion users worldwide. [15] This same phenomenon is at work for Chinese companies that are marketing technological platforms to global consumers in areas such as healthcare, finance, and education.

At the same time, American technology firms do not have full access to China's domestic technology market. This makes it even more important that American companies succeed quickly not only in the United States, but in many other international markets as well.

The United States currently has a patchwork of technology-related trade and investment laws rather than a holistic, cohesive, and strategic regulatory approach.

Last summer Microsoft had not just a front row seat but a direct participatory role in some aspects of the TikTok review. One thing we came to appreciate is the difficulty for government officials and private sector participants alike when making decisions about specific technologies in the absence of a clearer overall legal framework to guide technology-related trade and investment activities. The United States' current patchwork of laws in these areas not only lacks strategic coherence but also reduces predictability for everyone it affects.

On the *export front,* Congress in 2018 enacted the Export Control Reform Act (ECRA), the most sweeping piece of export control legislation since the 1970s. While this legislation directed the Commerce Department's Bureau of Industry and Security (BIS) to adopt new regulations, the process for doing this—still ongoing—is creating substantial uncertainty for the tech sector. This is a critical and ongoing issue for almost every large technology company in the United States, as firms seek to balance these compliance obligations with the demands of a global market that wants more American products ever faster—and where missing a single product cycle can make it very difficult to catch up.

On the *import front,* United States policy has moved rapidly to restrict technology investments and imports from China. This has its roots in the Committee on Foreign Investment in the United States (CFIUS), established in the 1970s. Congress expanded CFIUS's jurisdiction in 2018 through the Foreign Investment Risk Review Modernization Act (FIRRMA), which authorizes the Committee's review of non-controlling foreign investments. The National Defense Authorization Act for Fiscal Year 2019 requires federal contractors to ban certain telecommunications technologies

---

[14] Reid Hoffman and Chris Yeh, *Blitzscaling: The Lightning-Fast Path to Building Massively Valuable Businesses* (New York: Currency, 2018).

[15] Brian Dean, "TikTok Demographics Statistics: How Many People Use TikTok in 2021?", Backlinko, November 4, 2020, *https://backlinko.com/tiktok-users.*

from their supply chains. The last Administration also relied on the International Emergency Economic Powers Act (IEEPA) to broadly authorize Commerce's review of technology transactions and ban certain mobile applications.

In recent years, the government has relied on this complex set of laws to address several technology-related concerns. Some of these efforts have focused on specific companies and the technologies they provide. Others have involved broad categories of information and communications technologies. For example, the State Department in recent years encouraged other countries to adopt more restrictive policies in these areas through its "Clean Network" initiative.

It is worth recognizing that China's policies in this area reflect a similar desire to manage technology trade. China has long had a restrictive legal regime to manage technology imports and investments. This combines the filtering of foreign content with an array of domestic licensing requirements, joint venture obligations, and informal government signaling regarding the purchase of foreign technology. Last August, the Chinese Government adopted new rules to control technology exports as well. These measures substantially broaden controlled categories, now including social media algorithms and other new categories. These changes were followed by a new export control law that went into effect in December, representing China's most significant effort to date to implement a comprehensive "dual-use" export control regime.

As we look to the decade ahead, it is apparent that both the United States and China will want to scrutinize and restrict trade in dual use technologies. And with an increasing focus on digital sovereignty, the European Union and some member states are moving in a similar direction.

Given the stakes and uncertainty, the urge to err on the side of caution by adopting ever more restrictive policies in this space is understandable. But that approach could weaken national security by undermining American technology leadership. We need a balanced and coherent framework that will protect national security without isolating the United States. And as we consider issues related to China in particular, we should develop an approach to technology-related trade and investment that permits cooperation when it is clearly in the interest of American technology leadership. As modern as China may be today, the country still depends on American technology and standards. To pull away from that position and accelerate China's adoption of its own, competing approaches risks jeopardizing American leadership in critical areas.

The country needs to modernize its technology trade and investment policies.

- *The Commerce Department should identify the commercial technology exports it wants to control and adopt a modern, calibrated approach to control them.* A high priority for the Commerce Department should be the adoption of new regulations on "emerging and foundational technologies" under ECRA. As many companies across the tech sector noted last year, applying a traditional, restrictive export control approach based solely on a product's performance criteria not only risks limiting societally beneficial uses, but could hinder the development of new technologies by depriving companies of the scale necessary to compete internationally. Overly restrictive export controls also risk cutting off access to the best talent—not just from the country targeted for control, but also from allies and other like-minded nations.

A new and more calibrated approach is needed. Microsoft and Open AI proposed one in comments submitted to Commerce in November. Under this proposal, the Commerce Department would set policies that determine who can access sensitive technologies and for what purpose.[16] This would allow for protection against problematic users and uses in a more targeted, effective, and dynamic way—not just at the point of initial access but continuously in a deployed environment. These policies would then be implemented and enforced within the protected technology itself, as well as by hardening the infrastructure around it to prevent circumvention.

New technologies make this approach feasible. For example, software features built into sensitive technologies can enable real-time controls against prohibited uses and users. These features would include identity verification systems and information flow controls. "Tagging" can be used to ensure the same controls apply to derivatives of these sensitive technologies.

Similarly, "roots of trust" built into sensitive hardware technologies can require authorization to send code or data through the equipment. More robust hardware identity verification through secure co-processors akin to those used to secure pay-

[16] Sarah O'Hare O'Neal, "Microsoft and OpenAI Partner to Propose Digital Transformation of Export Controls," Microsoft on the Issues (blog), November 10, 2020, *https://blogs.microsoft.com/on-the-issues/2020/11/10/openai-partnership-digital-export-controls/*.

ment in mobile phones or to prohibit in-game cheating in game consoles can further protect hardware against unauthorized access and uses.

Technology may not eliminate the need for restrictive export controls in every particularly sensitive scenario. But in many areas, more targeted, technology-enabled solutions could help strike an optimal balance between security and the need for the American technology sector to remain globally competitive.

- *The government should ensure there exists an independent supply chain for both existing and certain anticipated critical technologies.* To address this challenge, at least two key questions await urgent answers.

First, the country must decide what technologies should be provided exclusively from domestic sources or from allied nations. The key criteria likely should focus both on the sensitivity of the technology and the danger of supply disruption in the event of international tensions. For example, the United States currently cannot source critical 5G technologies in a cost-effective way either domestically or from allies. It is impossible to imagine our potential adversaries being comfortable relying exclusively on American suppliers for these same technologies. The United States shouldn't think about these issues any differently.

Second, the United States must decide how to achieve supply chain independence in the selected technologies in a strategic, effective, and cost-efficient way. Some key tenets should guide this work. First, the government should take stock of market trends and build upon them, providing public financial support only where it is needed and in a manner that will accelerate sustainable development by the market itself. Second, the government should use the full range of its policy tools to accelerate essential market trends, including its procurement practices and the broad role in the economy of agencies such as the DOD. And finally, the government should ensure there is reciprocal trade access to the American market for suppliers from NATO and other allied democratic countries, based on common terms for American access to these other markets.

- The United States should modernize its broader technology import and foreign investment policies. This goes beyond the question of where the country wants to have an independent source of supply. Instead, it asks the government to decide where the presence of certain foreign technologies and investment poses a threat to the country's national security.

The challenge of managing technology imports is more daunting than for exports, in part because there has been no legislation in recent years akin to ECRA. While IEEPA is a powerful policy tool, it was developed in a different era and for different circumstances from those that exist today. On the investment front, Congress recently updated CFIUS. But the United States still lacks a coherent framework governing the related issues of technology imports and foreign investment in U.S. technology companies. There are several critical questions that require an answer.

First, the government must decide which technologies are so sensitive that imports or foreign ownership need to be controlled. It should then adopt consistent policies to manage both imports of and foreign investments in these technologies. The technology horizon will continue to evolve rapidly, and the government therefore will need criteria that stands the test of time. In part this should include digital infrastructure that would be susceptible to penetration or disruption in times of war.

Second, once these sensitive technologies have been identified, the government must decide how it wants to control them. While one approach would be to bar sensitive technologies or investment from certain countries entirely, this is not always the best or the only feasible approach. For example, Microsoft has long operated by creating transparency centers that enable appropriate inspection of source code for a product like Windows. Similarly, we developed last year and shared with United States officials what we regarded as a sophisticated and effective technology model to manage consumer services from China by addressing five key objectives—security, privacy, authenticity, digital safety, and transparency.

It is likely that global trade in key sectors increasingly will rely on these types of technology-enabled solutions. The United States should become an early adopter so that it can lead and shape the development of these solutions internationally.

Finally, just as the government must determine where to restrict technology trade, it should also identify certain areas where it is safe for technology to move freely across borders. The good news is that many technologies are not sensitive from a national or economic security perspective. Even more important, in an era of open-source code and broad-based basic research, human knowledge advances daily based on global collaboration. The United States should aspire to lead the world in advancing the frontiers of scientific understanding and spreading appreciation of humanitarian values. We need government policies that protect the country's

national security without cutting ourselves off from the global conversations that will shape humanity's future.

4. ACCELERATE THE ADAPTATION OF COMMERCIAL DIGITAL TECHNOLOGY FOR DEFENSE APPLICATIONS.

The biggest competitive challenge the United States confronts in competition with China is not in technology research and development. Instead, it is the advantage China has over the United States in faster *deployment and adoption* of new technologies, particularly in AI. There are multiple reasons for this, including China's centralized government direction, and to some degree, broad adoption of technologies in ways that Americans rightly find objectionable. But one unmistakable result is the need to encourage faster and broader deployment and adoption of emerging technologies in the United States in a manner consistent with democratic principles and American values. This includes more rapid adoption of emerging digital technologies by DOD, most importantly to ensure American military supremacy but also to help accelerate technology adoption more broadly.

Our national security will be best served through a three-pronged effort by the government to utilize digital technology. First, the government should *use* commercially available technology when it is sufficient for the task and as the foundation for additional development when more work is needed. This will both accelerate speed and reduce costs. Second, the government should *add* security layers to commercial technology when required, such as by protecting secret and top-secret workloads and military operations. Third, the government should *adapt* commercial products and development methods for military uses and applications, including through additional product development of the sort illustrated by the IVAS.

All these efforts should be guided by three goals, among others—speed, cost, and innovation. As discussed further below, there is an opportunity to build upon recent procurement reforms with additional, practical steps that advance these goals. As much as anything else, we need to build a foundation for rapid and creative co-development efforts that breaks down barriers between engineers in the private sector and the warfighters whose missions depend on effectively using the world's most advanced technology.

This Committee has pursued critical and impactful work in recent decades to reform DOD procurement. Much of this work has focused rightfully on the shift from the hardware-centric weapons systems of the post-World War II and Cold War eras to the digitally enhanced technologies of the 21st Century. Despite this progress, there remain important inefficiencies that collectively impede DOD's ability to rapidly adopt digital technology. From incentives that reward process over speed to protests that undervalue the urgency of deploying the newest innovations, the Pentagon is still not where it needs to be. DOD should adopt approaches that will:

- *Incentivize and train the acquisition workforce.* In the private sector, we see risk-taking, failure, and iteration as a natural part of the innovation process. The DOD acquisition workforce, on the other hand, is more heavily incentivized to be risk averse. This should change. DOD should recruit, train, and retain the tech talent needed to develop, test, integrate, and deploy new technologies. It should reward this professional procurement corps for agility, speed, smart risk-taking, and accountability.

  This Committee was instrumental in passing the Other Transaction and Middle Tier Acquisitions authority and procedures designed to dramatically speed up the adaptation of commercial technologies for defense use. The IVAS program is a case study in this innovation.

  Nonetheless, we see added opportunity for the Pentagon to take full advantage of the tools this Committee has given it. There are still days when parts of the Pentagon find comfort in the rigidity of the Federal Acquisition Regulation (FAR) over the speed and flexibility of these newer tools. Even when new procurement channels are used, the process is sometimes managed in ways that resemble the more restrictive and slower processes the new channels were designed to replace. The future mission-critical capabilities needed for battlefield superiority will require that those responsible for requirements, acquisition, and technology deployment all work together faster, more closely, and seamlessly—and in conjunction with private sector innovators.
- *Create an Innovation Infrastructure.* A recent report by the Center for a New American Security[17] found that the Pentagon lacks a robust digital infrastruc-

[17] Michèle Flournoy and Gabrielle Chefitz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration, Center* for a New American Security, July 13, 2020, *https://*

ture to support modern warfighting. Building this infrastructure will require additional investments in cloud computing, data labeling and storage, and the human capital needed to fully utilize and manage these tools.

The 2018 DOD cloud strategy[18] noted that "the DOD information environment is made up of multiple disjointed and stove-piped systems distributed across modern and legacy infrastructure around the globe." A more unified general purpose cloud environment is a key prerequisite for breaking down these barriers and speeding up the adoption and development of transformative technologies.

- *Review and reform the government contract protest process.* The government contract protest process needs to be reformed to strike a better balance between fairness and open competition, on the one hand, and the urgency of innovation on the other. The existing, outdated process often leads to uncertainty, extended delays, and protracted litigation, hindering the speed of innovation and often maintaining the status quo. When considering acquisition reforms, Congress should look at ways to modernize, streamline, and accelerate protest actions. These should include time limits, not only on the filing of protests but on case resolution and corrective actions. Concluding bid protests more quickly will help provide our warfighters the technology they need when they need it.

5. CONTINUE TO STRENGTHEN THE DEFENSE OF THE NATION'S DIGITAL INFRASTRUCTURE.

For two centuries, technology has been changing the nature of what is needed to defend a nation. The first two years of the 1940s illustrate this well. In early 1940, the tank rendered worthless two decades of French investment in the Maginot Line, as it was suddenly possible for an Army to go around it. And in late 1941, the United States learned that advances in naval aviation meant that battleships could no longer defend Pearl Harbor. If not defended against effectively, foreign cyberweapons pose a similar threat of comparable severity in our current day.

Nature's recent impact in Texas demonstrates the potential devastation that would result if a foreign adversary used cyberweapons to take down a nation's electrical grid. Yet it has been apparent since 2014 that Russian agencies have been targeting the United States electrical grid.[19] And in 2017 the citizens of Ukraine experienced an even broader cyberattack that was launched by disrupting the software supply chain, in that case through malware implanted in an update for local accounting software. As one author has noted, "in the cyber world, what happens in Kiev almost never stays in Kiev."[20] The recent malware attack on SolarWinds demonstrates the truth of at least part of this proposition.

