US Leadership in Artificial Intelligence

Matthew Rock, Yixin Lin

May 2018

Contents

1 Executive summary

This white paper argues that the United States government should pursue two simultaneous policy objectives related to artificial intelligence (AI).

AI is critical to US national security and economic dominance.

- **National security**: The development of advanced AI can give a nation or subnational terrorist group a decisive edge in warfare, which would threaten US military supremacy. Since the US's homeland defense and foreign policy depend on military superiority, failing to maintain leadership in AI would threaten domestic security. The US must credibly lead in AI capabilities in order to effectively lead the regulation of AI weaponry on the global stage.

- **Economic dominance**: AI technology has the power to vastly increase efficiency across almost all industries, while also potentially threatening the jobs of millions of individuals due to automation. The US must lead in AI technology to enjoy the power of passing policies that soften the blow of job loss while still enjoying vast efficiency gains.

The US should ensure AI leadership through policy.

- Attract and retain the best foreign researchers who specialized in domains related to AI–computer science, mathematics, statistics, and electrical engineering.

- Increase funding to the National Science Foundation to increase the quantity of university research.

- Build public computer infrastructure to make advanced AI development equipment available to a wider number of individuals.

- Forge public-private partnerships to combine public interests and funding with private sector technical expertise.

- Fund a NASA-like artificial intelligence agency to employ some of the nation's best researchers to build AI exclusively for the public interest.

The US should establish an AI regulatory body.

- The US must establish an AI regulatory body composed of lawmakers, ethicists, technologists, and other interested parties.

- The regulatory board would be tasked with two broad powers:

    - Decide on ethical matters pertaining to the use and development of AI.
    - Regulate corporations in both the public and private sector in their use and development of AI.

In sum, the effective combination of AI promotion and regulation would enable the US government to cement its leadership in AI while ensuring ethical development and safe, responsible use in the US.

About the authors

Yixin Lin earned a Bachelors of Science in computer science from Duke University, graduating *magna cum laude* and Phi Beta Kappa. He has done research on reinforcement learning at Google Brain and facial recognition at Facebook Applied Machine Learning, and in deep learning and computer vision at the Carin lab at Duke and as part of the AMALTHEA program. Yixin also worked as a software engineer at Gusto as a Kleiner Perkins Engineering Fellow, in venture capital with Contrary Capital and has directed Hack-Duke, the premier hackathon focused on social good. He will join Facebook this fall to pursue machine learning in industry.

Matthew Rock earned a Bachelors of Science in economics and minors in French and statistical science from Duke University, graduating *summa cum laude* and Phi Beta Kappa. During his time in college, Matthew worked as an investment banking analyst for JP Morgan Chase & Co. and as a business analyst for McKinsey & Co. During his sophomore and junior years, he also operated the technology-fashion startup Joyce Technologies, specializing in the development of luxury, technology-enhanced jewelry products. On campus, he worked as a staff writer for the Duke Political Review and led the photography team for Duke's *Towerview Magazine*. Beginning in August, Matthew will be working full-time as a business analyst for McKinsey & Co. in Los Angeles.

Part I
Introduction

2   Objective

The goal of this white paper is twofold. First, we hope to convince lawmakers to pass policies that ensure America remains the world superpower in AI research, which will allow the US to effectively lead global discourse on regulation and ethics of AI. Second, we hope to convince lawmakers to set up an AI Regulatory Board to decide on normative issues in the application of AI and regulate AI development in both academia and industry.

