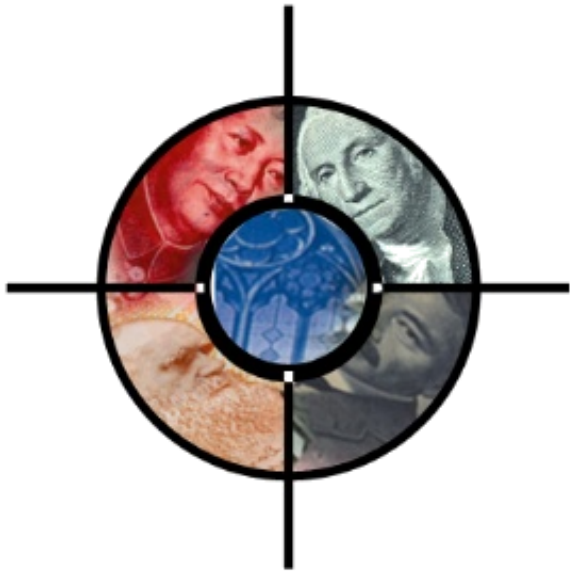
National Security Commission on AI Intelligence

Jan 4, 2020



Schulte-Research

Paul Schulte, MA, MALD
Paul@schulte-research.com
www.schulte-research.com
(+852) 9705 0777

Mirza Muhammad
mirza@schulte-research.com

Phuang Jing Yi
jy@schulte-research.com

Introduction

No.	How important is being at the forefront of AI & what are the implications of using AI for defense
1	Broad mandate to examine artificial intelligence (AI) through the lens of national competitiveness: • Understand and act on trends in international cooperation and competitiveness • Look into ways to foster greater investment in basic and advanced research • Identifying potential risks of military use, ethical concerns • Establishment of data standards
2	Most urgent challenges and the most transformative opportunities presented by AI for our national security: • Foreign threats to our national security in the current AI • Relationship between AI and economic competitiveness as a component of national security • Ethical considerations in fielding AI systems for national security purposes

Schulte Research

The challenge in front of us

No.	What is needed to advance in the field of AI technology
1	Increase in competition: • China, a strategic competitor, has declared its intent to become the world leader in AI by 2030 as part of a broader strategy that will challenge America's military and economic position in Asia and beyond. • Strategic risk demands that our government and society find common purpose and face these challenges with the same imagination, decisive action
2	Are optimistic that the education system(universities & firms) will cooperate and support research and development into AI.
3	Hopeful that public officials will support AI investments to protect our national security and sustain our economic prosperity.

Schulte Research

What is AI

No.	Importance of AI and what facilitates advancement
1	These systems are improving as the state-of-the-art shifts from expert systems based on explicit models to machine learning systems that can learn from experience and improve their performance, including those that can learn from sufficiently large and robust data sets.
2	• Current AI is Narrow AI: machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets. • Responsibly utilizing today's narrow AI applications as they apply to national security will pave the way and help prepare us for greater human-machine collaboration and machine-autonomy in the future
3	Machine Learning: • AI has shifted from an era of reliance on explicit models created by experts to an era of statistical machine learning where engineers create statistical models with the capacity to be trained to perform within specific problem domains given exemplar data. • This has been possible due to Deep Learning. Learning from data, DL can solve problems never before solvable, or with a level of performance never before achievable.
4	Technical Core:. • Labeled and curated data enables much of current machine learning used to create new applications and improve the performance of existing AI applications. • Underlying hardware provides the computing power to analyze ever-growing data pools and run applications.
5	AI ecosystem: • Ecosystem of support in place including laws, funding, institutions, policies, talent, intellectual property protection, supply chains, and counter-AI defense.

WHY DOES AI MATTER?

No.	
1	• In the past, many AI projects have been discarded. Now, times have changed and many of the techniques, algorithms, and theories developed in the past are now paying dividends because of breakthroughs in computational power, cloud computing, the availability of massive amounts of training data, improvements in machine learning algorithms, and mobile connectivity.
2	• AI will drive waves of advancement in commerce, transportation, health, education, financial markets, government, and national defense. • Nation with the most resilient and productive economic base will be best positioned to seize the mantle of world leadership.
3	• AI is "dual use" technology—usable for military and civilian purposes. • Tech focusses on Deep fakes. Deepfakes—computer generated video or audio so sophisticated that it is indistinguishable from reality—produce harmless entertainment (like apps to superimpose your head on the bodies of a movie character), but could also be used to slander an individual or interfere in our political process.
4	Information Operations and "Deep Fakes": • Deep fake technology could be used against the United States and U.S. allies to generate false news reports, influence public discourse, erode public trust, and attempt to blackmail diplomats. • Media Forensics (MediFor) project, which seeks to "automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media."