These issues also reach our democratic infrastructure, connecting national needs that are as old as our Republic with the most modern technology of the 21st Century. As George Washington recognized in his Farewell Address, democratic societies depend on a unique combination of free expression and social cohesion that must be protected from foreign interference.[21] Yet recent years have seen Russian successes in turning American social media into a Weapon of Mass Confusion, illustrated by the 2016 success of the Internet Research Agency in St. Petersburg in organizing a synchronized protest and counterprotest in Houston.[22] The nation's digital defenses today must include stronger measures to protect against disinformation campaigns, the misuse of personal information, and the voting process itself.

The DOD and other parts of the U.S. Government have made rapid progress in addressing many of these issues in recent years, but there remain several new and additional priorities that should be addressed, including:

- *Strengthen supply chain security for the private and public sectors for both software and hardware.* The public sector at all levels of government should strengthen the protection of their software, including through secure develop-

---

www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration.

[18] Department of Defense, *DOD Cloud Strategy,* December 2018, *https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD–CLOUD–STRATEGY.PDF.*

[19] David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), 163–68.

[20] *Ibid.,* 163.

[21] George Washington, "Washington's Farewell Address of 1796," Avalon Project, Lillian Goldman Law Library, Yale Law School, *https://avalon.law.yale.edu/18th—century/washing.asp.*

[22] Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press, 2019), 96.

ment practices, better software maintenance and vulnerability management, and integrity controls that apply throughout the software development, testing, and delivery processes. The implementation of this year's National Defense Authorization Act provides an opportunity to develop new software acquisition security requirements that may be appropriate across federal agencies.

- *Broaden use of cybersecurity best practices, including through improved cyber hygiene and a commitment to IT modernization.* The public sector in the United States needs to continue to modernize its technology base, in part through cloud migration that can better ensure ongoing state-of-the-art software code and improved threat detection. This should be coupled with the broader adoption of strong security practices such as the establishment of a Zero Trust environment, assessments of the security of cloud providers, and the re-orientation of risk management activities to complement third party services and security automation.
- *Develop a national strategy to strengthen the sharing of threat intelligence across the entire security community, including through a clear, consistent disclosure obligation on the private sector.* Much as radar advances proved indispensable in helping to defend against air attacks in World War II, modern threat intelligence can help defend against cyberattacks today. But only if threat intelligence is shared quickly and effectively. There is a critical need to improve the sharing of threat intelligence across the Federal Government, with key American allies, and in an appropriate but collaborative way with tech companies that often are cybersecurity first responders. This also requires consideration of new measures to ensure that attacks on private enterprises are reported in an appropriate way to a federal agency, consistent with the protection of personal privacy.

6. PURSUE A STRONG AND RENEWED COMMITMENT TO TECHNOLOGY COLLABORATION WITH OUR ALLIES.

The United States cannot secure its digital defenses by acting alone. One of the country's greatest strategic advantages is its global network of allies and partners. In part this is because of the global nature of technology innovation and markets. Microsoft's quantum computing efforts illustrate this well, with cutting-edge labs in Indiana, California, and Washington, as well as in Denmark, the Netherlands, and Australia.

Moreover, as noted above, one of the key drivers of successful development and deployment of technology is scale. The larger the potential market for U.S. technologies, the larger the pool of private and human capital that will be dedicated to the research and development efforts needed to maintain America's competitive edge. Scale plays a major role in AI development, in particular. AI runs on data. That means that China, with a population of 1.4 billion, has a comparative advantage when it comes to mustering sheer quantities of personal data. But the combined populations of the United States, our NATO and Five Eyes allies, Japan, and Korea, total over 1.1 billion. If Mexico, India, and Brazil are added, the combined population of this potential coalition of democracies would be close to 2.9 billion.

The United States should work with its global network of alliances and partners to:

- *Invest in and build coalitions with like-minded partners to develop, adapt, and deploy new technologies.* In part this should include selected basic research programs, like those discussed above, to bring together NATO members, the Five Eyes, and other democratic allies. It should also include efforts to align our technology trade policies and laws, as discussed above, with those of our allies.
- *Address privacy issues that undermine trust across the Atlantic.* There is a pressing need to address a short list of high priority privacy concerns, starting with improvements to the U.S.-E.U. Privacy Shield. These efforts should build a foundation for more durable global solutions to address issues around government access to data and should include international agreements under the CLOUD Act with the European Union and other American allies.
- *Pursue an ambitious digital and technology trade agenda.* The United States should build on the landmark digital trade rules in USMCA by upgrading other free trade agreements to include rules on data localization, cross-border data flows, and forced disclosure of proprietary source code and algorithms. At the same time, the country should continue to push for high-standard outcomes in the ongoing WTO digital trade negotiations. It should also explore the possibility of an even more ambitious plurilateral digital trade pact with like-minded countries and seek cooperation on standards for a range of emerging technologies.

- *Advance strong norms for global cybersecurity protection.* The United States should embrace international standards such as the Paris Call for Trust and Security in Cyberspace, already endorsed by more than 75 governments and more than 1,000 other signatories. It should similarly advance norms for the cybersecurity protection of software supply chains in the United Nations and elsewhere.

7. LEAD WITH MORAL AUTHORITY AND NOT THE STRENGTH OF TECHNOLOGY ALONE.

Finally, while the United States will remain a preeminent economic power for the foreseeable future, we must recognize that the nation no longer retains one of the strategic advantages it enjoyed for much of the 20th century, namely an economy that was orders of magnitude larger than its principal rivals. In addition, the country must grapple with one of the biggest challenges confronting the nation's defense—the need to preserve bipartisan and broad support for our national security policy in an era defined by a polarized public and a divided world.

Yet the country retains an enormous strength and strategic advantage. When the United States stands firmly for its historic democratic principles and the protection of human rights, it speaks and acts with a moral authority that none of its adversaries can match. There are few institutions that reflect and embody this strong ethical tradition better than the United States military. It is an asset that provides a strong cornerstone for future national and global leadership, and the country needs to nurture and build on it further.

As Microsoft and so many other tech companies experience every day, a new generation of Americans asks not only what will make their country strong but their society great. It is the type of question that should inspire us to be bold in our ambitions. As we've found, it is critical to talk with our employees about the American military's strong ethical traditions. When we do this and share our commitment as a company to provide the U.S. military with the best technology we create and simultaneously use our voice to advance ethics for AI, almost uniformly our employees do not object. They applaud. Literally. It is this type of appreciation that enables a company like Microsoft to recruit top tech talent internally and externally for an "all-volunteer" and "all-star" team for a project like IVAS. This type of understanding also helps to strengthen America's technology leadership through the active engagement and support of this country's technology talent, as well as people who are not American by birth or citizenship.

Continued leadership in technology will require that we meet the ongoing challenge to make sure American democratic principles and values are an integral part of developing and deploying the next generation of technology. This should include the following:

- *Continue to strengthen ethical practices and policies for DOD's use of AI and other new technologies.* DOD's adoption last year of ethical principles to govern the use of AI not only represented a critical step forward for the United States but also defined an ethical role model for the world. Building on the recommendations of the Defense Innovation Board, these principles sent a powerful message by stating that military personnel "will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities."[23] The DOD principles also addressed the importance of reliability, safety, transparency, and bias. The Joint Artificial Intelligence Center (JAIC) is already taking steps to implement these practices broadly. The NSCAI similarly has offered additional and important ideas to implement ethical AI principles throughout DOD and other agencies. The U.S. Government should continue this work and discuss it broadly with the American public.
- *DOD should encourage the adoption of similar ethical principles and practices by its allies.* The United States should exercise its moral authority by encouraging NATO and other allied nations to adopt similar ethical principles for their own militaries' use of artificial intelligence. The AI Partnership for Defense (AI PfD) announced last year between the United States and twelve allied nations can serve as a forum for these discussions. The government similarly should advance human rights norms and safeguards for new technologies, including the use of facial recognition and government access to personal information.
- *DOD should integrate environmental sustainability concerns into its policies and practices.* Finally, climate and energy issues are having and will continue to

[23] C. Todd Lopez, "*DOD Adopts 5 Principles of Artificial Intelligence Ethics,*" DOD News, February 15, 2020, *https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics.*

have major consequences on our national security. DOD has significant opportunities to substantially enhance resilience, reduce carbon emissions, and catalyze innovation though its own operations and supply chain. Many of these opportunities are enabled by digital transformation. Cloud computing tools not only can lead to significant operational energy and carbon efficiency gains, but also provide key information for security landscape assessments in countries around the world.

* * *

The challenges described above are formidable. But with concerted effort, appropriate investment, and strong leadership from members of this Committee and others, the United States can maintain its competitive edge in technology and secure the nation's defenses. I look forward to your questions and welcome the opportunity to discuss how Microsoft and other technology companies can assist in these efforts. Thank you.

Chairman REED. Thank you very much. General Carlisle, please.

STATEMENT OF GENERAL HERBERT J. CARLISLE, USAF (RET.), PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

General CARLISLE. Chairman Reed, distinguished members of the committee, thank you for this opportunity to share my experiences and industry perspective on emerging technologies to ensure that our nation continues to be the preeminent force in the 21st century. I would like to echo my colleagues' comments of we really appreciate the opportunity to spend time with you and give you our perspectives and help our nation move forward in this area.

The last time I testified was during my final tour in uniform, where I had the honor of leading Air Combat Command at Langley Air Force Base. In that role, I was responsible for organizing and training combat-ready forces. Before assuming command of ACC, I was the commander of Pacific Air Forces, responsible for all Air Force activities in about half of the globe.

During my 40 years of service, I witnessed firsthand numerous technological advances that focused on ensuring our warfighters operate with the best, most innovative equipment to ensure they are never in a fair fight. From my first flight in a T–37, a long, long, long time ago, to my final flight in a F–15, technological advances helped our forces go faster, farther, and safer with greater lethality. My role at the National Defense Industrial Association (NDIA) continues that mission, to work with you and your esteemed colleagues, the Pentagon, and the hundreds of thousands of members of industry who strive to imagine and create the best and most advanced equipment and capabilities to arm those young women and men that serve our nation today.

We are almost a quarter of the way into the 21st century and the character of war has changed somewhat. The threat to our nation's defense is not necessarily countering state and non-state actors in the domains, but it is looking at cyberspace and actual outer space, and how we defend in those areas. I think adversaries know they cannot outlast our American industrial might today, but they are making gains in changing the calculus every single day. Our competitors get stronger, unconstrained, frankly, by fiscal year budgets, and continuing resolutions are continuing to be a challenge. The 2018 National Defense Strategy identified 11 bipartisan modernization priorities, including hypersonics, microelectronics,

and directed energy. We all agree that these 11 priorities are the emerging technologies priorities.

We know our peer competitors are investing in these areas extensively, especially China. I have to say, I served in the Pacific Theater throughout my career. Much of my 40 years was in the Pacific, and as a squadron commander and in Pacific in the early '90s, China was essentially a third-world nation. We really did not consider them a legitimate threat at the time. As Pacific Air Force (PACAF) commander in the 2010s, they were not just a rising threat; they became, and are today, the pacing threat. China has made particular inroads in hypersonics by outspending us, outpacing us, and building on our work. China's ambitious plans in space have led them to make incredibly rapid advancements. They seek to build a microelectronics capability within their nation. Even now, they can very rapidly put state-of-the-art components into their equipment, while U.S. military systems, in some cases, are two generations behind. In some areas, like rare earths, we have already fallen behind and are dependent on others. In other areas, the question is no longer whether our adversaries will close the gap, but whether we will catch up.

Where our competitors can, they have stolen our technology, and where they cannot they have used predatory investments, directed investments, and compulsory cooperation between domestic and military in their countries. DOD needs to utilize all the tools they have and adjust a risk-averse culture. Fewer regulations, with more uniform enforcement, will ease the burden on companies and the Department and speed up the acquisition process. A workforce empowered and given authority to make decisions provides the opportunity to unleash innovative companies. This may lead to some failures in programs and some long terms, but DOD can take a page from the corporate world and learn from research and development (R&D) failures.

We need to encourage and expand new and innovative partnerships across government, industry, and academia to exploit the pace of innovation and rapidly scale transformational research and operational prototyping. We have several mechanisms with which to do this and field products quickly. We have small business innovation research (SBIR), we have Defense Advanced Research Project Agency (DARPA), Defense Innovation Unit (DIU), Space Development Agency, AFWERX, SOFWERX, and many more. They demonstrate daily they can bring nontraditional players into the defense industrial base in a timely manner.

We need to be nimble and thoughtful, encouraging the services to identify and support the transition of world class, disruptive technologies.

Ladies and gentlemen, we truly appreciate congressional support in helping DOD adopt an approach to accepting risk intelligently—it is taxpayer dollars and we have to be smart—taking a more collaborative approach across services to identify and deploy game-changing technology that allows the Department to maximize our limited resources. The men and women in uniform sacrifice daily to protect our nation, our freedoms, and our way of life. They deserve every protection that we can afford them, and the equipment,

capabilities, and training to do the missions this nation asks them to do.

Thank you again for the opportunity to be here today. Thank you, sir.

[The prepared statement of General Carlisle follows:]

PREPARED STATEMENT BY GENERAL HERBERT "HAWK" CARLISLE

INTRODUCTION

Chairman Reed, Senator Inhofe, and distinguished Members of the Committee thank you for the opportunity to share my experiences and industry perspective on emerging technologies so that we will ensure our nation continues to be the pre-eminent force for the 21st Century.

The last time I testified was during my final tour in uniform, where I had the honor of leading Air Combat Command (ACC). In that role, I was responsible for organizing, training, and equipping combat-ready forces for rapid deployment and employment while ensuring forces were ready to meet the challenges of peacetime air sovereignty and wartime defense. Before assuming command of ACC, I was the Commander of Pacific Air Forces, responsible for Air Force activities spanning more than half the globe.

During my 40 years of service, I witnessed firsthand numerous technological advances that focused on ensuring our warfighters operate with the best, most innovative equipment to ensure they are never in a fair fight. From my first flight in a T–37 to my final flight in a F–15, technological advances helped our forces go faster, farther, and safer with greater lethality. My role at the National Defense Industrial Association (NDIA) continues this mission—to work with you and your esteemed colleagues, the Pentagon, and the hundreds of thousands of members of industry who strive to imagine and create the best and most advanced equipment and capabilities to arm our men and women today, with an eye to what future engagements will require.