3   Background

3.1   Artificial intelligence

Artificial intelligence (AI) is the science of making computers "smart". Specifically, recent advances in the subfield of *machine learning* (ML) has led to a renaissance in AI development, equipping computers with the ability to see, hear, and think more powerfully and enabling a whole host of new applications.[5]

This has brought the subject to national attention: according to the Executive Office of the President, AI is an important technology that "have opened up new markets and new opportunities for progress in critical areas such as health, education, energy, economic inclusion, social welfare, and the environment".[13] However, the rapid development of AI also runs the risk of creating unprecedented societal dangers. For example, according to prominent AI expert Stuart Russell, autonomous weapons powered by AI technology represent "the third revolution in warfare, after gunpowder and nuclear arms," and should be similarly regulated.[17]

3.2   Current landscape

The powerful implications of this technology means that a nation has every incentive to develop and reap the benefits from AI, but that it must do so safely and responsibly. Furthermore, *how* and *where* this technology develops will determine who controls the technology, thereby shaping its societal implications. As of now, the US government has no national initiatives seeking to promote the development of AI, and it has passed no regulations to ensure that it is safely developed and used.

This is in contrast to China,[10] South Korea,[20] or France.[9] Although they have not passed the necessary regulations we will ultimately recommend in this white paper, they have made significant national investments in the technology. The lack of similar investment by the US government represents a missed opportunity to cement US leadership in both capability and, perhaps even more crucially, regulation.

China is especially concerning. While the US has long been the center of AI research and development, over the last five years China has begun to make increasingly aggressive investments in the AI space, threatening America's dominance in the field. Alarmed by Google's success with the AlphaGo project, which demonstrated machine superiority in the ancient Chinese game of Go, China has experienced a "Sputnik" moment.[15]

The Chinese government has since resolved to make its core AI industry generate a gross product of at least $150 billion by 2030 ($1.5 trillion for AI-related industries) Meanwhile, President Xi Jinping has been pushing hard for Chinese technology companies to collaborate with the military in "pursuing new technologies." In fact, this "civil-military fusion" is becoming increasingly important Chinese Communist Party's plans for the development of advanced AI.[8] This has severe implications not just for the competitiveness of the American technology sector but also for American national security and economic leadership.

Part II
Implications

Without intentional policy changes from the US government, the development of AI by other nations will threaten national security and challenge US economic leadership.

4   National Security

4.1   Kinetic warfare

AI has the potential to transform the nature of kinetic war.[4]

AI would enable the creation of fleets of **autonomous drones**, small unmanned aircraft loaded with ammunition and explosives. Coupling thousands of such devices with cheap explosives, data mining, and modern facial recognition allows mass killing with extremely specific parameters– for example, it would be trivially easy to target race, gender, or political affiliation by matching facial recognition with social media information. One could even target specific people, making assassination far less expensive than ever before. The commercial cost of a semi-autonomous drone is decreasing every year: a premium consumer device already costs on the order of a few thousand dollars,[1] an inconsequential cost for a nation-state or even a well-funded terrorist organization.

Whereas nuclear weapons provided an extremely expensive, inexact means of mass destruction, these AI-powered weapons could cheaply and easily kill thousands with surgical precision. Thus, one could refer to a nation with advanced AI weaponry as a **"precision nuclear"** power. As all of the necessary technology already essentially exists, the invention of a fully autonomous drone is extremely close to realization, reflected by the show of increasing alarm in the international community.[2]

The ease of use and cheapness of this technology would enable less well-resourced nation-states and even sub-national terror ists groups to potentially acquire this highly precise destructive power. If AI does enable a commodification of these highly powerful weapons, one would not be able to rely on the classical notion of deterrence to prevent their use. Deterrence only works if the actors are clearly defined and solid expectations are put in place, which would certainly not be the case if AI-powered weapons were easily made and widely available.

Furthermore, in this world of commoditized weapons of mass destruction, the ability of the US to shape the international landscape would be greatly diminished. The US's ability to conduct an expansive **foreign policy** rests on its military superiority, which enables it to police sea lanes, defend the freedom of air space, lead a powerful bloc of allies, and credibly

enforce international agreements and norms.[6] These capabilities, all of which form part of the foundation of American national security, would be severely compromised should the US allow foreign entities to lead in AI and produce AI-powered weaponry.