HOW COULD AI ADVANCE NATIONAL SECURITY?

No.	Uses of AI
1	• AI-enabled tools and systems can help protect our borders, detect and combat malicious cyber operations, safeguard our critical infrastructure, and respond effectively to natural disasters. • Capability to process large amounts of data enables real-time risk assessment and response, and provides tailored situational awareness to first responders. • AI algorithms can sift through vast amounts of data to find patterns, detect threats, and identify correlations.
2	Military uses: • Cooperation with private sector technologies: Private sector technologies give all types of actors access to what were once only government capabilities. Our national security agencies will need to understand the motivations and technical capabilities of adversaries––states, terrorists, and criminals––who may use AI to spy on us or do us harm. • Military could use AI-enabled machines, systems, and weapons to understand the battlespace more quickly; develop a common joint operating picture more rapidly; make relevant decisions faster. • Algorithmic warfare. Algorithmic warfare will pit algorithms against algorithms in a contest dominated more by the speed and accuracy of knowledge and action than traditional factors such as force size, levels of armament, or the range of weapon systems.
3	Lethal Autonomous Weapon Systems (LAWS): • AI will foster a new generation of semi-autonomous and autonomous combat systems and operations

Schulte Research

Military AI Integration Challenges

No.	Why is AI apt to be used in National Security
1	• Overarching Ideas: What an adversary could do with AI, and what consequences an AI system could have if employed without safeguards, irrespective of who wields the technology.
2	**Erosion of U.S. military advantage:** • Strategic competitors, led by China and Russia, want to use AI-enabled autonomous systems in their military strategies, operations, and capabilities to undermine U.S. military superiority and conventional deterrence.
3	**Strategic stability at risk:** • Global stability and nuclear deterrence could be undermined if AI-enabled systems enable the tracking and targeting of previously invulnerable military assets
4	**The diffusion of AI capabilities:** • Likelihood of reckless and unethical uses of AI-enabled technologies by rogue states or non-state actors is increasing as AI applications become more readily available. Many of the algorithms and applications available in the public domain will have beneficial uses, but may also be utilized for malign ends.
5	**Spread of Disinformation:** • AI will accelerate the already serious threat of cyber-enabled disinformation campaigns, including false-flag efforts. It will enable deepfakes

Schulte Research

Military AI Integration Challenges

No.	Why is AI apt to be used in National Security
5	**Erosion of individual privacy and civil liberties:** • While citizens' data can be used for lawful and legitimate purposes, the proliferation of new data sources–such as those generated through smart cities or smart policing–increases the risk of human rights abuses or violation of individual privacy.
6	**Accelerated cyber attacks:** • Intelligent malware will autonomously find and exploit system weaknesses, play offense and defense at the same time, and smartly target specific systems.
7	**New techniques bring new vulnerabilities:** • AI systems could be rendered ineffective if security is not built into AI systems from the beginning. Without trust and reliability, users will lose faith in AI's utility.
8	**The danger of accidents:** • Some nations or actors may lower their safety and reliability standards and adopt AI-enabled technologies before they are ready, increasing the potential for mistakes, misperception, and unintended consequences.

Schulte Research

Uncertainty & Debate

No.	Why is AI apt to be used in National Security
1	• Defense experts urge the United States to move more quickly to field AI-enabled weapons systems and other capabilities, once the technology is ready, in light of growing international threats and the possibility that AI-enabled systems could save American lives and reduce civilian casualties.
2	• Some tech workers, concerned that their efforts will be used for military purposes, have called on their employers to limit the scope of their business with the Department of Defense (DoD) or avoid it altogether. • Tech firms are establishing ethics committees to develop guidelines for fielding. AI, protecting privacy, sharing data, and weighing whether or not to do business with the U.S. government or with countries that use AI to oppress their citizens.