Almost a quarter of the way into the 21st Century, the character of war has changed. The threat to our nation's defense is not necessarily boots on the ground in far-off theaters; we're securing our networks and countering state and non-state actors in the domains of cyberspace and actual space. Adversaries know they cannot outlast American industrial might today. But they are making gains in changing this calculus. Our competitors get stronger every day—unconstrained by a fiscal year budget and without the concerns of possible continuing resolutions to inhibit their ability to innovate while placed in a budgetary holding pattern. The 2018 National Defense Strategy identified 11 bi-partisan modernization priorities, including hypersonics, microelectronics, and directed energy, which we agree are the right focus.

We know our peer competitors are investing in these areas as well, especially China. I served in the Pacific Theater throughout my uniformed service. As a squadron commander and in the 1990s, China was essentially a third-world nation we did not consider a genuine threat; as PACAF commander in the 2010's, they were not just a rising threat; they became the pacing threat. China has made particular inroads in hypersonics by out-spending us, out-pacing us, and building on our work. China's ambitious plans in space have led them to make incredibly rapid advancements. They are also investing heavily in AI and biotechnology. They seek to build a domestic microelectronics capability, but even now, they can put state-of-the-art components in their systems, while US military systems are two generations behind. In some areas, like rare earths, we have already fallen behind and are dependent on others. In these areas, the question is no longer whether our adversaries will close the gap, but whether we will catch up to our competitors.

Where our competitors can, they've stolen our technology, and where they can't, they've used predatory investments, massive directed investments, and compulsory cooperation from domestic industry through military-civil fusion. Combating these predatory economics requires a whole of nation approach to both protect and promote American industry to support our warfighters. From a defense industrial policy perspective, this includes identifying ways to efficiently and effectively deliver from research and development to acquisition, from commercial as well as traditional defense firms, to pull forward and not leave this technology to solely the commercial market or sitting on the shelf. DOD needs to utilize the authorities they have and adjust a risk-averse culture. Fewer regulations, with more uniform enforcement, will ease the burden on companies and the agency and speed up the acquisition process. A workforce empowered and given authority to make decisions

provides the opportunity to unleash innovative companies. This may lead to some dead or wrong turns, but DOD can take a page from the corporate world and learn from R&D failures. Strengthening the transition of SBIR investments into programs of records is one such method. On the promote side of the ledger, we need to make sure the Department is a customer of choice for emerging technology providers. This will require acquisition processes that operate at the speed of relevance and budget stability so we can send a clear demand signal so industry can effectively plan and commit resources.

We need to encourage and expand new and innovative partnerships across government, industry, and academia to exploit the pace of innovation and rapidly scale transformational research and operational prototyping into robust and scalable capabilities that will enable technological, and operational, superiority. We have several mechanisms to develop and field products quickly and in an innovative manner; SBIR, DARPA, DIU, the Space Development Agency, AFWERX, demonstrate daily they can bring nontraditional players into the DOD in a timely manner. We need to be nimble and thoughtful, encouraging the services to identify and support the transition of world class, disruptive technologies.

As part of the acquisition strategy, review prior SBIR projects and assess opportunities to utilize SBIR authorities or projects. Leverage the agile, time-saving authorities resident in the SBIR Phase III contracting to get those technologies under contract and delivering to the warfighter.

We appreciate Congressional support in helping DOD adopt an approach to accepting risk intelligently. Taking a more collaborative approach across services to identify and deploy game-changing technology prevents duplicative efforts and allows the Department to maximize limited resources. The men and women in uniform sacrifice daily to protect our nation, our freedom, and our way of life. They deserve every protection that we can afford them.

Chairman REED. Thank you very much, General, and gentlemen, thank you for your excellent testimony.

Before we begin questions, since we have some of our colleagues that are attending remotely I want to let everyone know how we will conduct the hearing. Since it is not possible to know exactly when our colleagues who will be joining by the computer arrive, we will not be following the standard early-bird timing rule. Instead, we will handle the order of questions by seniority, alternating sides until we have gone through everyone. Once we reach the end, if there is anyone we missed we will start back at the top of the list and continue until everyone has had their turn. We will do the standard five-minute rounds, and I ask my colleagues, particularly those virtually attending, to keep an eye on the clock, which you should see on your screens.

Finally, to allow for everyone to be heard, whether in the room or on the computer, I would ask all colleagues to please mute your microphone when not speaking. Thank you very much.

We were chatting before, and reminiscing about days gone by, and one of the relics of those days gone by is the current DOD budget process, the PPBE, Planning, Programming Budgeting and Execution. It was a product of the McNamara, the Whiz Kids, and I can assure you those Whiz Kids are not kids anymore. It is 70 years.

So I will ask all the members, beginning with Dr. Schmidt, do you think we need to modify this process in order to provide the kind of organizational responsiveness, and are there any other specific recommendations in terms of the current programs and doctrines of DOD that you would suggest, Dr. Schmidt.

Dr. SCHMIDT. So there are a lot of problems with the current procurement process, Mr. Chairman, and as a result, every few years there is a redo of them, which just makes it more complicated. There was a joke that the only way to understand the procurement

process was to have an AI system explain it to everybody, I am sorry to say, but that is the joke.

There are a number of problems with it. One has to do with its design cycle. There is something called a POM, or a program of record. There is a two-year planning cycle ahead of actually approving anything. So if you want to do something new, you have to plan it, and then it starts two years from the time you get it, because that is when you get the money for it. Because of the way the appropriators work, money that is not used in a particular time is taken away unless it is on an identified POM-based program.

This structure means that the people who should be making the decisions, who, in my opinion, are the combatant commands (COCOMs) and the heads of, you know, the Secretary of the Army and Navy and so forth and so on, find that they do not really have control over what is going on. They are responsible but they do not have the ability to affect these things. The result is the procurement systems are typically increasing. Every generation is increasing two years in design cycle, and the costs, of course, go up.

There are a number of mechanisms that you all have given the DOD over the years which are special authorities of one kind or another, and one of the questions that I do not understand is why, if you give them the special authority, they do not take it. So what I would suggest is that you give them more authorities and you also ask them to try to figure out why they are not taking advantage of them, because we are all in it together to get faster design cycles.

To give you an idea, and I will finish, to give you an idea of how strange the current design cycle is, in a normal business you would have an idea, you would have the engineers and the product people, you would have a chat, you would figure out how much it costs. The CEO or product person would say, "Let's do it." That is precisely not what happens in the military. There is a requirements document, which is not allowed to be communicated to the people who actually are going to build it. There is no feedback between the people building it and the actual requirement document. As a result, the requirement document gets longer and longer and longer, and the requirements cause the tradeoffs to get more and more complicated, and you end up with a camel rather than a horse.

And that is the overall cycle, and that is why these systems are so incredibly expensive. Changing that would save money and it would make us much, much more effective.

Chairman REED. Mr. Smith.

Mr. SMITH. I would offer two ideas, one, building on what Eric said. I think the more we can encourage the Pentagon to use the authority that you have created for some of these emerging technologies, the better off the nation will be. I am not here to say that you buy an aircraft carrier the same way you build software, but it is clear in the software space that you can be agile. And what we have found, in a very, I think, positive way, is when you can bring software developers and, say, warfighters together, so they iterate in a training site, and the warfighters identify a feature they need, and the developers go off and create it over the next day, and then they try it again, you can suddenly enable the mili-

tary to move forward at the speed of technology. So that is something worth pursuing further.

And then second, I do think it is a good moment in time to step back and look at our protest process. The protest process today definitely does not move forward at the speed of technology. And we all want to ensure fairness, and that includes a fair right to be heard. But we could definitely benefit from an accelerated timeline to do so.

Chairman REED. Thank you. General Carlisle, please.

General CARLISLE. Thank you, Mr. Chairman. I could not agree more with my colleagues on the panel. The problem that I faced when I was making decisions, I was a programmer in the Air Force so sadly I know PPBE very, very well and very painfully. And because of its two-year process there are so many people that can stop it along the way. There are so many levels that you go through.

So how you flatten that that is referenced as a suggestion we have an office in the Air Force called the RCO, the Rapid Capabilities Office. And the head of the RCO has authorized money to work on programs and goes directly to the Secretary of the Air Force, with nobody in between. And that ability to flatten that and get it done more rapidly is really a suggestion moving forward. And the other services, Space Force and the Navy and Army and the Marines have adopted this same type of thing.

And the other suggestion is the programs become—it was referenced in a previous discussion, that, you know, the F–35 program slowed down significantly because of a problem with the helmet. But it is because it was one giant program, and whether it is a platform, an airplane, a ship, a tank, the plan form, the platform that it is in is a development cycle of X number of years, 8, 10, that they are good for that period of time. They are 8- to 10-year, 12-year capability. The sensors, the hardware in them you probably need to change out every three or four years, in a plug-and-play, in an open systems architecture, because the technology and sensor capability and com capability changes that rapidly.

In the software area it should be a consumable. It should be like petroleum, oils, and lubricants (POL), because you change software so often, it is almost like the way you use gas and fuel in an airplane, that you have to change it continuously to stay up to speed.

So if there is a way to take a major defense acquisition program (MDAP) and break it down so you are not one giant program, that one flaw in either the software or a helmet or one component slows the entire program down. Thank you, sir.

Chairman REED. Thank you very much, General. Thank you, gentlemen, for your insights.

Senator Cotton, please?

Senator COTTON. Thank you, gentlemen, for your testimony today and your appearance.

Dr. Schmidt and Mr. Smith, I want to ask, to what extent do your companies or, Dr. Schmidt, in your case, maybe the company that you used to lead, or other companies that you may represent, rely on Chinese suppliers for electronic hardware, things like printed circuit boards, raw materials, like rare earth elements? Dr. Schmidt, do you want to take that first?

Dr. SCHMIDT. I am no longer with Google.

Senator COTTON. Yes, I understand, but to the extent that you still have knowledge of their operations.

Dr. SCHMIDT. Yeah. So, in general, the reliance is on Taiwan, and I think that as a matter of national strategic priority, Taiwan becomes more important to the United States for that reason. The reliance on Taiwan is quite serious. I am not aware of Mainland China dependencies, but there may be.

Senator COTTON. Mr. Smith?

Mr. SMITH. Yeah, I think what we see at Microsoft is pretty representative of what we are seeing across the IT sector for hardware production, which is a pretty seismic shift towards what I would call the diversification of the supply chain, which means, frankly, moving more suppliers out of China and to other countries. We are really focused on what I would describe as a multi-country, multi-continent strategy, and what you are seeing today is a lot of hardware manufacturing start to move to countries like Thailand and Vietnam and Singapore. You certainly see Taiwan, as Eric mentioned, as critical, South Korea, Mexico, and the United States itself.

I think it is right to think of it in the following way. The supply chain in China was created over the course of about 20 years, and I think with the exception of semiconductor chips, where the fabrication costs are so high, we are probably working through a transition of what I would call five years or so, where you are going to see us and everyone else have a much more diversified supply base.

Senator COTTON. Dr. Schmidt, you mentioned reliance on Taiwan in particular. Are you talking about reliance primarily on Taiwan for semiconductors?

Dr. SCHMIDT. Yes.

Senator COTTON. And that is an especially dangerous reliance because Beijing considers Taiwan to be part of the People's Republic of China. Correct?

Dr. SCHMIDT. That is correct, and if I may add that there was a time when the United States was the great leader in semiconductors, and indeed this Congress, in the 1980s, approved something called SEMATECH, to make sure—it was headquartered in Austin and was pretty successful in the eyes of many people. But over the last 20 or 30 years, the majority of the production of powerful semiconductors is now offshore, with the exception of some of Intel's fabs and a few foundry fabs.

But it is fair to say that if you want a leading piece of hardware, which is what we all need to do what we do, you are probably going to use a vendor called TSMC, which is the one in China. They are just faster, better, et cetera.

One of the key recommendations that is in the AI report coming out on March 1, is that America needs to stay two semiconductor generations ahead of China, and that we need to do the steps necessary to do that, which are long and complicated and painful. But it is really important. We were in this business. We got out of the business. We should back into it.

Senator COTTON. Yeah. I just want to point out that our dependence on TSMC is great, and the vulnerability of them to China is

great as well. Mr. Smith, you talked about South Korea. There are some other countries you might diversify into, in Southeast Asia. Those countries are still, let's just say, within striking range of Mainland China, but China does not have a core claim to want to forcibly seize their territory. And this is one reason why Taiwan is not just a strategic and a moral question for the American people but also vital to make sure that we do not allow the Chinese Communist Party to seize control of the world's most important chip manufacturer.

So I strongly support the efforts that we have to build more semiconductors here in the United States. That is why I worked with Senator Cornyn, Senator Schumer, and Senator Warner last year on the American Foundries Act, and we are trying to get money for it this year, but also to diversify, out of striking range, let's say, from China, and in particular, out of Taiwan itself. We want to be good partners with TSMC, and we will always defend Taiwan's sovereignty and autonomy, but this is not a vulnerability that the American people can continue to permit.

Dr. SCHMIDT. If I could just add, there are quite a few research efforts in America leading to new designs and new approaches to semiconductor that would create the possibility of a leapfrog. Those need to be investigated. That is part of American greatness, and we need to emphasize them.

Senator COTTON. I agree, and Taiwan Semiconductor Manufacturing Company (TSMC) is planning to open a plant in Arizona. That is great as well. We want to help that kind of reshoring of manufacturing of semiconductors as well.

My time has expired. Thanks, gentlemen, for showing up.

Chairman REED. Thank you, Senator Cotton. Senator Shaheen, please.

Senator SHAHEEN. Thank you, Mr. Chairman, and thank you all for being here and for your testimony this morning.

You have all mentioned workforce as one of the challenges that we face. Mr. Smith, do you believe we are producing the science, technology, engineering, and mathematics (STEM) workforce that we need to be producing to be competitive right now, and how would you suggest we improve on that?

Mr. SMITH. I think as we look to the future we are going to have to invest more and we are going to need to do more, and it really touches every aspect of not just education but skilling for the entire population. I think we need to invest early in the K–12 system. I think we need to support more teacher training to get more computer science teachers into the nation's high schools, in particular.