4.2 Information warfare

AI would vastly improve military capabilities in the domain of **cyber offense**, empowering governments to launch crippling cyber attacks against an enemy's information infrastructure. For example, it can automate the highly intensive and specialized skills required to persistently seek out software weaknesses at all hours and with superhuman speed, to the point where human-operated defenses cannot keep up. On the other hand, AI would equally improve **cyber defense**. AI would be able to "automatically detect software code vulnerabilities and use machine learning to detect deviations from normal network activity".[4] If the US enjoys a leadership position in AI-based cyber security, it would have a significant ability to prevent cyber attacks, secure the US against intelligence breaches, and further enable the US to engage in effective intelligence gathering. If this leadership position falls to another nation, all of these capabilities would be compromised.

Subtler but no less dangerous, modern computer vision can generate ultra-realistic **falsified video content**.[19] For example, one could make a video of a world leader making a declaration of war against another state, which could generate widespread hysteria and damage even if eventually proven false. Even today, technology can generate sex tapes of arbitrary public figures by splicing their photos onto a pornographic video; these videos are known as "deepfakes".[16] Ultimately, advancements of this technology will make it difficult to distinguish fact from fiction and lead to erosion of civic trust. Video will lose its power as a tool for the propagation of truth and only foster confusion and resentment.

4.3 How to respond

One point must be made extremely clear: our call to maintain US leadership in AI is not because we believe the US *should* develop autonomous drones, engage in cyber offense, or exploit ultra-realistic falsified video content. In fact, excessive pursuit of this goal may lead to an arms race situation and engender mass proliferation of these techniques– the worst case scenario. However, we believe the US must come from a position of *credible leadership* in AI in order to effectively lead the regulation of the technology on the global stage. In the same way the US established a clear superiority in biological weapons in order to credibly broker their widespread international ban,[12] so too must it establish AI superiority to ban its most atrocious uses. This will be crucial for American domestic security and ensuring a broader global peace.

5 Economic leadership

In the long term, AI technology will vastly improve efficiency in many sectors of the economy.

5.1 Efficiency gains

In the near future, **autonomous vehicles** enabled by new AI technologies will fundamentally transform transportation: full autonomy not only implies a potential thousand-fold

improvement in vehicular safety, according to Amnon Shashua of Mobileye,[3] but it also will lead to drastic cost reductions in ride-sharing services and potentially a new model of car ownership. For example, instead of purchasing a vehicle, which on average is only used 4% of the time, a consumer would merely use a fully autonomous ride-sharing service. This would amount to vastly improved usage of resources as well as at least a threefold reduction in cost to the consumer and obsolescence of consumer car ownership.[21]

In the **healthcare** space, AI will vastly improve medical diagnosis, drug discovery, and preventative healthcare. For example, targeted healthcare data obtained by wearables and interpreted by AI can catch early signs of disease far earlier than previously thought possible, moving healthcare from a reactive to a proactive regime. AI-powered drug discovery promises a drop in the ever-increasing clinical failure rates plaguing the pharmaceutical industry today by more efficiently simulating chemical reactions and sorting through troves of clinical data.[18]

Modern AI applied to robotics may soon make **manufacturing** automation significantly more versatile and adaptable by broadening the scope of automatable work while simultaneously increasing safety. Current robotics on the factory floor typically are manually programmed and therefore labor-intensive to adapt to new designs, while AI can make this process highly adaptable, easily reprogrammed, and simultaneously aware of its surroundings to reduce workplace accidents.[11,22]