Schulte Research

Alternative Visions of the future

No.	Aim/Purpose of this field of work
1	• Hope AI can free people from dangerous and monotonous tasks so that more people can pursue meaningful and creative work
2	• AI empowered systems will be used to diagnose disease and improve our health, forecast and improve our responses to natural disasters, and fuel scientific discoveries across all fields.
3	**Dangers:** • Avoid a future where AI contributes to a world of greater centralized control; empowers authoritarianism; is utilized as an instrument to repress dissent and impose conformity. • China is using AI to build a dystopian surveillance state, and aspires to create social credit systems that assign people to "blacklists" based on who they communicate with, where they travel, what they buy, and how they use their mobile phones. • China is leveraging facial recognition technology to identify and repress its minority populations.

7 basic principles

No.	To maintain a balance between AI advancement and national security
1	**Global leadership in AI technology is a national security priority:** • While American companies play a significant role in advancing AI research and development, the government retains a core responsibility to steer advancements in ways to protect the American people and foster basic research environment.
2	**Adopting AI for defense and security purposes is an urgent national imperative:** • In light of the choices being made by our strategic competitors, the United States must also examine AI through a military lens, including concepts for AI-enabled autonomous operations
3	**Private sector leaders and government officials must build a shared sense of responsibility for the welfare and security of the American people:** • The government must strengthen industry by articulating clear standards and policies for responsible use, rebuilding trust through greater transparency, and offering a vision of a shared purpose.
4	**People are still essential:** • America needs to encourage that talent to come, contribute, and stay. Within government, recruiting, training, and retaining AI-talent will be essential to maximize AI's potential.
5	**The power of free inquiry must be preserved:** • The U.S. must protect our intellectual property and sensitive technology • Ensure that American technology and innovation is not exploited to advance adversaries' militaries or undertake human rights abuses.

Schulte Research

7 basic principles

No.	To maintain a balance between AI advancement and national security
6	**Ethics and strategic necessity are compatible with one another:** • Ethical imperative to accelerate the fielding of safe, reliable, and secure AI systems that can be demonstrated to protect the American people, minimize operational dangers to U.S. service members, and make warfare more discriminating, which could reduce civilian casualties. • Everyone desires safe, robust, and reliable AI systems free of unwanted bias, and recognizes today's technical limitations.
7	**The American way of AI must reflect American values :** • The U.S. military must find ways for AI to enhance its ability to uphold the laws of war and ensuring that current frameworks adequately cover AI.

Schulte Research

Concerning trend lines

No.	To maintain a balance between AI advancement and national security
1	R&D: China has overseen a 30 times increase in its overall R&D funding from 1991 to 2015, and is projected to surpass the United States in absolute R&D spending within 10 years.26 U.S. federal investment in AI R&D has increased only marginally, as we discuss in greater detail below. Incrementalism will not assure U.S. leadership
2	Increase in competition: Chinese tech firms have reached enormous scale and are poised to become leaders in applied AI, excelling in numerous commercial AI applications, including healthcare,education,ande-commerce.28 Some of these applications may pose national security risks.
3	Military-civil fusion: China is intensifying efforts to exploit civilian and commercial developments in AI and leveraging a growing number of companies to advance Party-state and military purposes.
4	Military threats: China and Russia each have established research and development institutes to advance their military applications of AI, akin to the Defense Advanced Research Projects Agency (DARPA).
5	Talent drain: The United States is facing new competition for global STEM talent, especially in AI where there is a critical shortage of expertise. China is undertaking an active effort to recruit global AI talent and persuade Chinese nationals working abroad to return to China.

America's Advantage

No.	Advantages
1	U.S Universities remain top centers for AI research ● The US continues to attract, train and retain top talents for its companies and labs ● 80%~ of international computer science PHDs trained in the US, including those from China, stay in the country post graduation
2	American companies remain world leaders in AI research and some areas of applications ● ¾ world's top 100 AI startups are located in the US ● Home to >2,000 AI Startups, twice the amount of "nearest competitor", half are unicorns – private companies valued >1 billion USD
3	Authoritarian regimes amass and centralize data with little regards to privacy protections ● Have greater propensity to issue centralized AI development plans backed by government funding and are more risk tolerant in fielding AI-Systems quickly without the same standard of ethical and legal safeguards that constrain democracies
	Technical advantage of access to larger data may be overstated as data will have diminishing returns as algorithms improve and is supplemented by synthetic data ● i.e. China's data pool gives it an unsurpassed advantage in understanding Chinese consumer habits, but may not confer wider advantage ● i.e. Russia's battlefield testing of robotic systems on behalf of a ruthless dictator in Syria and the Chinese Communist Party's creation of a massive AI-enabled surveillance state are signs of governments that fear their own people, do not trust their soldiers, and seek technical solutions to centralize power.

