China AI Development Report 2018

China Institute for Science and Technology Policy at Tsinghua University

July 2018

Contents

FOREWORD

Artificial intelligence (AI) has gradually become a reality from a sci-fi dream along with the approaching of the Fourth Industrial Revolution. Since the idea was put forward for the first time in 1956, AI has experienced ups and downs in its development. It is not until the second decade of the 21st century, with the confluence of breakthroughs in core algorithms, rapid improvement of computing capabilities and the availability of massive amounts of digital data, that AI has finally taken a leap forward and grabbed worldwide attention. After AlphaGo's victory over Go player Lee Sedol in 2016, however, the global excitement about AI has been mixed with concerns about its negative implications. Nonetheless, it is obvious that countries around the world have seen AI as a critical arena of international competition and are rolling AI initiatives to secure a favorable position in the new round of technological revolution. From the perspective of China, AI presents a historic strategic opportunity and has a crucial role to play in alleviating the pressure of a future ageing population, meeting the challenges of sustainable development and advancing economic transformation. Since 2015, China has released a series of major national strategic plans including Made in China 2015, Guiding Opinions of the State Council on Vigorously Advancing the "Internet+" Action and the Next Generation Artificial Intelligence Development Plan, which, together with AI policy initiatives of local governments, have propelled the rapid development of AI in the country.

While AI has penetrated all aspects of society, production and everyday life, opinions still vary as to the definition of AI and its current development and future direction. Governments, the public and the business community have all shown a strong interest in this emerging technology. Domestic and overseas research institutes have also paid close attention to China's AI development and published various research reports, but their views and observations and even some basic facts they cited were not entirely objective and less than comprehensive. In view of this, China Institute for Science and Technology Policy (CISTP) at Tsinghua University, Government Documents Center at Tsinghua University School of Public Policy and Management (SPPM-GDC) and Chinese Institute of Engineering Development Strategies (CIEDS), together with Clarivate Analytics, ScientistIn, China Academy of Information and Communications Technology (CAICT) and Beijing Bytedance Technology Co., Ltd., have jointly prepared this China AI Development Report 2018 to provide a comprehensive picture of AI development in China and in the world at large with a view to increasing public awareness, promoting the AI industry development, and serving policy-making. Compared to similar reports, this report has four prominent characteristics:

Forward-looking perspective: This report describes China's AI development on the four dimensions of technological development, market

applications, policy environment and social impact, drawing upon data and survey findings on talent input, paper and patent output, business development, industry financing, national and local policy, public perception and education. On the basis of the comprehensive analysis, it offers reflections on the current stage of AI development and forward-looking insights into future AI development and especially governance challenges.

Domestic and international coverage: This report offers a multi-dimensional comparison between China and developed countries in AI development and analyzes China's strengths and weaknesses and its position in the international AI competition landscape. Meanwhile, it identifies China's regional differences in AI development, market applications and policy environment with the focus on active regions in AI development.

Reliable first-hand data sources: This report uses an AI keyword list provided by Clarivate Analytics based on literature-based keyword analysis and validation by AI experts, which provides a unified standard for data search in all parts of the report. The four parts of this report are completed by leading specialized organizations including ScientistIn (Talent), Clarivate Analytics (Paper and Patent), CAICT (Industry Development and Market Applications), SPPM-GDC (Policy Environment) and Bytedance (Social Impact) based on first-hand data of specialized databases and a solid research methodology.

Systematic in-depth policy analysis: In addition to presenting comprehensive industry development data, this report, based on close examination of a total of 1,074 foreign and Chinese national and local policy AI policy documents, compares and analyzes the strategic priorities and development directions of AI policies in different regions, marking the first use of this research approach in similar reports.

EXECUTIVE SUMMARY

This report examines China's AI development from four perspectives — S&T output and talent input, industry development and market applications, development strategy and policy environment, and social perception and general impact. Below is a summary of the main findings of each part.