I think that our community colleges are an enormous research that we are underutilizing today. There is an enormous shortage in the United States today for cybersecurity professionals, and I think we can harness our community and technical college, and certainly our four-year and graduate programs remain of imperative importance as well.

I do think we are also at a point in time where we should think about providing people with digital skills as a life-long endeavor. It means more investment in digital skilling for the members of the military, but really every company, every organization. And I think there are those of us in the private sector—Microsoft has

LinkedIn—we can do more and we are working to do that, but it is going to require a collective effort.

Senator SHAHEEN. I certainly agree with that. As a former governor I know we worked very hard to focus on STEM in New Hampshire. And one of the areas that we had some of the biggest gaps were encouraging women, young women, to get involved. And I think it is a place where Silicon Valley has not done a very good job of providing equal opportunities for women. So we have got challenges both in the public and private sector.

So do any of you have any thoughts about how we encourage more women to——

Mr. SMITH. I would first say we need to become more diverse on every indicia of diversity. There is no area where——

Senator SHAHEEN. Absolutely.

Mr. SMITH.—we should feel like we are ready to pat ourselves on the back. We need to recruit and advance the careers of more women. We need to do a better job of recruiting and advancing more opportunities for black Americans and for our Latinx population. And we should do it, I think, with the recognition that our industry does its best work when we have a workforce that is as diverse as the customers we serve, which means the country as a whole.

Senator SHAHEEN. I certainly agree with that, and I think the comments I think you and Dr. Schmidt both made with respect to immigrants and trying to keep in the United States those immigrants who have graduated from our colleges and university with degrees that we need here is really important as part of our national policy.

I want to go on to another topic, because I agree with the sentiment that I think we all share, that China is the biggest long-term threat to the United States. But as we look at what we need to do to harden our digital infrastructure, clearly the biggest recent threats come from Russia, and yet we are not talking about how we combat that kind of cyber hacking into our systems that are going to affect our ability to achieve all the other goals that we have.

So do any of you have a thought about how we should be responding to Russia and their cyber hacking, and what kind of innovation we need in order to protect against those kinds of hacks?

Mr. SMITH. I would offer a few quick thoughts. Number one, we need to modernize the information technology (IT) infrastructure where it is dated, and it is often most dated in the public sector. We are seeing this right now with vaccine distribution and public health agencies across the country.

Number two, we really need to instill the broader application of what are clear cybersecurity best practices. A lot of these recent attacks have taken advantage of lapses in just good practices.

Number three, we are going to need to secure the software supply chain. We were talking before about hardware, but the software supply chain, and really the build systems for software need to be strengthened.

And then, finally, I would say we need to continue to strengthen the rules of the road and hold other nations accountable when they violate them, and do it with our allies.

Senator SHAHEEN. Thank you. General Carlisle, you mentioned the SBIR program, which has been really critical in developing innovation that has been adopted by the military. Right now that program is scheduled to expire in 2022. How important is it, do you think, that we need to extend that and make it permanent?

General CARLISLE. Senator, thanks very much for the question. I cannot tell you how important we think that is, and I think the ability to utilize SBIR, it is underutilized now. It is another way that I believe, in reference to the chairman's question of how we can accelerate the process. You get an SBIR contract Phase 1, you maybe make it to Phase 2, and you have a promising technology, but then how do you get it into program of record? How do you cross that, quote/unquote, "valley of death"? And there are different ideas about it, whether it is a fund that allows you to put them into programs.

As a person that was the consumer, the problem we would have is I would find this great technology and I would want to put it into my F–22s or my F–35s, but I could not do it for two years. A small business cannot survive two years on a promise. You know, they are mortgaging their house so that they can make payroll, so they can continue to develop this technology.

I think SBIR is incredibly important, and I think we need to find a way in the authorization and appropriation process and within the Department to have funds available to continue those programs through Phase 3 and get them onto contract, and more practical, use them in programs of record with the large primes.

Senator SHAHEEN. Well, thanks very much. My time is up, but if you have thoughts about how we should reform that program to make it more effective for small business I hope you will share that with us.

Chairman REED. Thank you, Senator Shaheen. Senator Rounds, please.

Senator ROUNDS. Thank you, Mr. Chairman. Gentlemen, let me just begin by thanking you all for being with us today. Your expert testimony in these fields is critical, and this communication is very, very helpful to us.

Let me begin, I would like to begin with a question for General Carlisle. Last year, the National Defense Industrial Association, or the NDIA, sent our committee a letter stating their concerns about the potential interference between the proposed Ligado system and GPS. Last month, the Federal Communications Commission rejected the National Telecommunications and Information Administration's petition to stay the commission's April 2020 Ligado order and authorization.

What are your thoughts on the potential impact of Ligado's proposal on the Department of Defense, and has anything changed since the NDIA's letter last year? I think this is a critical issue that needs to be addressed, because we are going to have this come up time and time again in the future.

General CARLISLE. Sir, thank you very much for your question, and let me start by saying the work that the chairman, the ranking member, and this entire committee has done in support of the position that I believe is the correct position with respect to Ligado cannot be overstated how much we appreciate it. There are the two

studies that go back to a DOD study in 2018, and an Air Force classified study in 2016. I was part of the Air Force classified study in 2016. I think that it still stands. I think that the potential for interference is great. They went from a space-based to a terrestrial base, and knowing what the power of the global positioning system signals are and the importance of position navigation and timing, not just to the Department of Defense but to the whole government and to every American, I think the potential for an interference is something that has to continue to be looked at.

I think we have to follow the science, and I think we have to continue to study and learn. And until we really understand, then I do not think I believe that you cannot move forward with the Ligado until you finish the science and you actually know and you can demonstrate that there is interference, or if there is not then you can demonstrate that. But the risk of continuing not knowing the answer to that and not having all the science, I think that is unacceptable, sir.

Senator ROUNDS. Thank you. And for Dr. Schmidt and Mr. Smith, what can be done to make sure that the Department of Defense can maintain access to spectrum to meet warfighter requirements while balancing the needs of the private sector to build commercial 5G systems? Are there improvements to DOD's related infrastructure that would help? Part of my question also goes to being able to share the information, and sometimes which is classified in nature, but to share the risks involved when we have that challenge between commercial operations and DOD, and the significance of the release of spectrum that may very well be needed within the DOD's long-term plans.

Dr. SCHMIDT. About 12 years ago, the White House issued a report, and I know because I was one of the authors, that talked about the concept of preemption. And the basic idea is rather than owning the highway you can occupy the highway, but if a higher priority police person comes along you have to get off the highway, or some metaphor like that.

So the way these systems work is the radio says, is this busy with somebody who is more important, and if so then they do not transmit. So this technology is now well mature and is being used in something called Citizens Broadband Radio Service (CBRS). I am one of the people who believes that we could share the military spectrum such that the military had pre-emption. That is, the military could always get what it needs but still make that spectrum available when it is not used.

One of the more humorous example is that some of the interesting key mid-band spectrum is using naval radars, and the vast majority of those naval radars are not in the middle of our country, on land. So you can imagine that there is an opportunity to sharing. Anything that you were to do with military spectrum would have to have an absolute rule that the military had the highest priority, and further, I would propose that the military run that sharing system to ensure it.

Senator ROUNDS. Thank you. Mr. Smith?

Mr. SMITH. I would say, just building on what Eric said, I think there is a broad recognition today that we are going to need to use more effectively the so-called mid-band, between 3.10 and 3.45

megahertz, both for the DOD and for the civilian sector of the economy. We are going to have to find a way to share it, and I think he just offered a good description of the kinds of approaches that have proven effective elsewhere.

And then we, you, are really going to need to decide what is the best way to do that. There are two alternative models. One has the DOD own it and then have others lease and operate it. The other is to auction it and let the DOD have priority access to it. I think that is an important discussion to have.

Senator ROUNDS. Thank you. My time has expired. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Rounds. Senator Blumenthal, please.

Senator BLUMENTHAL. Thanks, Mr. Chairman, and thank you for having this hearing, which is such a great way to begin this session of the Congress, with a topic that is so timely and critical.

First of all, let me say, on the semiconductor issue, this shortage is real, urgent, and present right now. A group of us, bipartisan group, wrote to the White House recently about the shortage of semiconductors in the automotive industry, which threatens to inhibit actual production right now in our manufacturing of automobiles in this country. The same is true in other critical sectors of the economy. I recently visited a much smaller company, Sema4, in Seymour, Connecticut, which produces medical equipment. It is affected by the shortage of semiconductors as well. Its plea to me was, "Please do something to help us." So I thank you for calling attention to this problem, but it is not some abstract future issue. It is here and now.

Let me say to all of you thank you for your contributions on the developing threats that we are discussing today. And, Mr. Smith, in particular, I appreciate that Microsoft has been such a leader in helping us to recover and understand the recent SolarWinds attack. In fact, we are meeting here about two months after the discovery of the largest cyberattack in our nation's history, a devastatingly brazen and damaging attack on our cyber defense, in fact, revealing the lack of cyber defenses.

And I think that your reference to the recent crisis in Texas shows us the mushroom cloud that, in the nuclear area, would be the symbol of a similarly devastating attack in the nuclear area. It is very difficult to sort of understand in real terms what a cyberattack could do to this country unless you look at what happened in Texas—loss of water, loss of electricity. Our nation is in no way prepared.

So I would like to take your reference to the offense/defense. You and I have discussed it a little bit. What can we do to deter that kind of attack? Right now, we have failed to make clear to our adversaries that they will pay a price, as General Paul Nakasone said when he testified in his confirmation hearing. He said our adversaries do not fear us. What can we do either to make them fear us or establish, as you put it, rules of the road that would establish some kind of framework that will prevent this kind of attack on us or on other nations?

Mr. SMITH. It is a critically important question and, of course, the ultimate answers will come from the people who lead the gov-

ernment, not from those of us in the private sector. But I would offer two thoughts.

First, it takes real clarity about the lines that others cannot cross without consequences, because without that kind of clarity I do not think any deterrent doctrine can be effective. I am not even sure there is a deterrent doctrine in such a situation. And I think it is easy to sort of lose hope that we will ever bring the entire world together around new rules of the road, but I do not think we need to. I think we need to start with ourselves and bring our allies with us, and make clear what lines we do not believe are crossable, and I would say the disruption of the civilian supply chain, in a disproportionate and indiscriminate way, should be one of them.

And then I think, like anything, there needs to be a graduated set of tools. I think it needs to start by public accountability with the United States and other governments, as the country did in 2017, twice, after WannaCry and NotPetya. But then there need to be responses as well, and there should be a range of responses for different circumstances, but it needs to be a robust menu, and we are going to need an Executive branch that has the confidence and the support of the American public to carry them out.

Senator BLUMENTHAL. As yet there has been no response, at least, that is known to us in the Congress. Maybe I missed that response, either covert or apparent in some public way. There has been no proportionate response, no response whatsoever that I have seen to the SolarWinds attack, and I think that making our adversaries, Russia, in particular, pay a price for this attack is absolutely necessary. That is one of the ways to establish some rules of the road.

But I agree with you that strengthening the supply chain defenses is also important. And we have seen a wide variety of competence in that area. For example, just in the government, the VA has been much more defense-oriented, much less vulnerable than, for example, the courts or the Department of Justice. So we have seen varieties that I think we need to learn from.

So thank you very much for your testimony today.

Chairman REED. Thank you, Senator Blumenthal. Senator Ernst, please.

Senator ERNST. Thank you, Mr. Chair, and gentlemen, thank you very much for being here today. And, of course, as the ranking member on Emerging Threats and Capabilities this is a very, very important hearing for us today.

And, Dr. Schmidt, I would like to start with you. A number of years ago I introduced legislation which became the National Security Commission on Artificial Intelligence, which you chair today, so thank you very much for that. And you did mention you have a report coming out very soon on artificial intelligence, and so maybe some of the questions I have for you today might give us a little bit of a sneak peek on some of those efforts.

But as you know, and all of us understand, is that we have a lot of different efforts across Department of Defense in the area of artificial intelligence. So we have the Joint Artificial Intelligence Center (JAIC), we have DARPA's initiatives when it comes to AI, and, of course, then we have our service branches and special operations forces all trying to develop their own needs for AI to meet their re-

quirements. So a lot of different efforts coming from all different directions, and, of course, that creates a challenge with the coordination of those AI efforts.

So how is DOD working to make the different R&D centers, the military branches and special operations forces efforts available for AI development and those applications?

Dr. SCHMIDT. Thank you for giving all of us the honor to serve on this commission. It has been a remarkable experience, and I think you will be pleased the final report in a week.

With respect to your question, we recommended that the JAIC be kept at a three-star level. In the military, hierarchy determines everything, and it is important that it be at the right level so that it has influence across the other operations. The JAIC is well run. It does not have enough resources.

In general, the way to understand the military is that there are very few actual AI resources and there are an awful lot of people who are attempting to help who do not know much about it. And so we go over and over again the need for human promotion, technical training, getting the right specialists in the right positions, working with partners who are at the state of the art. AI is extremely hard and confusing for a normal programmer to understand, or a normal human to understand. It is a new thing. It is very challenging. It needs specialists.

Senator ERNST. Yes, and thank you for that, and I think you are right, in that we have many people attempting to take the hill, and that is why the collaboration is so important with the JAIC.

The current state of the AI strategy deployment at DOD, and how, again, you know, talking about our near-peer adversaries, how does this compare to the approach and the goals that have been laid out by China with their own AI efforts?

Dr. SCHMIDT. It is hard to know what China is doing internally. There is a classified report, which I obviously am not going to mention now, that I would encourage you to take a look at.

Senator ERNST. Thank you.

Dr. SCHMIDT. But a simple summary is that China has announced that they wish to be the global leader in all aspects of AI by 2030, and they are relentlessly focusing on that. They are doing it with their STEM training, their investments, their companies, and so forth, and presumably because of what is called civil-military fusion, all of that information just naturally goes back and forth within their military, unlike our structure.

In the United States, we believe we are one or two years ahead of China, not five or ten, and because of the diffusion of the technology you have to expect that anything that is invented in open-source AI world will immediately be adopted by China. So the threat is very, very real.

Senator ERNST. Yeah. Thank you. And I think we should all take note that, Dr. Schmidt, you said one or two years ahead of China, and we cannot afford to lose that edge. And it would be a much more comfortable margin to be five to ten years ahead of China. So thank you.

If you had to prioritize, just very briefly, one or two areas that would have an outsized impact at DOD when it comes to AI at scale, what would those one or two be?