State of AI in US Government

No.	Description
1	White House's 2019 Executive Order on Maintaining American Leadership in Artificial Intelligence is a strategic guidance that acknowledges AI as the core for national security ● Members of Congress have filed >30 AI bills in the last 5 years
2	Military ● >100 AI projects underway in Department of Defense (DoD) ● Project Maven narrowly focused the use of AI to detect, classify, and track objects on video streams so human analysts do not have to stare at screens for hours on end
3	Energy ● Established AI office to coordinate and ensure AI researchers have access to government data models and high-performance computing resources
4	AI poses a tough problem due to its nature of mostly commercial use and does not fit the traditional paradigm of a technological development driven by national security needs and federal dollars ● DoD adopting commercial technology for military use ● Today's AI leaders and biggest funders can be found in universities, startups, and big tech firms and is no longer limited to federal research
5	Reversal of Cold War Paradigm whereby government technology are reversed engineer into commercial sector, the opposite holds true now as trying to integrate AI into existing government infrastructure and technology, which are decade old is a major challenge ● The government depends on the commercial sector, while the AI industry, far from depending on government business, often sees government regulations and bureaucracies as hindrances to their business models and therefore an unworthy pursuit ● Many of the gains from AI-enabled systems can only be realized through transformation of organizational structures and business processes; the inherent rigidity of government in this respect poses a major obstacle

Five lines of effort of maximising AI for the US Government

No.	Description
1	Invest in AI Research and Development
2	Apply AI to National Security Missions
3	Train and Recruit AI Talent
4	Protect and Build Upon US Technology Advantages
5	Marshal Global AI Cooperation

Schulte Research

Invest in AI Research and Development – (1/3)

No.	Description
1	R&D in the US has always been driven by a triangular model of government agencies, universities and private companies since Cold War ● Commercial sector is key for AI research now, however investments are necessary but insufficient for sustaining US advantage ● Government retains a critical role, need to support both basic research and research dedicated for national security ● US AI leadership may be at risk sooner than expected due to lack of government support and planning, may mean US need to buy tech elsewhere, potentially off China
2	Federal R&D funding for AI has not kept pace with the revolutionary potential it holds or with aggressive investments by competitors. Investments that are multiple times greater than current levels are needed. ● Requested FY 2020 federal funding for core AI research outside of the defense sector grew by > 2% from FY 2019 ● In the last five years, federal R&D funding for computer science (which houses AI) increased by 12.7%, barely sustaining a field in which tenure track positions grew by 118% over the same period ● While the Chinese government has made ambitious public commitments to technology megaprojects, the United States has returned to pre-Sputnik levels of federal R&D funding as a percentage of GDP with a proposed 5% cut to R&D funding (and 10% in basic research) in the FY 2020 budget ● The United States now trails nine nations on the measure of total R&D expenditure as a percentage of GDP
3	Increased federal R&D Funding could spur the development of: ● core AI technologies, such as unsupervised or self-supervised ML, AI systems with greater common sense, and AI inspired by neuroscience; ● AI systems that are safer, more robust, and resistant to attack; ● AI techniques to accelerate progress in important science and engineering problems, such as slashing the time needed to discover advanced materials; ● cloud infrastructure, labeled training data and other resources for AI researchers; ● next generation hardware, dedicated chips, and novel computing paradigms needed to fuel AI; ● the workforce needed to develop and use AI effectively.
4	National Science Foundation (NSF) manages 85% of federal funding for computer science research, NSF budget for basic research need to double

Invest in AI Research and Development – (2/3)

No.	Description

5	Untapped opportunities exist to build a nationwide AI R&D infrastructure and encourage regional innovation "clusters." Such AI districts for defense would benefit both national security and economic competitiveness.
	● US government considering range of organizational models that could accelerate R&D nationwide
	● NSF expects to launch six institutes in 2020. Other ideas include:
	  ● Establishing an entity within the NSF analogous to the National Cancer Institute,
	  ● A structure resembling the National Institutes of Health to coordinate research and set standards;
	  ● or an interagency AI effort akin to the National Nanotechnology Initiative
	● Economic trends suggest that people and firms will be drawn to geographic "clusters," such as Silicon Valley.
	  ● E.g. Canada has taken a nationwide approach by spreading AI research centers across Edmonton, Toronto, and Montreal
	  ● E.g. The new NavalX Tech Bridges program and the Navy Surface Warfare Center in Crane, Indiana are promising efforts to build such tech hubs