S&T Output and Talent

Paper output: China leads the world in AI papers and highly cited AI papers

China's AI papers as a percentage of the global total increased from 4.26% in 1997 to 27.68% in 2017, far ahead other countries. Universities have contributed the vast majority of AI papers, with 87 of the top 100 AI research institutions in the world being universities. Top Chinese universities have shown impressive performance internationally in the output of AI papers. Moreover, China's highly cited papers have also grown rapidly, overtaking the U.S. to take the first place in 2013. State Grid Corporation of China (SGCC) is the only Chinese company to rank among the world's top 20 companies in AI paper output. In terms of categories, computer science, engineering, and automatic control systems have the highest AI paper output. International collaboration has a significant effect on AI paper output, with as many as 42.64% of top papers being the product of international collaboration.

Patent application: China has more AI patents than U.S. and Japan; SGCC has an outstanding performance

China has become the largest owner of AI patents, followed closely by the U.S. and Japan, and the three countries combine to have 74% of the world's issued AI patents. Global AI patent applications have focused on categories including voice recognition, image recognition, robotics, and machine learning. Among China's top 30 institutional owners of AI patents, research institutions and universities are comparable with enterprises, with the former's patents accounting for 52% and the latter's 48%. However, performance varies greatly among main enterprise assignees of AI patents, with SGCC being a towering presence which has developed rapidly in AI research especially over the last five years and not only holds far more AI patents than other domestic assignees but ranks fourth among enterprise assignees globally. China's AI patents have been concentrated in data processing systems and digital information transmission, with image processing and analysis related AI patents accounting for 16% of the total. Electrical power engineering has also become an important area of China's AI patenting.

Talent: China has the world's second largest AI talent pool, though with a lower percentage of top talents

By the end of 2017, China's AI specialists reached 18,232, or 8.9% of the global total, next only to the U.S. (13.9%). Universities and research institutions are the main cradles of AI specialists, with Tsinghua University and the Chinese Academy of Sciences being the world's largest institutions of AI talent development. However, China has only 977 AI specialists in the world's top-tier AI talent pool based on the H-index, being only one fifth

of number in the U.S., ranking sixth in the world. Chinese companies have a comparatively low level of AI talent input. Companies with a high level of talent input are concentrated in the U.S. Huawei Technologies is the only Chinese company to make into the global top 20. China's AI specialists are concentrated in the eastern and central regions, though some cities in the western region, such as Xi'an and Chengdu, have also been prominent. International AI specialists are concentrated in categories including machine learning, data mining and pattern recognition, while Chinese AI specialists are scattered in different categories.

Industry Development and Market Applications

AI companies: China ranks second in the number of AI companies; Beijing has the highest concentration of AI companies in the world

Chinese AI companies began mushrooming from 2012 and had reached a total number of 1,011 by June 2018, ranking second in the world, though still significantly behind the U.S., which has 2028 companies. Chinese AI companies are highly concentrated in Beijing, Shanghai and Guangdong. Among the world's top 20 cities in terms of AI companies hosted, Beijing ranks first with 395, and Shanghai, Shenzhen and Hangzhou are also among the top 20. China's AI companies mainly specialize in three categories—voice, vision and natural language processing—with only a small percentage focusing on basic hardware.

Venture investment: China has the highest venture investment in AI

From 2013 to the first quarter of 2018, China received 60% of the world's total venture capital investment in AI, but in terms of the number of VC investments received, the U.S. remained the most active country in VC investment in AI. In China, Beijing led other regions by a big margin in the amount and rounds of VC investment, followed by Shanghai and Guangdong which have been fairly active in AI investment as well. From 2014, early-stage investment in AI as a percentage of the total investment in AI has gradually decreased as investment activity has become more rational, though Series A funding has remained in a dominant position.

Market scale: China's AI market grows rapidly; computer vision is the largest segment

In 2017, China's AI market reached RMB23.7 billion, up 67% Y/Y, with the top three segments being computer vision (34.9%), voice (24.8%) and natural language processing (21%), and hardware and algorithm combining to account for less than 20% of the market. The market is expected to grow 75% in 2018.