Dr. SCHMIDT. So when you speak to the senior leadership what they want is a battlefield command center that takes all the centers and helps them identify what to do. That should not be the highest priority, because, one, it is hard, and two, they do not have access to all the sensory data anyway because they are all so stovepiped. So it is a good idea but do not do that first.

Senator ERNST. Good advice. Thank you.

Dr. SCHMIDT. But it is important to say what not to do. Most of the military spends most of its time watching things. They watch for launches. They watch for cars. They watch for aberrant appearances. AI and machine vision is particularly good at that. An example is that I was on a minesweeper, which is a wooden boat, where the young man who was doing it was watching a screen to tell him—and his accuracy, by the way, I asked his commanding officer, two-thirds of the time he found the mine. Well, does that mean one-third of the time he doesn't? Computers can do this much, much better, and plus the guy is bored beyond belief.

So my point is vision, monitoring, and analyzing are the best strategic uses of this technology—quickest to inform, quickest to implement, highest payoff.

Senator ERNST. Absolutely. Thank you, gentlemen, so much. The applications for AI are endless, and I thank you, Mr. Chair, for bringing this hearing forward. Thank you.

Chairman REED. Thank you very much, Senator Ernest. Senator Kaine, please.

Senator KAINE. Thank you, Mr. Chair, and thank you to the witnesses. I want to ask you about two topics. One is immigration and the second is alliances.

So on the immigration side, just as in your industry, so many of the most prominent advances in national security have been innovated by immigrants or the children of immigrants. Robert Oppenheimer, the Manhattan Project, child of German immigrants. Jerry Jordanoff, who helped design the B–29, Bulgarian immigrant. Father of the nuclear Navy, Hyman Rickover, Polish immigrant. Father of stealth, Ben Rich, Filipino immigrant. And then broader national security priorities like vaccinations, Jonas Salk, child of Russian immigrants.

How important is it if the United States wants to maintain an edge in these emerging technologies, how important is it for us in Congress to do comprehensive immigration reform that continues to make the U.S. a destination of choice for talented people from around the world?

Mr. SMITH. I think it remains a very high priority. One of the interesting things about technology is it always starts with talent, so it starts with people. And if you want to have the world's best technology, especially if you have a country as we do, that has the world's best universities, you want to continue to attract the best and brightest, not just to study here but to stay here. And I think the more we can do in especially these high-demand fields and these critical graduate degrees, to give people the assurance up front that they can not only get a visa but a green card, we put ourselves on a path to do that.

I think one of the other reasons that comprehensive immigration reform is so important is we have so many other extraordinarily

talented people here, including working in the tech sector, who need the added certainty. They are either stuck in a green card backlog because they came here from India, and they risk actually having their children age out, or they are dreamers. I am very struck. We have an extraordinarily talented young person at Microsoft. He is working at Microsoft to our benefit rather than on, frankly, what he would like to do, which is the aerospace field, because as a Deferred Action for Childhood Arrivals (DACA) registrant he can do one thing but not the other. And so I just think we need to address this range of issues to continue to nurture the world's best talent.

Senator KAINE. Let me ask Dr. Schmidt, if I could, about alliances, and I would like to hear from others on this as well, but to begin with, Dr. Schmidt. In your opening comments you talked about seven areas where China is trying to get dominance over the United States, where we are in competition, seven technical fields.

My assessment, as a member of this committee and the Foreign Relations Committee, is one area where the United States still has some significant advantage over China is in the area of alliances. We have longstanding alliances, participation in multilateral organizations, and we do multilateral alliances different than China does. China has a little bit more of a mercantile, what-can-I-get-out-of-you approach, and the countries seem to understand that. And it does seem like adversaries like China and Russia, to the extent that they are nervous about us, one of the things that most makes them nervous is alliances like NATO and others, or when the United States was leading, potentially, into the Trans-Pacific Partnership (TPP). That made China very, very nervous.

In the area of emerging technologies, how can we use our alliances to help us drive an expanded capacity without running into a problem, say, for example, the F–35. Built it with allies, Turkey has been sort of a wavering ally, and then we end up building something, and there is a security compromise as the technology now is available to a wavering ally. How can we leverage the value of alliances in advancing in these emerging technologies while protecting ourselves from an example like I just made with the F–35?

Dr. SCHMIDT. Thank you, Senator. I note with concern that Boris Johnson announced today that they are all Sinophiles and that he is heavily motivated to work with China. This is our longest-standing partner, the United Kingdom. This is a bad sign and a bad omen for what is going to happen. We must build every possible technological sharing path between our key alliances, and who are they? Israel, France, Germany, the United Kingdom, Japan, Korea, maybe India. There is a list of about ten. The word that is coming to the industry is the T–10. And what it means is constant harvesting of the best ideas, putting companies together, and so forth.

If you start from my premise that American global companies are our greatest asset because they move so quickly, let's have American companies working closely across all those boundaries. Everything that we do to make it harder to work across those boundaries also hurts our national security.

I also think that the government should have a national competitiveness plan, which includes a list of the key technologies and a list of the key countries. There should be money—not a lot of

money, but basically money to basically fund the communications, travel, and the partnerships, with somebody driving it out of the White House.

Senator KAINE. Illuminating answers. Thank you. Thank you, Mr. Chair.

Chairman REED. Thank you, Senator Kaine. Senator Cramer, please.

Senator CRAMER. Thank you, Mr. Chairman, for having this really impressive panel and hearing. You all have drilled down pretty deeply on several issues that I have an interest in, so I am going to try to drill just a little deeper on one, first of all. It gets to what you said, Mr. Smith, in talking about procurement reforms. I do not know that we could disrupt enough to be as effective as we need to be, but we, in this exceptional system of ours, protect things a little more probably than other places, and that is okay.

But you specifically raised reform of the protest—you talked about some protest reforms. Could you elaborate a little bit on that, because I agree. That is a problem. You have all talked about the delays that lead to delays, and time leads to mischief—those are my words, not necessarily yours—but protest reform seems to be one of those areas maybe we can do a little better while still protecting everybody.

Mr. SMITH. Well, it is a really important question. It is certainly another one that we have experienced as a company over the last year.

I would start with the recognition that these new technologies that we are talking about today really, for the most part, start as commercial technologies and then they are put to military use, rather than the other way around. So the best way for the Defense Department to move faster is use commercial technology, add security layers, as we have done with the DOD and the intelligence community for, say, secret and top secret workloads, and then create adaptations. But it is so important to move quickly. Then the question is, how do you move quickly when the protest process moves slowly?

So I do think there is a real opportunity to look at the process, streamline it, put in place some tighter deadlines, consider legal reforms that would apply those deadlines to the judicial aspects as well. We do not think that others should be denied an opportunity to protest. Maybe for better and worse that is part of the American way, to some degree. But it sure would be beneficial if it could move faster.

Senator CRAMER. Others on the same topic, Dr. Schmidt or General?

General CARLISLE. So the only thing I will tell you I noticed, and Mr. Smith and I had this discussion ahead of time, is I agree, there has to be an opportunity, but the speed with which you go through it—and the fact is there is absolutely no disincentive to protest. And except for the consumer, the customer that is going to actually use the equipment and is denied that equipment for an extended period of time. So the question is, how do you accelerate that, allow those things to happen fairly, but at the same time do not disadvantage the person that is waiting for the equipment while you are waiting for the protest to be resolved.

Senator CRAMER. For sure. Well, I would love to drill down more on that, if anybody has any brilliant ideas, whether it is our judicial system, legal system, regulatory system, or government, whatever we can do.

You also have all talked a lot about the skilled workforce, and I think you have answered a lot of the questions really well on that. One area I might just seek a little more input on. First of all, I agree wholeheartedly. We have so blown the opportunity to maximize the incredible high-skilled immigrants that have come to this country, whether for education or for work, or all of the above, putting them in these boxes. The backlog of green cards is immoral to me. The per-country caps I have been trying to get rid of for a long time. It punishes certain countries, obviously, that have a lot more to offer us.

But it also opens up another one of those security risks, right, I mean, whether it is chip manufacturing or immigrants. How do you see moving forward with high-skilled immigrants and some of the reforms, whether it is—I think you have talked a little bit about comprehensive, and comprehensive is fine, but comprehensive seems to always get in the way of doing some other good things. And I am just looking for lane here in this next Congress to finally get something over the top as it relates to the backlog of green cards and high-skilled immigrants.

Dr. SCHMIDT. So Brad and I have spent 30 years here saying basically the same thing.

Senator CRAMER. Well, good. I feel better. I have only been spending about six.

Dr. SCHMIDT. I know, and I am sorry to say the same thing again. Our industry is critically dependent upon high-skilled workers. Today, our industry represents 20 or 25 percent of the total stock market value of America. So we are sort of important in at least the economic output, if not the pride of the country. And we need these people because they are the creators of our products.

What I would suggest with respect to the questions of concern about security is that you could imagine, for example, a Chinese national comes in, and you would ask them, "Have you ever been associated with this group, this group, and this group?" and presumably they would say no. When you discover that that is the alternative truth, through some mechanism, you can get them out. And I think that there is an investigative process that is relatively straightforward. There is set of red flags. The vast majority of the Chinese people that we work with are not political, not dangerous, and they are incredibly important.

One more comment. We looked at the question of how important are Chinese researchers for the AI effort in our report, and it turns out that the Chinese researchers are the number one foreigners on the key papers. So if you were to, if you incorrectly get rid of all of them, because you just do not like them or something, you will, in fact, hurt America's AI leadership.

Senator CRAMER. Well, I might—as I just wrap up with my time gone—submit to you as well that you have discussed allies and alliances, and this is another area of opportunity, it seems to me, to build maybe some new alliances with some large countries. And with that I yield. Thank you.

Chairman REED. Thank you, Senator Cramer. Next will be Senator Gillibrand via WebEx. Senator Gillibrand?

Senator GILLIBRAND. Thank you, Mr. Chairman. Thank you for testifying. Since Cyber Command unified the cyber defense of our nation in 2010, we have adopted a strategy of persistent engagement, which intends to keep our adversaries continually challenged in order to stop attacks like this before they begin. The SolarWinds attack has been going on for nearly ten months and was likely designed by over 1,000 software engineers. What resources do you believe that we need to develop in order to avoid missing something like this again?

Dr. SCHMIDT. Can I add, Senator—can I add that the vulnerabilities of the nation's infrastructure are well known and we have chosen not to fix them. If we wanted to fix them we would upgrade all the software and we would have some rules. So, for example, the data that is inside these systems is encrypted at rest. It is encrypted in transit. We would use proper authentication keys. The military actually does this. Many of the rest of the aspects of the Federal Government do not.

So until we commit to bringing our infrastructure up to the state of the art of defensive tools we will continue to have this exposure, independent of what United States Cyber Command (CYBERCOM) does.

Senator GILLIBRAND. Right.

Mr. SMITH. And, if you want, I would add just two quick responses to your question. One is the recent attack exploited the fact that while the National Security Agency (NSA) has authority to look outside the United States, it does not inside the United States, and it was, in fact, it appears, data centers of commercial companies in the United States that were used really for much of this activity. So I think the Congress and the country are going to need to decide how it wants to better protect our internal resources.

And then second, related to that, I think there is a real question, when must companies, under the law, a law to be decided, report these kinds of attacks, and to whom and how in the government? I think we need to consider how these things fit together so we have more aggregated and comprehensive threat intelligence.

Senator GILLIBRAND. Thank you. On January 6th, we saw what can happen when extremism, incubated in online social groups, spilled over into the real world. Many hate groups, present at the Capitol insurrection, used online platform to organize and rally. The development of emerging technologies, including improved encryption and other communications tools, are a boon to the privacy of our citizens but also obscure already murky online extremist networks.

What responsibilities do you believe private industry has to disrupt the spread of violent extremist ideology, and what are the possible regulatory changes that Congress should make?

Mr. SMITH. I think this really goes to the question of addressing harmful and dangerous content online. If you look at the trend around the world, you know, we have seen other governments take this on. Australia was a leader a couple of years ago in enacting new legislation, that imposes obligations, legally, on tech compa-

nies, including, you know, Microsoft, Google, and others, to address extremist violent content and terrorist content.

As an industry, we have moved to work more globally and beyond the law, in a collaborative way, through what is called the Christchurch Call, which has brought together a number of governments and the leading tech companies. We are doing more to address this. I do think this is a moment in time when we should ask where we want the law in the United States to go and where we want collaboration with our allies to go.

The U.S. work is always more complicated, frankly, than in other countries because of the nature of the First Amendment to our Constitution, but a lot of these efforts have identified weak points we can work together to address.

Senator GILLIBRAND. Thank you. Just one last question on China before my time expires. Obviously, China is becoming, and aiming to become the global science and technology leader by 2049. How can we best prepare to outpace China? What obstacles do you see the U.S. having to overcome in the science and technology race? I did hear your testimony about software and the importance of investment and collaboration. What do you believe are the biggest missteps to date, and what do you think are the best ways to avoid it in the future?

Dr. SCHMIDT. My personal view is that our industries' success has largely been due to the extraordinary decisions made by this body over 50 years to fund basic research, starting with Vannevar Bush, et cetera, et cetera. Today, R&D funding, as a percentage of gross domestic product (GDP), is lower than it was at Sputnik. So one of the problems is that we are, to some degree, leading off of our seed corn, if you will, on all of that. We have already talked about immigration. We have talked about the importance of STEM education, and those things.

I think we have to confront the following problem. There is a set of platforms, which I identified in my technology, which are going to happen but they are going to happen first in China, unless we have a more concerted effort in America. I would like to see a national list of key technology platforms that we collective agree must emerge, must emerge using Western values, must be the ones being used by our partners.

And to understand what happens if we do not do that, consider Huawei, which we are basically trying to ban as hard as we can, because their products were less expensive, more easily subsidized, and faster, in some cases, than the competitors that are from Europe. America got out of that business. That is an error. I want us to be in those businesses with world-class products. I think we need to know what that list is, I think the government will need to help with some forms of funding, and we need to let the private sector build those things and make it successful.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Gillibrand. Senator Sullivan, please.

Senator SULLIVAN. Thank you, Mr. Chairman, and, gentlemen, thank you for testifying today and your service. General Carlisle, always good to see you, sir. Great career in the military. And, Mr. Smith, I appreciate our opportunity to chat last night. It was very

informative for me. And, Dr. Schmidt, thank you for all you are doing in your post-Google world.