5.2 Threat to employment

However, automation also leads to potentially severely **negative consequences** with regards to human employment. Autonomous vehicles will result in the replacement of over 3.5 million truck drivers and over 1 million taxi or ride-sharing drivers. According to the McKinsey Global Institute, under a moderate-speed adoption of automation technologies powered by AI, 23 million workers will lose their jobs in the United States and 400 million will lose their jobs globally by the year 2030.[14] As AI becomes even more advanced, even white collar jobs such as those in the medical and legal professions, formerly thought to be safe from the tide of automation, may become in large parts obsolete due to rise of machine able to conduct intelligent analysis. This will compel vast numbers of people to switch to professions which still show a demand for humans, such as care providing and technical roles. If managed poorly, this transition could mean the long-term loss of livelihood for million of citizens, place considerable strains on democratic political systems, and upend the normal understanding of the relationship between humans and relationship. Importantly, US leadership in AI enables the US government to **proactively respond to job losses**, since the US can regulate and provide relief for *domestic* companies much more easily than *foreign* companies.

5.3 How to respond

Overall, AI will lead to incredible gains in both efficiency and safety across vast swathes of the economy. At the same time, these incredible gains threaten to be overshadowed by mass unemployment. To ensure continued economic dominance, the US must continue to push for the development of AI within its own borders. Simultaneously, the US must lead in AI in order to effectively regulate the introduction of AI into the economy so as to soften the loss of jobs and ensure a smoother transition between a pre- and post-AI economy. However, if the best AI companies are foreign, the US loses its leverage to regulate AI in its

own country, leaving American jobs at the mercy of foreign markets.

Part III
Recommendations

From the discussion above, two fundamental truths emerge. First, being the world leader in AI is crucial to US national security and economic leadership. In the near future, our current leadership in AI development will be challenged by China, which is pouring unprecedented national investments into the technology. Second, without proper regulation AI can produce deleterious effects with severe societal consequences. Both of these facts call for government intervention. In response to the first fact, the US government should pass effective policies that you foster AI development. In response to the second, the US government should regulate AI development and use to ensure that it serves the broader good of society.

6 Promote AI Leadership

6.1 Talent Retention

The US must attract and maintain the best AI talent from around the world in order to lead the world in AI development. We therefore propose the US government grant visas to researchers in fields essential to AI development–computer science, statistics, mathematics, and electrical engineering. These could be recent graduates of American universities looking to remain in the US or qualified individuals looking to immigrate to the United States for the first time.

One possible policy tool that could be implemented would be adding a new provision to the H-1B application process that would expedite the granting of visas to any researcher in the aforementioned fields. This would essentially be a special H-1B process that removes the applicant from the typical lottery, placing them on a fasttrack to work in the United States.

In addition, another course of action would be to remove the limit on extensions to the H-1B for STEM researchers. Currently, only a single 3-year extension is allowed for an H-1B, bringing the total possible uninterrupted working years in the US to 6. This effectively sets an expiration date on American utilization of these skilled and American-trained workers, unless they manage to successfully petition for permanent residency status. Unlimited extensions would remove this deadline for STEM researchers, enabling a transition to full immigration if desired and ensuring indefinite American talent retention of foreign nationals.

These proposals would have two positive effects. First, the US will get to keep the best STEM researchers for its own companies and universities. Second, this will dramatically increase the number of foreign nationals seeking to study and contribute to American leadership in artificial intelligence, since it will represent a fast track to American residency. This process will continue until foreign nationals meet all excess demand for STEM-based research at American universities and corporations, at which point applicants will begin to be denied.

6.2 Talent Enablement

In addition to ensuring that the best AI researchers are permitted to remain the United States, we propose that the US pass policies that aim to improve the research environment for AI in the US. Only by setting the researchers up for success can the United States maximize the odds of maintaining its leadership in AI development.

First, large corporations have been driving AI development in recent years, causing a brain drain from academic institutions. This has two primary negative effects. First, this deprives the universities of the individuals who can most effectively teach the next generation of STEM researchers, compromising the long-term buildup of STEM research talent in the US. Second, this trend forces the most cutting-edge AI research to be conducted in accordance with corporate interests, which may not be aligned with the interests of the general public. Because researchers at universities have a freer hand to pursue their own research projects, they have a greater incentive to generate research that generally benefits society as opposed to any other specific interest group (Of course, regulation for university research will still be required, which will be discussed in depth below).

