Dr. Eric E. Schmidt Co-Founder, Schmidt Futures Chair, National Security Commission on Artificial Intelligence Testimony Before the Senate Committee on Armed Services

Emerging Technologies and Defense: Getting the Fundamentals Right February 23, 2021

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 U.S. government must develop a unified strategy to advance and protect the technologies that will underpin national competitiveness in the middle decades of the twenty-first 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.

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 U.S. innovation model has been the envy of the world. The open exchange of ideas and free markets, with targeted

¹ Smart City Index, IMD, 8 (Oct. 2019),

https://www.imd.org/research-knowledge/reports/imd-smart-city-index-2019/#:~:text=The%20Top%2010%20smart est%20cities.and%20Dusseldorf%20(10th).

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

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

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 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.

Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021); see also *First Quarter Recommendations*, NSCAI at 12 (Mar. 2020), <u>https://www.nscai.gov/previous-reports/</u>.

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

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 <u>stay at least two generations ahead</u> 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 U.S. 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 <u>at the Department's current pace of technology integration, the military will not be capable of carrying them out in time</u>. To fight as the military intends to fight in 2030 or 2035, the Department needs to get the fundamentals in place well before then.

⁴ See Testimony of Elsa Kania before the U.S.-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.

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 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

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.

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.

https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf.

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

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),

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
- 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

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).

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.

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.

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

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.

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.

¹² I am encouraged that the FY 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.

My graduate work in computer science in the 1970s and '80s 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.