Let me ask a question. There has been some press back and forth, and I think given you three leaders, right, big leaders in America, in a whole host of different ways, there has been some press in the last couple of years where some concerns I have read, and I would love you to just comment on it, our tech industry, Silicon Valley in particular, kind of maybe not being so interested in supporting our military, supporting the Pentagon.

You know, Mr. Smith, as you and I talked about it, I had the opportunity to go out to Microsoft's Integrated Visual Augmentation System (IVAS) partnership and development center. I thought it was incredible seeing these young men and women who were very motivated to help our men and women in uniform. Dr. Schmidt, I am sure you saw, there is some Google press that I thought was very unfavorable, where, you know, there was this idea, hey, we do not want to help the Pentagon. My view, as an American, it is a free country. You can do whatever the heck you want, but do not then be found to be helping the Chinese Communist Party. Like that is going to be a problem.

So can you three—I would love hear just succinct statements on, from your perspective, just how important that is. We have a challenge with this very new, great power competitor and the technology aspects of our country. Working with our military is going to be indispensable. And it does concern me some when you hear—and again, they are allowed to do it; that is one of the great things about our country, it is free. You can say whatever you want. But I would love to hear from you guys on just how important it is to be doing what you are doing and what we are talking about here, because if we do not have that kind of cooperation it is going to be tough on all of us.

Mr. SMITH. Well, I would say first I think one of the great challenges for this committee, the Congress, and the country is to keep the public united around the importance of our national security at a time when we live in a polarized political climate. And the key to that, not surprisingly, is, as always, leadership and communications.

The formula that we have found to be effective is to be clear, that we, as a company, at Microsoft, will provide to the United States military all the technology that we create. We will simultaneously engage to address the issues that a new generation I think rightly focuses on, things like the ethics of artificial intelligence. And we will honor people's choices, and when we have a project like IVAS it is really an all-volunteer project, and we have no shortage of volunteers.

Senator SULLIVAN. And those young men and women, I will tell you, having spent a day with them, were incredibly impressive, motivated, patriotic, because they knew what they were doing, which is helping the frontline troops who put their lives on the line for our nation.

Mr. SMITH. And I think there is one other thing where communication can be invaluable. Look, most people in the tech sector or perhaps most industries are simply not aware of the deep ethical tradition of the United States military. And when they learn about

it we actually realize that we have more to learn from the military, and it really changes the climate among especially a new generation of employees.

Senator SULLIVAN. I appreciate you saying that, Mr. Smith. Dr. Schmidt or General?

Dr. SCHMIDT. So the only thing—I am sorry, sir. I did not mean to interrupt. The only thing I would add is, you know, my experience is the American population is further and further, in many cases, removed from the military. It is an all-volunteer force, which is exactly the right thing, in my opinion, and the quality of the force in the United States military, I tell everybody if you want to be impressed with America's youth, go out to your flight lines, your ships, your tanks. These 19-year-olds are just amazing.

Senator SULLIVAN. It gives you hope and optimism. There is no doubt about it.

Dr. SCHMIDT. But I think it is an education. I think that, just as Mr. Smith said, I think, you know, a lot of it is not because they fundamentally, you know, do not like the military. They just do not know the lengths we go to to deter and prevent—the last person that wants to go to war is the person getting shot at. And so the prevention and deterrence. And then when we are to follow the most ethical rules, if we have to engage and how we engage and how we do everything we can to only follow the enemy combatant.

So I think it is an education process, Senator Sullivan.

Senator SULLIVAN. Dr. Schmidt, do you have a view on that? And I did not want to come down too hard, but I have ripped some Google employees in hearings like this before, where maybe it was bad press reporting, but I was like, you have got to be kidding me. I mean, again, free country. You can do whatever the hell you want. But if you are not going to help the Pentagon please do not go help the communist party of China with their AI research.

Dr. SCHMIDT. I did not agree with the Google decisions on Maven, et cetera. As you know, I worked as a government employee, working for the DOD for five years, using the DIB, so my personal view is clear. I also funded and have continued to work with a large number of startups in the areas that we are interested in, who are really, really committed to working with the DOD. So I can tell you that the Google experience you had was probably an aberration compared to the industry as a whole.

Senator SULLIVAN. And, Mr. Chairman, if I may, just very quickly, since this is such a distinguished panel—sorry to my colleagues—but I know you have been getting a lot of questions on China. Just very quickly, to be respectful here—I am over my time—comparative advantages that we have versus what they have, particular in this tech sector. I mean, I will give you, I think the fact that we are an energy superpower right now, producing more oil, gas, and renewables than any country on the planet, China would love to be in that driver's seat. Unfortunately we have an administration right now that wants to diminish that, which I find ridiculous and crazy.

But where do you think the comparative advantages are, particularly in AI? I read that part of their advantage is their massive population, that in some ways their own population is guinea pigs

that helps them advance in AI. Where are our comparative advantages, and vice versa, theirs?

Dr. SCHMIDT. So the Chinese are well ahead in areas like face recognition, because of what they do to surveil their citizens.

Senator SULLIVAN. So that is the idea of guinea pigs and billions of people that they can just test it on?

Dr. SCHMIDT. Their technology is generations ahead of what is possible in the West, and you can understand why. Their technology is extremely far ahead in electronic commerce and in mobile payments, and most recently they have announced the development of a central bank digital yuan, their currency, to actually—and they obviously have, from their perspective, internal security benefits from watching where all the money goes. These are all things that the United States would not do. So those are two where there is no question that they have an advantage.

There are people who believe that because they have essentially no privacy rights, in the terms that we think of it, that they will be able to aggregate very large databases, in particularly in health care, and that will allow for them to discover new things and so forth. We need to address these, and again, without compromising our core American values.

Mr. SMITH. I would just say, very briefly, we often talk about research and development, but especially for something like AI we should talk about research, development, and deployment. In other words, broad adoption and use, especially when you think about the positive feedback cycle that is created when technology is deployed. It creates more data. That data then leads to further improvement.

I think China is doing a better job right now than we are in deployment. Part of it is it is government-led in many ways. Part of it is there are uses where we, quite rightly, say no. Part of it is the entrepreneurialism we are seeing in many parts of the Chinese economy. So I think for the United States we have to think about how we foster faster deployment, and I think in the government, for the DOD, how the DOD, for example, can foster faster deployment.

Now, at the same time, the American comparative advantages in other respects remain considerable—our universities, our commercial technology sector. And I think the principles. One thing we have not noted that I think is very important in the world today is the fact that the DOD, last year, adopted ethical principles to guide the use of artificial intelligence by the military. And I think the more we can encourage our allies to adopt these principles, the more we separate ourselves in a way that will benefit us in numerous respects.

Senator SULLIVAN. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Sullivan. And now via WebEx, Senator King.

Senator KING. Thank you very much, Mr. Chairman, and welcome to our distinguished panel. We have touched on a lot of important issues. Let me start with a little bit of a detailed question for Mr. Smith from Microsoft.

You touched upon this. It strikes me that we have a gap in our authorities towards detecting and dealing with cyberattacks in that

the Central Intelligence Agency (CIA) and the NSA are restricted from operating within the borders of the United States, and yet the attacks, like SolarWinds and more and more, our enemies are getting more sophisticated about using servers within the United States. It leaves the FBI as sort of the de facto only cyber defense. Am I correct that is something that we really need to look at? We do not want to be spying on our citizens. On the other hand, we do not want to leave ourselves defenseless. Brad, your thoughts on that?

Mr. SMITH. Yeah, no, Senator, I think it is a really important question, and I think the first question for the Congress and the Executive branch is what part of the government do we want to have assume responsibility for what I will call the aggregation of threat intelligence domestically. Is it the Cybersecurity and Infrastructure Security Agency (CISA)? Is it the Federal Bureau of Investigations (FBI)? Is it somebody else?

The FBI, obviously, is principally responsible for law enforcement, which means it can work with the Department of Justice (DOJ), it can use its subpoena power, but, you know, it then needs to protect the confidentiality of information to investigate a crime. And what we are really talking about here is threat intelligence information that needs to be shared rapidly, oftentimes immediately, with the other parts of government.

So I think this is a key question. What part of the government should do it? What should the process be for collecting it and for sharing it?

Senator KING. Great. Thank you. Dr. Schmidt, an additional question on a different area, and you have really touched upon it today. Industrial policy has a bad name in this country but that is really what China is engaged in. And you mentioned we used to do a lot more R&D, we need to establish priorities, we need to bring semiconductor manufacturing home. Are we really talking about some kind of at least a more pragmatic and planned attack on maintain the technological edge? Is it Industrial Policy 2.0?

Dr. SCHMIDT. Senator, I hate to say yes, it is industrial policy, but can we not call it that? I think what would be useful would be to say there is a set of things that have to happen in America to maintain leadership globally in the important areas, and remember, these are the technologies that drive all of our economic output, our global presence, and so forth, and we need to do whatever it takes.

I think in many cases, with a little bit of focus, with a list, with leadership from the White House, leadership from here, a set of gatherings, and so forth, we can agree on what to do, and it is not as much the money as it is getting all the forces aligned.

What I learned in working on your AI report is there are plenty of people doing a lot of things, and they are somewhat discontinuous. And getting them unified around five or six or seven activities would be very helpful. In particular, we have highlighted—Senator Cotton and others have highlighted this question about semiconductors. That is a key issue. How are we going to solve that problem? Let's get some people in a room. Let's try to figure out what is the fastest path. If they cost $50 billion and it works then

maybe that is the right tradeoff, but I would like to have that debate.

Senator KING. Thank you. One final question, again for Brad Smith. I went to a defense policy conference in Singapore three or four years ago, two or three years ago, and met with a dozen or so officials of a variety of Asian nations. I came away from that with the conclusion that we have allies and China has customers, and that most of those countries wanted to work with us but they were always looking over their shoulder at China. In terms of cyber defense, in terms of national defense, in terms of technological innovation, it seems to me that allies are one of the most important assets that we have, that really most other countries, and particularly our adversaries, do not have.

Mr. SMITH. I think that is very well put. One of my favorite publications every year is the January edition of The Economist. It is an assessment of the world's democracies by The Economist intelligence unit. This year it says that there are 75 democracies in the world. They account for 49.4 percent of the world's population, roughly half of the world's people. And what it also notes this year is that democracy is growing in a number of important countries in Asia.

And I think it is a powerful remainder for all of us that there is an alliance of the world's democracies that we need to nurture as a nation, that we need to invest in and support as a technology sector. And we do that well, it not only advances the values that we all support in this country, it makes our technology base stronger. When you pull together these countries, you do not even have to pull them all together. Eric was talking about this before. But when you get India together with NATO and countries like Japan and South Korea and the like, and you pretty quickly get more than 2 billion people, that is a bigger market, obviously, than China.

Senator KING. And it is also a huge aggregation of talent——

Mr. SMITH. Absolutely.

Senator KING.—that can be taken advantage of.

I will leave you with a thought from Churchill. You can never miss with Churchill. He said, "The only thing worse than fighting with your allies is fighting without your allies."

Thank you very much, gentlemen.

Chairman REED. Thank you, Senator King. Senator Tillis, please.

Senator TILLIS. Thank you, Mr. Chairman. Thank you, gentlemen, for being here. I am sorry that I was not here. I have been watching it on TV and participating in two other committees that are meeting simultaneously. But I was here for your opening comments.

One thing that, as I was reading the committee prep materials I was thinking we need to do differently is how can we really accelerate the pace of innovation within the DOD for our defense. And I went back to Operation Warp Speed. Are you all familiar with that? We made, in record time, innovated a vaccine, did a public-private sort of bet on people in the private sector who were willing to take the risk, but the on the back end had Federal funding available for them if they produced a result in a shorter period of time.

Do you think if we are really going to accelerate, break through some of the—Mr. Smith, you and I talked last night about some of the hurdles that we have in DOD to just accelerate and field technology—should we be thinking about innovative ways of preparing or moving up to the NDAA to really incent more private risk-taking with some federal backstop, based on specific outcomes? I can think of a number of specific areas, but does that make sense? Is that something that a Microsoft would look at?

I want to go down the line. We will start with you, Mr. Schmidt, Dr. Schmidt.

Mr. SMITH. Yeah, I think it is an excellent question and there are two thoughts worth considering. Look, first, any time we can have more risk-taking in the private sector that is a good thing, and not every company can afford to do it. Microsoft can do things that a small businesses cannot. But look, we built a manufacturing facility in Milpitas, California, for our IVAS goggles for the Army before we won the contract with the units that we would produce there. That was private risk-taking.

We have literally been frozen by a Federal court on our performance under the Joint Enterprise Defense Initiative (JEDI) contract for more than 12 months. We have never stopped working on it, not even for one day. We may never get paid. That is a risk we are running. The customer may never be able to use what we create, but we have the confidence that what we are building will be of benefit to the United States some way, somehow. So the more we can encourage private risk-taking I think is a good thing.

And then, specifically, I do think there is something to think about in terms of lessons from Warp Speed for certain areas of technology. If you think about quantum computing, there are some that think it will take 20 years. There are some people that think it will take a decade. A year ago we were debating whether it would take 10 years to get a vaccine, and it took less than 12 months. And it did benefit from government spending, putting some money behind a series of companies with different techniques. Do not bet it all on one company or one method. Prepay and do it on the basis of particular milestones, so the government is getting in advance what it would then own or be able to use if something crosses the finish line.

But, you know, there is something there, I think, that we have all learned that sort of surprised us, I think, in the last year, that we should now apply to some of these new fields.

Senator TILLIS. Dr. Schmidt?

Dr. SCHMIDT. I agree with Brad. I would recommend that in this year's NDAA you all identify four projects where you say they will be run radically differently. I would pick one in missiles, one in satellites, one in personnel, and another one in some other areas. And you would, by law, state that they will not be run using the normal procurement mechanisms, but rather you will appoint a joint committee from the Congress as well as the Pentagon and give them the freedom to run the experiment.

Senator TILLIS. And General Carlisle, I am also thinking about the reality is some of the most brilliant ideas may come from some of the smaller players that are virtually impossible for them to do, just because of their scale with the DOD. But do you think that

that concept would apply with the right portfolio of some of the smaller companies? That is what I have in mind. The big players have to be there because they have the scale, but how would we structure that, I think building on Dr. Schmidt's suggestion for the NDAA. I honestly believe we have to have accelerators like this if we do not want to be talking about this next year when you come back.