Product applications: AI gains wide applications, with voice and vision products being the most mature

AI has been widely applied in healthcare, finance, education and security. The global smart speaker market has grown rapidly, where major Chinese and international internet companies have expanded their presence, with Google and Amazon having taken up more than 60% of the global market, followed by Alibaba in third place and Xiaomi in fourth place. In 2017, the global robotics market reached US$23.2 billion, of which the Chinese market represented 27%. Other AI-related markets such as drone, smart home, smart grid, smart security, smart healthcare and smart finance have also seen rapid development.

Development Strategy and Policy Environment

International comparison: countries vary in their AI strategies and policy priorities

Since 2013, the U.S., Germany, the UK, Japan and China have rolled out their AI strategies and policies, each with their own priorities, with the U.S. focusing on the impact of AI on economic growth, technology development and national security, the EU on the ethical risks brought by AI in such aspects as security, privacy and human dignity, Japan on building "Society 5.0", and China on industrialization of AI applications in the service of its "Manufacturing Power" strategy. This leads to remarkable differences among the countries in their AI research priorities and application areas.

National policy: from IoT to big data to AI

Since 2009, China's AI policy has undergone five stages with changing keywords which reflect the different priorities in each stage, with the focus shifting from basic research in such categories as IoT, information security and database in the early period, to big data and infrastructure in the middle period, to AI itself and also intellectual property protection after 2017. Overall, China's AI policy mainly focuses on six categories: "made in China", innovation-driven development, IoT, Internet+, big data, and scientific and technological R&D.

Local policy: aligning with national policy under distinctive local themes

"Made in China 2025" is at the center of the China AI policy citation network and has served as a programmatic document for local governments' AI policymaking as they respond to the national AI development strategy. Based on policy documents, China's AI powerhouses are Beijing-Tianjin-Hebei, Yangtze River Delta and Guangdong-Hong Kong-Macao regions. At the provincial level, policy themes vary widely, with Jiangsu focusing on infrastructure, IoT and cloud computing, Guangdong on AI applications such as manufacturing and robotics, and Fujian on IoT, big data, innovation platform and intellectual property, reflecting their local development conditions.

Public Perception and General Impact

Public perception: The Chinese public has a high AI awareness, with half respondents expressing support of comprehensive AI development

From 2016 to 2017, AI drew massive public attention and became the most discussed popular science topic. According to a Toutiao survey of users, only 6.23% reported ignorance of AI; 53% expressed support of comprehensive AI development; and 27% held a conservative attitude towards AI development. Concerns included the replacement of jobs by AI and social crises that might be caused if AI is out of control. Overall, the Chinese public has distanced from the extremes of being overly optimistic or overly pessimistic and become more rational about AI. Interest in AI also varies significantly according to application area, age, gender and region.

Social impact: AI is capable of significantly increasing efficiency in different sectors but also poses risks

AI development is transforming the development patterns in different sectors including retail, agriculture, logistics, education and finance and reshaping production, allocation, exchange and consumption. AI is expected to be applied to more industries and bring substantial efficiency increases in the coming five years—specifically, efficiency improvements of 82% for education, 71% for retail, 64% for manufacturing and 58% for finance. AI will facilitate personalized education and promote the development of education. On the other hand, it will pose serious challenges in such aspects as employment, privacy, security and social equality.

Education survey: More AI programs are offered in universities and enthusiastically embraced by students

By July 2017, there were 36 universities approved by the Ministry of Education to offer the bachelor's degree program in "Intelligence Science and Technology" and 79 offering AI-related programs. Top Chinese universities have set up their AI labs. Currently, China's AI teaching and research activities are mainly concentrated in computer science, electronic information and automation faculties of universities. According to an online survey, online platforms have surpassed universities to become the No. 1 channel for young people to take AI courses. Netizens have shown a strong interest in learning AI, with 61% of respondents stating that they devote 10-20 hours a week to AI learning.

Based on existing research and the abovementioned findings of this report, we arrive at the following preliminary judgements and reflections on China's AI development.

