

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

A Testimony by:

William Carter

Deputy Director and Fellow, Technology Policy Program

January 9, 2018

2118 Rayburn House Office Building

Introduction and Main Points

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

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

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

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

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

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

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

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

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

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

¹ Shirley Kan, "<u>China's Anti-Satellite Weapon Test</u>," CRS Report for Congress, RS22652, April 23, 2007

² Richard D. Fisher, Jr., "<u>China's Progress with Directed Energy Weapons</u>," Testimony before the U.S.-China Economic and Security Review Commission hearing, "China's Advanced Weapons," February 23, 2017

³ U.S.-China Economic and Security Review Commission, "<u>2015 Annual Report to Congress</u>," November 17, 2015, p. 297

⁴ U.S.-China Economic and Security Review Commission, "<u>2015 Annual Report to Congress</u>," November 17, 2015, p. 294

⁵ Bill Gertz, "<u>Ship collisions raise specter of Chinese electronic warfare</u>," Asia Times, August 29, 2017

⁶ Simon Baker, "<u>Which countries and universities are leading on AI research?</u>" Times Higher Education, May 22, 2017

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

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

Investing in Resiliency and Avoiding Conflict

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

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

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

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

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

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

¹¹ Gabriel Popkin, "<u>China's quantum satellite achieves 'spooky action' at record distance</u>," Science Magazine, june 15, 2017

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

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

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

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

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

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

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

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

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

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

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

We Need a National Strategy to Maintain Our Technological Dominance

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

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

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

¹⁷ Dominic Barton, Jonathan Woetzel, Jeongmin Seong, Qinzheng Tian, "<u>Artificial Intelligence:</u> <u>Implications for China</u>," McKinsey Global Institute, April 2017

¹⁶ Elsa B. Kania, "<u>Battlefield Singularity: Artificial Intelligence, Military Revolution, and</u> China's Future Military Power," Center for a New American Security, November 2017

¹⁸ "<u>Total Revenue of China's IC Industry to Grow Above Global Average at Annual Rate of</u> 19.86% for 2018, Says TrendForce," BusinessWire, November 9, 2017

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

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

Invest in Long-Term Fundamental Research and Development

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

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

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

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

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

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

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

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

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

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

²¹ Elsa B. Kania, "<u>Battlefield Singularity: Artificial Intelligence, Military Revolution, and</u> <u>China's Future Military Power</u>," Center for a New American Security, November 2017

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

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

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

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

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

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

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

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

Invest in the Workforce of the Future

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

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

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

²³ Cade Metz, "<u>Tech Giants are Paying Huge Salaries for Scarce A.I. Talent</u>," New York Times, October 22, 2017

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

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

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

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

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

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

²⁵ World Bank Global Development Indicators. Retrieved January 7, 2018. <u>https://data.worldbank.org/indicator/SP.POP.TOTL</u>

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

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

Avoid Dogmatic Views of New Technologies like Autonomous Weapons

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

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

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

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

²⁷ Stuart Russell, "<u>Slaughterbots</u>," YouTube, November 12, 2017

²⁸ Sydney J. Freedbert Jr. And Colin Clark, "Killer Robots? 'Never,' Defense Secretary Carter Says," Breaking Defense, September 15, 2016

²⁹ Elsa B. Kania, "<u>Battlefield Singularity: Artificial Intelligence, Military Revolution, and</u> <u>China's Future Military Power</u>," Center for a New American Security, November 2017

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

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

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

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

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

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