6	The U.S. government should implement more flexible funding mechanisms to support AI research. Business as usual is insufficient.
	● Exploring alternative funding
	  ● i.e. mid-career faculty awards for AI researchers could encourage professors to remain in academia, rather than jump to industry, at a typically productive point in their careers.
	  ● i.e. Subsidies to universities for AI degree development at the undergraduate and graduate levels, and for certifications in AI and advanced computing, could expand the talent pool.
	  ● i.e. Expanded fellowships for graduate and postgraduate researchers would help develop more future professors.

Invest in AI Research and Development – (3/3)

No.	Description
7	The U.S. government must identify, prioritize, coordinate and urgently implement national security-focused AI R&D investments. ● Government investments in AI research should put a premium on issues that are especially relevant to national security missions that the commercial sector may not have incentive to prioritize ● E.g. In defense and intelligence contexts, labeled data may be in short supply, requiring algorithms that can learn from limited or synthetic data ● E.g. Greater need for tactical computing, for operators who are deployed at a distance from centralized resources, in a contested environment with only intermittent communications links ● E.g. The degree of robustness of the AI systems that DoD and the IC need exceeds what is commonly available on the commercial market. To ensure robustness, fundamental research into the science of validating AI technologies is critical ● E.g. As deepfakes become more difficult to detect, research into digital forensics will become even more important
8	Bureaucratic and resource constraints are hindering government-affiliated labs and research centers from reaching their full potential in AI R&D ● DoD's federally funded research and development centers (FFRDCs), where a lot of the most critical, mission-focused AI R&D is happening, are limited by legislative caps on funding and staffing ● The Government Accountability Office found that the current ceiling "significantly constrains" DoD's use of these research centers, and that demand for their services is "significantly greater" than what the legislation allows. ● Department officials reported that "FFRDC related work must be deferred to later years when these limits are reached, since there are no other legally compliant alternatives capable of fulfilling these requirements." ● Red tape in the DoD-owned lab network slows its ability to innovate. Layers of management and long approval processes lead researchers to choose older hardware and software for their work, because these can be obtained more quickly than the best products available. ● Such issues create risks that DoD labs will fall behind the curve of current AI research and development

Apply AI to National Security Missions – (1/2)

No.	Description
1	To remain competitive, the U.S. government must accelerate efforts to apply AI and rethink military doctrine, strategy, organization, budgeting, acquisition, talent management, tactics, training, and infrastructure ● AI can process information and react at superhuman speed, providing an advantage in missions where speed is critical, such as cybersecurity or missile defense. ● In electronic warfare, cognitive systems could autonomously detect and respond to signals jamming ● AI-enabled autonomous systems can also operate with superhuman endurance ● E.g Around-the-clock overhead reconnaissance. In anti submarine warfare, an unmanned vessel could navigate the open sea and hunt adversary submarines for months at a time ● AI can help scan vast quantities of data to provide options to decision-makers ● E.g prioritizing maintenance needs or selecting which forces and equipment to send into battle.
2	Implementation of the government's security strategies for AI is threatened by bureaucratic impediments and inertia. Defense and intelligence agencies must urgently accelerate their efforts ● On paper, the government clearly acknowledges the importance of AI for national security ● The National Security Strategy, the National Defense Strategy, DoD's AI and Digital Modernization strategies, and the Intelligence Community's AIM Initiative all recognize AI as a transformative technology ● However, it is not clear that these top level beliefs and strategic priorities have been fully embraced by departments and agencies. ● Without clear communication linking vision to organizational change, adoption will stall and AI could be consigned to a series of niche applications, or dismissed by skeptics as the next tech fad to be waited out
3	Pockets of successful bottom-up innovation exist across DoD and the IC. These isolated programs cannot translate into strategic change without top down leadership to overcome organizational barriers. • Estimated >600 active AI projects across DoD • Though the projects are promising, DoD is struggling to shift bottom-up experiments into established programs of record. Individual programs are not creating a critical mass for organizational change

Apply AI to National Security Missions – (2/2)