Internationally, China ranks in the top echelon of AI development

Unlike in the past industrial revolutions where China was left behind and struggled to catch up, China has got a head start for the fourth industrial revolution. In AI, in fact, China has secured a leading position in the top echelon in both technology development and market applications and is in a race of "two giants" with the U.S.

In terms of the quality of development, China's AI development is far from admitting optimism

China's strengths are mainly shown in AI applications and it is still weak on the front of core technologies of AI, such as hardware and algorithm development, China's AI development lacks top-tier talent and has a significant gap with developed countries, especially the U.S., in this regard.

In terms of participating entities, China's AI companies leave much room for improvement in knowledge production

Research institutions and universities are the main producer of AI knowledge in China. Compared to their foreign counterparts, Chinese AI companies are technologically inventive and far behind domestic universities and research institutions in AI patenting. Even recognized domestic AI giants such as Baidu, Alibaba and Tencent (BAT) don't have an impressive performance in AI talent, papers and patents, while their U.S. competitors like IBM, Microsoft and Google lead AI companies worldwide in all indicators.

In terms of application areas, the integration of AI with energy systems is an important area that has been neglected

Electrical power engineering is an important AI patenting area of China, where SGCC has been the most prominent company in both AI paper publication and AI patenting. The fact that it has been either unmentioned or not highlighted in previous AI studies shows that the integration of AI with energy systems is likely an area that has been more or less neglected and represents a potential new direction of expansion of AI applications in China which will contribute to low-carbon transformation of the energy sector.

In terms of the pattern of development, China needs to strengthen industry-university research collaboration to promote knowledge application and transformation

International collaboration and industry-university collaboration are important means of advancing AI development. In China, a lot of AI knowledge is lying idle at universities and research institutions,

and it is imperative to increase industry-university collaboration to promote AI knowledge application and transformation. Going forward, China needs to not only vigorously promote industry-university collaborative innovation but also explicitly support companies to engage in AI basic research by leveraging their data and computing strengths.

In terms of policy environment, local governments should avoid blindly following suit in AI policymaking

The Chinese society has, overall, a positive and optimistic attitude towards AI development which has a very favorable environment in terms of policy, public opinion, finance, market and talent pool, but at the level of local government policymaking, there has been a tendency of "following the steps of the central government" and "chasing after hot areas". Currently, China's AI policy has emphasized on promoting AI technological development and industrial applications and hasn't given due attention to such issues as ethics and security regulation.

AI: Concept, Methods and Data

01 AI: Concept, Methods and Data

1.1 Concept of AI

AI is already a popular concept, but there is not yet a universally accepted definition for it. The traditional approach to AI development is to study how human intelligence occurs and create machines that imitate human thinking and behavior. John McCarthy, who developed the first modern theory of artificial intelligence, believed that AI machines do not necessarily have to obtain intelligence by thinking like a human and that it is important to make AI solve problems that can be solved by a human brain. Brain science and brain-like intelligence research and machine-learning represented by deep neural networks represent the two main development directions of core AI technologies, with the latter referring to the use of specific algorithms to direct computer systems to arrive at an appropriate model based on existing data and use the model to make judgment on new situations, thus completing a behavior mechanism. While only limited progress has been made in the first direction, tremendous strides have been taken in the second direction so much that machine learning has not only become the main paradigm of AI technology but been equated by some with AI itself. In general, the artificial intelligence we know today is based on modern algorithms, supported by historical data, and forms artificial programs or systems capable of perception, cognition, decision-making and implementation like humans.

1.2 Research Methods and Data

This report examines China's AI development from four perspectives—S&T output and talent input, industry development and market applications, development strategy and policy environment, and public perception and general impact. Bibliometrics and questionnaire survey are the two main research methods used in this study to examine the subject matter from the above perspectives. Bibliometrics refers to the use of mathematical and statistical methods to quantitatively analyze scientific and technological literature. The main objects include literature (various publications), authors (individual, collective or group), and key words (document identifications). In this report, the main objects include AI output (journal articles and technology patents), AI specialists, and policy documents. The questionnaire survey is a method of collecting standardized information from a number of respondents selected to complete the questionnaire with a set of standard questions on a certain phenomenon or subject. This report uses the questionnaire survey method to collect information about public perception and learning of AI. In addition, it draws upon specialized databases to analyze the current status of the AI industry.

