Strengthening the Role of Digital Technology in Defending the Nation

Written Testimony of Brad Smith
President, Microsoft Corporation

Senate Armed Services Committee
Hearing on Emerging Technologies and Their Impact on National Security

February 23, 2021

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

[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/.

Microsoft CEO Satya Nadella has noted, 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

---

[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.

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. 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

[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.

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 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 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

---

[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.

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 U.S. 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.

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.

---

[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, Nov. 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/.

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*, U.S. 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

[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.

Investment Risk Review Modernization Act (FIRRMA), which authorizes the Committee's review of non-controlling foreign investments. The National Defense Authorization Act for FY2019 requires federal contractors to ban certain telecommunications technologies 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 <u>and</u> 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 payment 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

[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/.

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 U.S. 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. <u>Accelerate the adaptation of commercial digital technology for defense applications</u>.

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 ***<u>use</u>*** 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 ***<u>add</u>*** security layers to commercial technology when required, such as by protecting secret and top-secret workloads and military operations. Third, the government should ***<u>adapt</u>*** 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 infrastructure 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.

---

[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://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.

- *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 U.S. 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 development 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

[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.

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. <u>Pursue a strong and renewed commitment to technology collaboration with our allies</u>.

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. <u>Lead with moral authority and not the strength of technology alone</u>.

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 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 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.

[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.