General CARLISLE. Yes, so I could not agree more, Senator Tillis. You know, I think the Department has got to be willing to take risk. It is risk averse. If you are a program manager in acquisition or a contracting officer you do not get promoted because you took risk. You get promoted because you are on cost, on performance, and on schedule. So you do not try to get a stretch goal on performance, and that is where innovation comes from. You do not try to get it faster, because you may not make it. So we have to figure out how to incentivize inside the Department and industry. And I think your point on, you know, what we talked about earlier with Senator Shaheen, is the Small Business Innovation Research fund, we have got to find a way to get those through the tough times of an extended process, make it faster, and then allow them to be able to stay competitive and bring those technologies to the warfighter.

Senator TILLIS. Thank you, Mr. Chair.

Chairman REED. Thank you, Senator Tillis. And now via WebEx, Senator Duckworth, please.

Senator DUCKWORTH. Thank you, Mr. Chairman. Gentlemen, I apologize. I am having a little trouble with my video, because of bandwidth, but I am going to go ahead and do this via audio. Thank you so much for your testimony today.

The entire DOD has to innovate to compete against the other great powers, but U.S. Transportation Command (TRANSCOM) faces a unique set of challenges. Transportation Command's communications network, systems, and software have to support deploying troops and sustainment around the world. They receive inputs and data from many different government entities and also via doing business with private companies, for example, shipping companies and commercial air carriers.

But cybersecurity vulnerabilities in Transportation Command's network risk risks exposing our troops' locations, readiness levels, and operational plans, and the requirement to work with private business complicates addressing these weaknesses.

Dr. Schmidt, during your time on the Defense Innovation Board, the board produced a number of recommendations regarding the DOD's digital networks and cybersecurity vulnerabilities. In your opinion, how should Transportation Command, in particular, approach rapidly improving its cybersecurity without losing its ability to respond to warfighters and work with civilian entities? Your suggestions could include technical innovations, organizational changes, or perhaps policy proposals, for example. And I love this idea of picking several projects and approaching them radically differently in terms of procurement. Thank you.

Dr. SCHMIDT. Thank you. So our group actually visited St. Louis and the Transportation Command it was a very, very interesting visit. The key room is the room where you have people in uniform who basically have two screens, and there is an order from one

shipping system and they type the number of the order into the other screen and cause it to move along. So that is the level of automation that we, unfortunately, have in that. Any company would have integrated that, and we recommended that.

My own view is that there is a proposal in Transportation Command to do a new transportation system, which was hung up in a bunch of procurement issues. But the 80 or so different systems are going to have to get replaced by a more unified system, and that more unified system will have to have modern security. That is how we would address your concern. Because of the way it is currently architected, you are correct that we are very exposed to attack because there are so many different systems that are disparate and they are not unified.

Senator DUCKWORTH. Thank you. General Carlisle, do you have any recommendations, based on your work with the commercial members of the National Defense Industrial Association?

General CARLISLE. Yes, ma'am, and, Senator, thank you for the question. I agree with Dr. Schmidt, and I think we saw it in the command centers as well and how we integrate across different systems, even jointly between the services. And I think, you know, the comment was made earlier. We have a tendency to have our sensor suites are all stovepiped and our communications are often stovepiped. And what industry needs is the common architecture and the ability to work across the different systems, and I think Transportation Command is a great example of that, where they are working with the whole of government, really, and the commercial enterprise, but the systems are not compatible.

So what Dr. Schmidt said, and our ability to drive industry to have a set of standards and out of the stovepipe challenges that we face today in many of our systems as they try to communicate.

Senator DUCKWORTH. Thank you. Gentlemen, I am closely watching the progress of future vertical lift, mostly because I am personally interested in advancement of rotary-wing aviation, as a rotorhead myself, and also because the Army has made a number of smart decisions as it has developed a program now. I am hoping some of these decisions can be adopted across the DOD [inaudible].

Chairman REED. You broke up, Senator Duckworth. If you could repeat the question.

Senator DUCKWORTH. Okay. I am going to turn my video off, because that seems to be the problem here. I apologize.

I was talking about the future vertical lift, and language I had in last year's NDAA requiring a review of lessons learned and employing open systems architecture in the FVL program. Dr. Schmidt, what are the benefits of using open systems architecture in programs like future vertical lift (FVL), and what barriers do you see to the military services using this approach in future acquisition?

Dr. SCHMIDT. Thank you. I love your question because I am also a very big helicopter person.

Senator DUCKWORTH. Fantastic.

Dr. SCHMIDT. If you look at the way the aviation world has worked, many of the structures and so forth are relatively secret and proprietary. And what we have learned with more sharing across the industry, the whole industry moves faster. So I strongly

recommend that open source designs be made available. And my personal view is that the way the Defense Department should do these things is that the Defense Department should have design studios that design things which are owned by the government, and then that technology that they own is then given to the manufacturers to then develop further. But I would like the government to own much more of its own intellectual property by developing it itself, by funding teams, design teams. I also think that that will allow for faster iteration throughout the primes and their manufacturing cycles.

Senator DUCKWORTH. Thank you. And I am out of time, but if you could follow up with any type of barriers and any recommendations on overcoming barriers, in written form, after the hearing I would appreciate it. Thank you.

Chairman REED. Thank you Senator Duckworth. Senator Scott, please.

Senator SCOTT. Thank you, Chairman. First off, I thank each of you for being here.

General Carlisle, you recently retired. In the roles you had in the military, how concerned were you about, you know, what technology companies were doing, I mean, the theft by Russia and China of technology, the espionage, things like that, and did you feel like you were at a disadvantage as compared to what Russia and China military was doing?

General CARLISLE. Sir, we have the greatest fighting force and the greatest military in the world, and I believe we have the greatest equipment in the world. Some of the programs that I was in, that are now declassified, I was part of the exploitation of some of the capabilities of our adversaries, both the Soviet Union (USSR), at the time, back in the late, great days of the Cold War, and China. And, by far, our equipment is superior to our adversaries. And you can tell that not only from what we got to see but our friends, partners, and allies want to use our equipment as well, because of the quality of it.

I do believe that gaps is knowing because of the theft that occurred. I was in China when I was the commander of PACAF, and we were walking up and down the line looking at their airplanes. I actually got to crawl into a couple of their airplanes, a J–10 and a J–12, and when you looked inside you could tell that it was just—they took stuff from wherever they could steal it, to put it in those airplanes. And the result is that the gap we had, the superiority we had against our adversaries, because of intellectual property (IP) theft, course of action that I talked about in my opening statement, that gap is narrowing. And that is why we have to continue to get innovation out more quickly, because in today's world you just do not maintain——

Senator SCOTT. But then what you just heard, what Dr. Schmidt just said, that we do not even have systems that—you know, you had to put something from one system to put information into another one. I mean, in real time you are not going to win a war if you cannot do some basic things like that, where we do not have the ability to share information rapidly. You know, it just seems to me that we have not used the private sector, and we do not have the relationship with the private sector, for whatever reason. But

China does, and China might because they steal it, but they do have, you know, whether it is AI or things like that, they are going down a path that we are not even—we are going awfully slow in.

General CARLISLE. Senator, you know, I do not disagree with that. I think that is a challenge as we move forward. We do make it work, though. I mean, if you go to the Air Operations Center or the Maritime Operations Center, the Tactical Operations Centers and you see how we pass data, you are right. We have got a long ways to go and we have to get there, especially with the way our adversaries are moving.

You know, the decision advantage, there are two different terms, Fully Networked Command, Control, and Communications, FNC3, or JADC2, which is the Joint All-Domain Command and Control system. That is about passing information. That is connecting sensors of all types, from all varieties, from all domains, from all services, and from allies to the right nodes that can engage in the right nodes, it can do the command and control. And that is the part we have not gotten to yet.

Senator SCOTT. Mr. Smith and Dr. Schmidt, would that be true in your companies? Would you not be able to share data the way the military has inability to share all information? And something that is way more important than how well you run a company.

Dr. SCHMIDT. Well, information is incredibly important. As part of my DIB work, we spent a lot of time on this. Part of the problem here is that the military has systems but does not have software, and the systems have information and the information has to go from one system to the other. So a series of projects, they are generally known as Kessel Run and so forth—they are well known to the staff here at the committee—we are able, with relatively simply programming, to really, really improve the lethality and the usefulness of these systems.

Over and over again, the problem is that the military thinks software is not valuable and it sort of collects it. I propose that anybody who is in charge of a combatant command (COCOM), in fact, any four-star general, should have 50 software programmers to just solve problems. And whenever that has been done, the force productivity has risen very, very quickly. So I used the TRANSCOM example before. It is a relatively straightforward thing to have programmers write the code to take to our enlisted people and have them do something more useful than just copying numbers all day.

Mr. SMITH. And I would add different categories of information require different approaches. One of the concerns I was raising before is when we think specifically about threat intelligence, really the data about foreign cyberattacks on the United States, the information is very much in a set of silos, in the public sector and in the private sector. And I just think it is actually worth pulling out the 9/11 Commission's report, because I think it does speak to us, almost 20 years later. What they said was that the government needed to move from a culture where information was shared only when there was a need to know to a culture of a need to share. And we have to do it with privacy controls. We have got to have the right division between the public and private sectors. But we are only going to understand our threats better if we are doing a

better job of aggregating data and then harnessing things like AI to alert us to what is happening.

Senator SCOTT. Thank you.

Chairman REED. Thank you, Senator Scott. And now via WebEx, Senator Rosen, please.

Senator ROSEN. Thank you, Chairman Reed, Ranking Member Inhofe, and, of course, all of the witnesses for being here today. I really appreciate.

I really want to talk about international standards and emerging technologies, because international standards, they serve as the foundation for the development and the use of emerging technologies. Our global competitiveness, it depends on our participation and in our leadership in setting the standards for the next generation of technologies. That is why last year I helped introduce the bipartisan Promoting the United States Wireless Leadership Act of 2020, to ensure that U.S. has a seat at the table in the wireless standards-setting process.

China has an explicit plan to become a standards-issuing country by targeting emerging technologies, where global rules have yet to be fully defined. For the U.S. to remain the leader in this space, to maintain our national security edge, our response must include working with the private sector, investing in R&D and emerging technologies, coordinating with relevant agencies, and engaging in international standards-setting bodies. And as a former software developer I love the comment that we should have 50 programmers embedded in all these places. Programmers and analysts are key to solving so many critical issues.

But my question is for Dr. Schmidt and then Mr. Smith. Could you talk about the importance and the impact of U.S. participation in the international standards-setting bodies for the development and use of emerging technologies, and how should we, as the government, be coordinating with the private sector to really set those standards for the next generation technologies?

Dr. SCHMIDT. Your diagnosis of the problem is exactly right. It turns out that China now has a deliberate goal of basically participating at a significant level at all of the important standards-settings bodies, the most interesting being 5G Infrastructure Public Private Partnership (PPP), which is the one that sets the 5G standards, where they now have figured out a way to have a majority of the members. So that does not bode well for the kind of values that we care about getting embedded in these standards.

There are quite a few organizations, NTIA and others, that are in charge of these, and I think that this is a good project for the government to get itself organized around which are the ones that are most important, because there are so many. Brad?

Mr. SMITH. I would absolutely second that. First of all, I think it is such an important question because it is easy to overlook just how strategically important it is to the future of American technology for the country to be successful in influencing and helping to set international standards. It is not a case of all technologies being equal, so as Eric mentioned, you have to identify the technologies that we want to prioritize. Different standards are set by different standards-setting bodies, so then one needs to have an engagement strategy. And certainly you need to think about how to

bring together the resources in the Federal Government in a place like the National Telecommunications and Information Administration (NTIA) and in the private sector, and we need to do this by continuing to work with our allies especially.

The Chinese government has established for itself a leadership role. It is going to use its own standards-setting ability for its market to try to influence global standards, and we need to be allied with our partners and working together to ensure that we win the race to influence standards.

Senator ROSEN. Thank you. I am going to build on that with our STEM workforce shortfall, because in order for us to continue to be the most innovative country, to set the standards that we need to, we have to maintain a workforce that can innovate. In the United States we are expected to face a shortfall of nearly 3.5 million skilled technical workers. That is just by next year. To address this shortfall, I introduced a bipartisan bill called the PROMOTES Act, that is going to authorize the Secretary of Defense to enhance the preparation of Junior ROTC students for training and education in STEM fields. I am proud that this bill was signed into law in last year's NDAA, but more needs to be done if we are going to do all the things we need to.

So, General Carlisle, can we talk for a moment about how the Junior ROTC program, how we can leverage that to incentivize, train our high school and college students to enter these emerging technology fields like artificial intelligence, quantum computing, cybersecurity, and so many other spectrums? What role can the military play? How do we get the workforce that we need?

General CARLISLE. Thank you, Senator. I could not agree more. I think our ability to attract the talent and bring them into the STEM career fields, in particular. We, in the Air Force, face—well, actually all services face a severe pilot shortage, less so now, obviously, because most of the airlines have not hired, but that will, I think, come back.

But one of the things is how do we get to those folks that do not know about us. How do we get those communities that do not have the opportunity and maybe do not understand what those opportunities are in the military? Recruiting people, the Junior ROTC program, a very good friend of mine runs the Air Force ROTC program out of Maxwell Air Force Base, and what do we do to attract these folks, to let them know there are opportunities out there, and that the military can open up training opportunities, it can open up different educational opportunities, it can open up career fields to them that they are not aware of.

So I think the military can play a huge part of that, and as was mentioned earlier, I think it is K–12 is where it has to start and then it goes to the world-class universities that we have in this country and how they continue to attract, continue to promote, and continue to be the leaders in their fields. Again, I think the ability to get to the communities, because we have, you know, the incredible population of this country, and a lot of it is they just do not know. They do not know what those opportunities are out there, and I think Junior Reserve Officers Training Corps (ROTC) is a great way to start opening up those opportunities.

We did start, for the flying piece, we started a program with the Civil Air Patrol that would allow folks that could not afford to go get a pilot's license, because it is not inexpensive, at the cost of the program, go get a private pilot's license over the summer and learn about aviation, and then the ability to bring them back in to aeronautics or astronautics or aviation is another opportunity for them that they probably would not know existed beforehand.

So I think it is about making opportunities and getting to the full breadth and width of the American population and offer them those chances.