6.2.1 Discussion of Policy Options

6.2.1.1 Increase in NSF Grants

One way to mitigate these effects and simultaneously compete with Chinese investment is by increasing funding targeted at AI research. The National Science Foundation, which is the primary federal body that provides universities with funding for basic research, has had its budget cut by 11.2% from 2016 to 2018. As a result, universities will only continue to lose their AI research talent to private corporations that can more effectively compensate researchers and provide them with the resources to pursue interesting (if not independent) projects. We recommend the US government reverse the spending cuts to the NSF budget and index it to inflation. Beyond this, Congress should approve a specific spending allocation exclusively for AI-related research. The size of the fund should be aimed to equip professors with the financial resources that a large corporation would be able to provide them, discounted by the autonomy and independence that such a grant presents to the researcher.

6.2.1.2 Public Compute Infrastructure

Another complementary approach would be to provide public infrastructure for academic research on a scale commensurate with industry. Much of modern AI research requires massive amounts of specialized compute resources, which hinders those outside of major corporations who want to do advanced AI research. In order to expand the number and variety of entities conducting advanced AI research, AI-specific compute resources should also be built and publicly available for scientists to use in academia. One possible benchmark would be to build enough computing infrastructure to provide the top ten research programs with sufficient resources to conduct all of their AI research.

6.2.1.3 Public-Private Partnerships

Currently, AI research in industry is largely insulated from public interest. Furthermore, for all of the attempts to stop talent drain from the universities, a significant portion of AI research talent will likely remain within industry because top technology companies have

the financial resources to compete for the best researchers. One way for the government to tap this talent for the public interest is to pursue public-private partnerships with leading corporations that conduct AI research and produce computing infrastructure. For example, privately-competitive research grants could incentivize industry researchers to conduct experiments aligned with the public good, and industry professionals with relevant expertise could be contracted out to build computing infrastructure for public use.

6.2.1.4 A NASA-like Artificial Intelligence Research Agency

The United States may also benefit from directly employing AI researchers and scientists to conduct AI research. The model for such an agency would be something along the lines of NASA. While private corporations would always have to work partly in line with corporate interests and professors may always pursue projects partly according to personal interest, an agency sanctioned by the US government would be expected to exclusively act in line with the broader public interest. This is not be meant to replace academic or industry research; it is simply meant to augment it.

7 Regulate AI development

AI represents a technology that can bring enormous gains to economic productivity and provide novel, far-reaching technological capabilities. However, as we have briefly discussed, the technology also has the power to unleash severely negative societal consequences if used inappropriately. In the short term, AI-powered technologies like autonomous drones can cheaply and easily equip small groups of individuals with "precision nuclear" destructive power. Furthermore, the development of AI can empower unscrupulous governments to restrict the liberties of their citizens by vastly expanding the effectiveness of their state surveillance apparatus. Millions of American citizens may also face sudden unemployment if rapidly improved AI technology replaces human work roles too quickly without a contingency plan in place. In the long term, as AI capabilities increase and play an increasingly important role in shaping society, misregulation and misuse can lead to negative effects commensurate with its capabilities.

We recommend the US assemble a board of lawmakers, ethicists, technologists, and other interested parties to decide on normative questions related to the development and application of AI. This board should be empowered with:

- The responsibility to decide on normative issues in AI development and application as it relates to the public interest

- The right to decide on appropriate regulation in response to its decisions on normative issues in AI development and application

- The ability to audit any university, corporation, or public agency currently involved in development or use of AI

- The right to impose fines on corporations for failing to meet the standards set by the board in order to provide a real enforcement mechanism for violations of these decisions.

- The right to ban potentially dangerous avenues of research and development in cases of serious negative societal or ethical implications. Examples include unsafe autonomous weapons and navigating possible arms race scenarios.