No.	Description
4	AI adoption and deployment requires a different approach to acquisition. ● DoD is struggling to access the best AI technology on the commercial market. Many leading commercial AI firms are small, far from Washington, D.C. and are not consider the government market a priority. ● Traditional acquisition approaches have also made DoD an unattractive business partner for many top commercial AI firms, especially small and medium-sized businesses ● DoD has developed some innovative approaches, including promising Air Force partnerships with MIT and Army partnerships with Carnegie Mellon University. Services also utilize Rapid Capabilities Offices, and budget has grown ● The problem is that such efforts have not been scaled up, and DoD continues to over-rely on niche organizations and institutional workarounds ● Until the government overcomes these challenges, it will miss out on timely access to cutting-edge commercial breakthroughs and top AI talent
5	Rapidly fielding AI is an operational necessity. To get there requires investment in resilient, robust, reliable, and secure AI systems.
6	AI is only as good as the infrastructure behind it. Within DoD in particular this infrastructure is severely underdeveloped. • Modernizing DoD's IT infrastructure will require significant investments in: • Cloud and computing platforms for data storage, compute resources, network communications, and algorithm development • Treating data as a "strategic asset;" and to build the needed infrastructure and prioritise adoption of new routines to train algorithms for unclassified surrogate data and homomorphic encryption • Purpose-built edge processing and network architectures for AI applications in forward operating missions, including in harsh environments where communications may be disrupted
7	The U.S. government is not adequately leveraging basic commercial AI to improve business practices and save taxpayer dollars. Departments and agencies must modernize to become more effective and cost-efficient • Proven commercial AI solutions can make back-end processes such as human resources, financial management, contracting, and logistics more efficient and cost-effective across large organizations

Schulte Research

Train and Recruit AI Talent – (1/2)

No.	Description
1	National security agencies need to rethink the requirements for an AI-ready workforce. That includes: • Extending familiarity with a range of relevant AI technologies throughout organizations, • Infusing training on the ethical and responsible development and fielding of AI at every level, and; • Spreading the use of modern software tools.
2	National security organizations must have AI workforces capable of performing six functions: 1. Planning and executing an organization-wide strategy; 2. Purchasing and maintaining software and hardware infrastructure; 3. Managing and analyzing data; 4. Developing software when necessary, for unique needs; 5. Performing verification, validation, testing, and evaluation; and 6. Deciding when and how to employ AI tools.
3	DoD and the IC are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills. Four near term actions can help: • First, the military reserve components should develop a tracking system for civilian employment and accompanying skills, to better understand what skills are already in the reserve forces. • Second, DoD and the IC should reward employees for learning AI-relevant skills by paying bonuses for completing courses. The U.K. Royal Air Force has introduced a pilot program along these lines • Third, the Armed Services Vocational Aptitude Battery Test should include measurements of computational thinking required for AI software development proficiency. The Air Force is currently exploring integration of a computer language aptitude test to identify potential developers • Finally, Services should treat coding like a foreign language—by allowing service members to test for proficiency, and rewarding proficiency with incentive pay. The Air Force is already developing such a program

Train and Recruit AI Talent – (2/2)

No.	Description
4	The U.S. government is not fully utilizing civilian hiring authorities to recruit AI talent. Agencies need to make better use of pipelines for people with STEM training
5	Expanding AI-focused fellowships and exchange opportunities can give officials and service members access to cutting-edge technology, and bring talent from our top AI companies into federal service • The military sends a small percentage of uniformed officers to training with industry programs, and DoD and other agencies also encourage civilian rotations in companies, typically for one or two years • These could be increased and focused on AI-relevant fields
6	The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates • Two realities about the American AI talent pool have become clear: 1. Colleges and universities cannot meet the demand for undergraduate student interest in AI and computer science generally 2. The American AI talent pool depends heavily on international students and workers. The US global competitiveness hinges on the ability to attract and retain top minds from around the world

Schulte Research

Protect and Build Upon US Technology Advantages – (1/2)