Senator ROSEN. Well, thank you all. My time has expired but I am excited to work on all of these issues with all of you. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Rosen. Senator Hawley, please.

Senator HAWLEY. Thank you, Mr. Chairman. Dr. Schmidt, let me start with you. I am very concerned about the consolidation of the defense industrial base. This is a multi-decade problem, one that has really accelerated in recent years. And we are seeing this problem now with emerging technologies, the subject of this hearing today, where just a few large companies, like the ones that, frankly, you represent, or have represented and worked for, own a lot of the technology or can buy it up.

Two years ago, the Chairman of the Joint Chiefs and the Secretary of Defense sat right where you gentlemen are sitting and complained about Google, in particular. I was so struck that I went and I pulled the transcript. The Secretary of Defense said, "I am talking about Google and their support to China and their lack of support for the Department of Defense." The Chairman of the Joint Chiefs, General Dunford, said, "The work that Google is doing in China is directly or indirectly benefitting the Chinese military." Then he went on to say, "We are watching with great concern industry partners? work in China, knowing that there is indirect benefit." And, of course, Project Maven is what they were talking about the time but there is also the controversy about Boston Dynamics and the robotics collective.

Here is my question. How can we ensure robust competition so that we have a competitive market for emerging technologies that is not dominated by just a few big firms?

Dr. SCHMIDT. Well, first I am no longer at Google, and I disagreed with the activities that you were describing, and indeed I worked for the DOD during that period, so my personal views are clear. I think there is good news——

Senator HAWLEY. Do you think Google made the wrong decision—sorry, is that what you are saying, Dr. Schmidt?

Dr. SCHMIDT. Let me just leave my statement as what I said.

Senator HAWLEY. Well, I did not hear your statement here on the record now, so just reintroduce it. Why do not you answer my question? Are you saying that you disagree with——

Dr. SCHMIDT. I disagreed at the time with the decisions at Google.

Senator HAWLEY. That the Chairman of the Joint Chiefs and the Secretary of Defense were talking about, just to be clear?

Dr. SCHMIDT. Yes, that is correct.

Senator HAWLEY. Okay.

Dr. SCHMIDT. And it is important to know that during that time I was an employee of the DOD, so my view is clear.

So with respect to—there is good news, that there are plenty of companies that now want to work with and for the military. Part of the problem they have is they are having trouble getting through the valley of death. They have a good idea. They cannot get into the right procurements. They do not have access. The DOD has set up a set of initiatives, DIU being one, and there are a number of other ones that are quite good.

And so I think to the degree you have a concern about concentration around, for example, Google, your best strategy is to have as many touchpoints where private sector innovators can work with the DOD.

I should also note that Google's competitors, Microsoft and Amazon, made very different decisions than Google did during that time.

Senator HAWLEY. Let me ask you, Mr. Smith, speaking of Microsoft, the use of Chinese-made hardware like printed circuit boards, poses a significant cybersecurity concern for the United States. I think some of my colleagues have mentioned this earlier. Does Microsoft use Chinese printed circuit boards in the systems you provide to the Department of Defense?

Mr. SMITH. I would have to go look specifically. We have been diversifying our——

Senator HAWLEY. Well, just before you move on from that, will you do that and get me an answer on that question?

Mr. SMITH. Sure. I would be happy to.

Senator HAWLEY. Great.

Mr. SMITH. I will say, more broadly, two things are important. One is we, like other companies that produce hardware, have been diversifying our supply chain, which means less reliance on China, more focus, including on printed circuit boards, from Taiwan, as well as in other countries in Southeast Asia and Mexico, and even we are looking at the United States itself.

The second thing I would say is for anything that is going to involve national security system, use for, say, the U.S. Army, you know, every component is reviewed by the U.S. Government itself in terms of where we are sourcing it.

Senator HAWLEY. I am glad to hear about your diversification, and I heard your remarks on that earlier. Let me just press you on this point, though. Will you commit to ending Microsoft's use of Chinese printed circuit boards if, in fact, you are still using them?

Mr. SMITH. I would like to learn more. I would be happy to send you a letter and we will give you a commitment. I believe we may no longer be using any printed circuit boards from China, but I would like to go look.

Senator HAWLEY. That would be good. That would be good. If you are, though, will you commit to ending the practice?

Mr. SMITH. I have learned enough over the years that I should be informed by the other employees at our company before I give a definitive answer, but I will be happy, Senator, to give you a definitive answer.

Senator HAWLEY. Okay. You are not going to give me one here today, though, it sounds like.

Mr. SMITH. I would like to give you an informed and definitive answer.

Senator HAWLEY. Uh-huh. Yeah. We hear that a lot before this committee. Would you at least commit to being transparent and notifying DOD about which systems contained Chinese printed circuit boards, if, in fact, you are continuing to use them? Would you give me that commitment?

Mr. SMITH. I believe we already are. If we are not, that is—of course we want to be transparent with Department of Defense (DOD) with all of the components that are going into——

Senator HAWLEY. Okay, good. So yes, you will do that.

Mr. SMITH. Yes, I will do that.

Senator HAWLEY. Okay. Outstanding.

Mr. Chairman, I see that my time has expired. I have got some more questions for you, Mr. Smith, and also for you, Dr. Schmidt, but I will give them to you for the record. Thank you for being here and thanks for your work. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Hawley. Senator Kelly, please.

Senator KELLY. Thank you, Mr. Chairman, and thank you, Dr. Schmidt and Mr. Smith and General Carlisle. And, Mr. Chairman, I look forward to serving on this committee.

And, General Carlisle, in your opening testimony you mentioned that we are lagging behind our adversaries in a number of areas—hypersonics, directed energy weapons systems, and microelectronics. About 18 months ago, the People's Liberation Army (PLA) fielded what is perhaps the world's first operational hypersonic weapon system, DF–17. Has a hypersonic glide vehicle as well, and that vehicle can suppress its entry trajectory and accelerate to Mach 5. Intercepting this vehicle with existing anti-ballistic missile (ABM) technology is incredibly challenging, and we do not currently have a defense against that, as far as I know. It has a range of thousands of miles, putting our assets and our troops and our equipment in Japan and South Korea at great risk.

As a former commander of the Pacific Air Force, how big of a strategic impact is this in the theater?

General CARLISLE. Senator Kelly, it is a tremendous impact. It is a tremendous impact to all the entire joint force and the ability to operate. You have heard before us talk about the ability of the adversary to deny us entry into the space, whether it is by a naval—by air anti-satellite weapons is another case where they deny our ability to use a domain via laser or on orbit or direct descent at us, anti-satellite weapons. So it was a huge impact, and clearly, as I mentioned earlier, where China has come over the last 20 years in their fielding of capability at a pace that is extraordinary, it has changed the dynamic in the Pacific tremendously.

And the earlier question, I think one of the things that it is incumbent upon all of us, and certainly this body and use that have the opportunity to still work in the defense industrial area, is we have to educate the American population on what the Chinese are attempting to do, what they have written they want to do, and what they are blatantly going forward with, that is counter to our

values, our way of life, and our future. The DF–17, the ability to sense where they are, what they are doing, and then defeat them is a tremendous challenge, and sir, we will come back and at a classified level we can talk at a different level of what it did. But, I mean, when you think about our ability operate again via the maritime domain or the air domain or the land domain, it significantly impacted and changed the concept of operations for engagement in the Pacific.

Senator KELLY. Later I would like to talk to you about how do we catch up. You know, how do we build a system, a defensive system, but also how do we match that capability, or exceed it.

General CARLISLE. Sir, I would love to come over and talk to you about it.

Senator KELLY. And I have a couple more minutes. I want to follow up on Senator Hawley's question a little bit, semiconductor technology. And the CHIPS Act appropriated—did not appropriate—authorized about $10 billion to manufacture, to bring that manufacturing capability to the United States. The Taiwan semiconductor manufacturing company has a 5-nanometer chip that they currently make. It is my understanding that Intel and other companies cannot manufacture a 5-nanometer chip.

Can you outline, Mr. Smith, for us just where—and Dr. Schmidt as well—just what technologies, and what is the—and we only have about a minute left—what impact does that have for our country?

Mr. SMITH. Well, I do think you are right to identify this. It creates a weakness and a vulnerability for the country, and I do think a critical issue for the next couple of years is going to require decision-making on how to catch up in that space. Part of it is an issue of innovation, as you identified, the gap. But I think another part does involve investment, and, you know, Microsoft is obviously not in this part of the technology business, but if we are going to bring semiconductor manufacturing back to our shores I do think it is going to require some targeted Federal investments, and it is not going to be inexpensive. The kinds of dollars you were just talking about I think captures well just how enormous it is in terms of cost to build these kinds of fabrication capabilities.

Senator KELLY. Dr. Schmidt?

Dr. SCHMIDT. The CHIPS Act is a very good first step but it is not enough. The 5-nanometer technology at TSMC is the world class. They are now working on 3-nanometer technology, which is allegedly going to be available within 12 to 18 months.

I have often wondered why is it that one group can stay ahead, and the answer is that is year after year of precision and learning and proprietary innovation and so forth, and something which is very hard. Remember that the Chinese had, for 30 years, a goal of catching up to TSMC, and they have required, for example, fabs in China and so forth and so on, and they still have not been able to do so.

So I suggest that what we do is we take American ingenuity, which is profound, with some form of incentive system to sort of close this gap, and put those semiconductor operations, at least foundries, in the United States, and use them for both commercial but also military purposes. It is critical that our military chips be

made in the United States, for the reasons that everyone here would fully understand.

Senator KELLY. Thank you.

Chairman REED. Well, thank you, Senator Kelly, and thank you also for sitting through the hearing. I think you got some practice sitting for hours in a cockpit, which prepared you well for this committee.

Senator KELLY. And alert.

Chairman REED. Senator Tuberville, please.

Senator TUBERVILLE. Thank you, Mr. Chairman. Good morning, guys. I know it has been a long—very quickly, you know, your testimony today, I just hope everybody is listening across the nation. We are in trouble. Our country is in trouble, and it is going to be solved a lot by our technology. Most of us in here went through a little bit of Vietnam and all these wars, these no-nonsense wars that we have had over the years, and we have wasted a lot of money on these wars, and we have gotten behind China. We have not spent enough money, because we have not had it.

But thank you for being here today, and Dr. Schmidt, I enjoyed listening to you. In my former life of coaching I learned a long time ago it is not about the money, it is about organization. And if you are not organized you can throw all the money at it you want, but you are not going to survive. So I really enjoyed hearing that.

You know, in Huntsville, we lead the nation in many categories in technology, so if you have not had a chance to visit, it is the Silicon Valley of the South, I invite you to come.

So just a couple of questions. Mr. Smith, the phrase "American ingenuity" during my lifetime rose, and we all saw it grow and prosper. We thrived in an environment with less regulations, smaller government, risk-taking. Silicon Valley in the '80s and '90s worked much the same way. How do we get that back? How do we get that back to where we can continue to grow, instead of just the big companies? We have gotten away from it, of the smaller companies just being able to innovate and grow with us technology-wise. Because we have got to catch up, somehow, some way.

Mr. SMITH. Well, I think we still live in a country that rewards people with bold ambition and the determination to make that kind of dream come true. And, you know, when I joined Microsoft we had about 4,000 employees. This was 27 years ago. Today we have 165,000. It is a much bigger place, to your point about organizations.

Senator TUBERVILLE. What a country, right? What a country.

Mr. SMITH. Yeah. But, you know, there are days when I still feel like it is the smaller place. I think that is American ingenuity, that spirit of creativity. And one of the interesting things about the tech sector is it is an ecosystem. You know, Eric has talked about this for years. You cannot succeed at a big company unless you work closely with a network of small ones. And I think one of the interesting things about the NDIA is it really is the voice, in so many ways, of the small defense contractors.

I think we should not worry for the need for the government to invest more in large companies, absent, say, things like chip fabrication. What we should look at is where the government can ensure that there is an opportunity for small companies, and then I

would say for everybody across the board, so we can go to the great universities, the community colleges, and basically hire the talent we need.

Senator TUBERVILLE. I had the opportunity to travel all over, and campaigning the last two years in Huntsville, going to 800 or so defense contractors, and, of course, National Aeronautics and Space Administration (NASA), SpaceX, Blue Origin, all of those, and it is amazing the technology that we have. But it is also amazing, you know, what the private sector can do, just going through the new laser technology that you are seeing now, that our soldiers are going to hopefully be able to use in the very near future, and hyper-ballistic missiles. You know, we are behind China. You know, the general was saying we are the best equipped, but we are getting old. Our equipment is getting very old, and we need to do a lot of things with that.

Dr. Schmidt, you say Americans can compete and win on any playing field, and I know a little bit about that. But we have seen China that is willing to cheat to win. They are willing to steal our technology, use our own capitalistic system against us. But I know that there are no shortcuts in winning. So if you want to win you have to put out the work. How do we work as a team better? You know, my question is this country is best when our teammates work together, and our allies work together. Do you think we are doing that very well?

Dr. SCHMIDT. There are parts where we are and in many places we are not. I would urge, collectively, that we identify bipartisan agreement around the areas where we must win. We have mentioned hypersonics multiple times. Frankly, we have to win there. What is our strategy to win? How are we going to get there? We cannot spend 15 years building the first hypersonic weapon while China and Russia are already working on it. We need a different methodology.

So necessity drives the urgency and urgency then drives the outcome. There are plenty of ideas of how to do it. You can do it in a private model in a secure facility. You can do it through the government, what have you. But the urgency should drive it. The 5G issue that I highlighted, the issue of AI leadership. In our AI recommendation we speak about doubling the R&D budget for AI, which these numbers are small relative to the Federal budget, but it would be hugely leveraging. There is a list.

But the bipartisan consensus should be to build a national competitiveness approach, literally globally competitive, all of our technologies to wins, the military benefits and our industrial base wins as well.

Senator TUBERVILLE. Thank you, gentlemen.

Chairman REED. Thank you, Senator Tuberville. Gentlemen, thank you for your extraordinary testimony. It has been illuminating. You have provided us extraordinary insights, but also you have given us a long to-do list. So we appreciate that too, and we look forward to working with you as we approach all these problems.

Thank you. I have got to depart, along with my colleagues, to vote, but I appreciate very much your participation, and again, this

was an extraordinary hearing because of your insights, all of you. Thank you very much.

The hearing is adjourned.

[Whereupon, at 11:48 a.m., the Committee was adjourned.]

○