- The responsibility to interface with other governmental agencies and nongovernmental organizations and to provide recommendations to Congress in coordinating global regulation pertaining to AI.

The oversight board would be able to apply these powers to AI research within universities, corporations, public agencies, and their partnerships. Its purview would be all AI research and development within the United States. However, it also needs to understand the global implications of its decisions and provide recommendations and guidance to the appropriate governmental bodies in order to coordinate international action.

Any entity seeking to conduct AI research must register with the AI regulatory board. Assuming the entity meets the regulations set forth by the AI regulatory board, they will then be granted a license to proceed with their AI use or project. Any entity conducting AI research without having registered will be subject to heavy fines or to being shut down, depending on the circumstances surrounding the unsupervised research. While audits may be periodically conducted, the onus will be upon the entity to submit quarterly reports that accurately describe AI research efforts, like how public corporations report financial health to shareholders on a quarterly basis.

It is in no way the goal of this paper to comment on all of the ethical issues that may arise in the development and use of AI in the coming decades. We merely insist that a sufficiently broad set of distinguished individuals, with varying interests and backgrounds, be assembled to effectively decide on normative issues related to AI, produce appropriate regulation, and have the power of enforcement. While this may slightly increase the burden on those wishing to conduct AI research, we firmly believe that this board can be put in place without severely hampering effective AI research in the US while vastly increasing safety and firmly contributing to the public interest.

References

[1] Skydio shop.

[2] Ban lethal autonomous weapons, Nov 2017.

[3] Self-driving cars will profoundly change the way people live, Mar 2018.

[4] Greg Allen and Taniel Chan. *Artificial Intelligence and National Security*. Belfer Center for Science and International Affairs, 2017.

[5] Taylor Miller Ben Buchanan. Machine learning for policymakers. 2017.

[6] Hal Brands and Peter Feaver. Saving realism from the so-called realists. *Commentary*, 2017.

[7] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*, 2018.

[8] Josh Chin. China looks to close technology gap with u.s., Apr 2018.

[9] Romain Dillet. France wants to become an artificial intelligence hub, Mar 2018.

[10] Jeffrey Ding. Deciphering china's ai dream. 2018.

[11] Peter Dorfman. The future of artificial intelligence (ai) in manufacturing, Apr 2018.

[12] Jeanne Guillemin. *Biological weapons: From the invention of state-sponsored programs to contemporary bioterrorism*. Columbia University Press, 2005.

[13] White House. Preparing for the future of artificial intelligence. *Executive Office of the President, National Science and Technology Council, Committee on Technology*, 2016.

[14] James Manyika, Susan Lund, Michael Chui, Jacques Bughin, Jonathan Woetzel, Parul Batra, Ryan Ko, and Saurabh Sanghvi. Jobs lost, jobs gained: Workforce transitions in a time of automation. *McKinsey Global Institute*, 2017.

[15] Paul Mozur. Google's alphago defeats chinese go master in win for a.i., May 2017.

[16] Brian Resnick. We're underestimating the mind-warping potential of fake video, Apr 2018.

[17] Stuart Russell. Take a stand on ai weapons. *Nature*, 521(7553):415–416, 2015.

[18] Eric Smalley. Ai-powered drug discovery captures pharma interest, 2017.

[19] Justus Thies, Michael Zollhöfer, Marc Stamminger, Christian Theobalt, and Matthias Nießner. Face2face: Real-time face capture and reenactment of rgb videos. In *Computer Vision and Pattern Recognition (CVPR), 2016 IEEE Conference on*, pages 2387–2395. IEEE, 2016.

[20] David Josef Volodzko. South korea's fixation with ai after go master's defeat, Oct 2017.

[21] David Welch. Gm's self-driving cars to be ready for ride-sharing in 2019, Nov 2017.

[22] Mariya Yao. Factories of the future need ai to survive and compete, Aug 2017.