No.	Description
1	Certain features of the current geopolitical and technology landscape are straining America's ability to institute a coherent and effective technology protection regime: • The nature of AI technologies makes the protection of those technologies for national security very difficult. AI research has been largely decentralized and industry-driven; as a result, knowledge is more diffuse and accessible than historical breakthrough technologies such as nuclear or stealth • Open access to AI research is a strong norm in computer science. Even if restrictions were placed on AI products or services, much of the underlying code is publicly available • The United States and China have close linkages in the field of AI, including constant exchanges of people, research, and funding. Chinese AI researchers train at U.S. universities. American cities host Chinese AI research centers, and major U.S. companies have research ventures in China • Chinese venture capitalists have invested in American AI start-ups, and vice versa. At the same time, China takes advantage of the openness of U.S. society in numerous ways––some legal, some not––to transfer AI know-how. U.S. intelligence agencies confirm that the "targeting of national security information and proprietary technology from U.S. companies and research institutions will remain a sophisticated and persistent threat • America's research universities thrive by welcoming top minds from around the globe. At the same time, universities and other research institutes are vulnerable to foreign exploitation and other forms of influence by strategic competitors, notably China.
2	The U.S. government should continue to use export controls––including multilateral controls––to protect specific U.S. and allied AI hardware advantages, in particular those in semiconductor manufacturing equipment • About 90 percent of the SME industry is located in the United States, Japan, and the Netherlands, giving that small group of allies a major advantage • Controls to preserve U.S. and allied advantages in SME could ensure that U.S. and allied country firms retain a dominant position in the global semiconductor market, including in advanced hardware capabilities
3	Traditional item-based export controls and narrowly-scoped foreign investment reviews are by themselves insufficient to sustain U.S. competitiveness in AI 1. The past decade has seen an explosion of Chinese investment in U.S. AI companies: from $1.5 million in just one deal in 2010, to

Schulte Research

Protect and Build Upon US Technology Advantages – (2/2)

No.	Description
3	Traditional item-based export controls and narrowly-scoped foreign investment reviews are by themselves insufficient to sustain U.S. competitiveness in AI • The past decade has seen an explosion of Chinese investment in U.S. AI companies: from $1.5 million in just one deal in 2010, to $514.6 million across 27 deals in 2017. • Continued implementation is necessary, and CFIUS should consider establishing a permanent review structure for AI-related investments. The Treasury and State Departments should also continue working with allies and partners to develop their own investment screening programs to prevent adversaries from migrating malicious investment strategies from U.S. to allied markets
4	The United States must continue leading in AI-related hardware, and ensure the government has trusted access to the latest technologies • DoD's existing access to trusted hardware trails several generations behind commercial state of the art. • China has established a National Integrated Circuit Investment Fund to improve its hardware industry and increase self-sufficiency, investing over $100 billion in the next decade
5	Law enforcement and academic leaders can and should find common ground on preserving an open research system while reducing security risks from foreign government-directed activity on American campuses • The Commission is examining a number of ideas, including the role of an interagency task force on academic espionage, as proposed in recent legislation; • heightened scrutiny during the visa process for Chinese researchers with certain risk indicators, such as ties to the Chinese military; • security classification options for federally-funded AI research programs; • options for foreign students to remain in the United States after completing their studies; and • ways for universities and the IC to have a constructive dialogue aboutpotential threats

Schulte Research

Marshal Global AI Cooperation – (1/1)

No.	Description
1	As AI becomes a focus of multilateral bodies like the United Nations and the Organization for Economic Cooperation and Development, the Commission is considering ways to build coalitions that can advance U.S and allied interests and values • Also considering AI-related diplomatic discussions with rivals such as China and Russia, in areas such as AI safety and AI's implications for strategic stability
2	The United States must enhance its competitiveness in AI by establishing a network of partners dedicated to AI data sharing, R&D coordination, capacity building, and talent exchanges • DoD's existing access to trusted hardware trails several generations behind commercial state of the art. • China has established a National Integrated Circuit Investment Fund to improve its hardware industry and increase self-sufficiency, investing over $100 billion in the next decade
3	AI presents significant challenges for military interoperability. If the United States and its allies do not coordinate early and often on AI-enabled capabilities, the effectiveness of military coalitions will suffer • The Five Eyes alliance is a good place to start, because the United States can leverage existing technical cooperation and information sharing agreements. • The Five Eyes Technical Cooperation Program recently embarked on an AI Strategic Challenge, a three year effort focused on AI applications for allied militaries
4	U.S. diplomacy should be open to possible cooperation with China and Russia on promoting AI safety and managing AI's impact on strategic stability
5	The United States should lead in establishing a positive agenda for cooperation with all nations on AI advances that promise to benefit humanity

Schulte Research