The main indicators used in this report and their data sources are as follows:

- **AI Papers**

The dataset for analysis of AI research in this report is mainly based on data retrieved from Clarivate Analytics' Web of Science database using a list of AI keywords provided by experts which includes not only generic AI terms like "Artificial Intelligence" and "Machine Learning" but also specific AI technology categories such as "Natural Language Processing", "Computer Vision", "Facial Recognition", "Image Recognition", "Speech Recognition", "Semantic Search", "Semantic Web", "Text Analytics", "Virtual Assistant", "Visual Search", "Predictive Analytics"

and "Intelligent System" and additional author keywords of the highly cited papers identified by the search using the provided list of AI keywords and author keywords of the references of the highly cited papers, with the author keywords used being validated by experts.

As this part focuses on AI technology development, the search is limited to the three science-related databases of the Web of Science Core Collection: Science Citation Index Expanded (SCIE); Conference Proceedings Citation Index-Science; and Book Citation Index-Science.

As academic conferences are also an important part of AI research activity, the dataset draws on proceeding papers from representative academic conferences on AI (see Appendix 1). In addition, it includes papers in the "Computer Science, Artificial Intelligence" category of Web of Science (see Appendix 2: Category Description).

The dataset, with data from the abovementioned three sources combined, consists of a total of 1,875,809 qualifying papers (data retrieved on April 26, 2018, with no time or document type restriction) and provides the basis for data analysis in this study.

- **AI Patents**

The patent data in this report is from the Derwent World Patents IndexTM (DWPI) database, retrieved according to the scope (patent publication years 1997–2017 and patent citation time up to May 2018) determined based on the artificial intelligence (AI) keywords provided by experts, as refined by addition of keywords in related fields which fall under the thematic scope determined using Derwent Manual Codes for AI selected by experts. The Derwent Innovation patent database and Derwent Data Analyzer are used to perform multi-perspective analysis of the patent data. The results of multi-perspective analysis presented in this report are mainly based on patent-based records, which represent the current actual number of patents published, with other results being from analysis of patent records as deduplicated and rearranged according to their application numbers or patent families.

This report merged and deduplicated the application numbers of the patent-based records, where patent publication/grant numbers (i.e. multiple patent-based records) with the same underlying patent are merged as one patent record according to application number, so that each patent record retrieved after such merger represents one patent and, therefore, the number of patent applications in a given technological field can be determined.

- **AI Talent**

In this part, the paper and patent keyword list generated from Clarivate Analytics' Web of Science database and validated by experts are used to search ScientistIn's international and domestic expert databases. ScientistIn's international expert database is sourced from expert pages of Research Gate and Google Scholar with data cleansing and formatting and consists of valid information relating to about 6.5 million experts. ScientistIn's domestic expert database is sourced from heterogeneous data sources including Baidu Scholar, CNKI, NSFC Project Database and China Patent Full-text Database with formatting, deduplication and heterogeneous data matching and consists of valid information about 11 million experts. On this basis, AI experts are identified and marked according to their AI paper, patent and research area records to generate expert profiles based on label cloud and others.

International AI specialist data are obtained by matching the AI keyword list against ScientistIn's international expert database to generate a dataset

of experts that match at least one keyword.

Chinese AI specialist data are obtained by matching the AI keyword list against ScientistIn's domestic expert database to generate a dataset of experts that match at least one keyword.

- **AI Industry Data**

AI industry data are sourced from the data monitoring platform and industry research of CAICT Data Research Center. The data monitoring platform maintained by data experts monitors and collects data from more than 100 heterogeneous data sources including ICT news sources (Telecompaper, CNET, 36kr, etc.), major venture capital databases (CB insights, Crunchbase, etc.), venture capital websites (itjuzi.com, cyzone.cn, etc.) and the industry and commerce administration databases. The platform tracks industry developments, constructs an ICT enterprise monitoring platform, generates an enterprise basic information database, and supports statistical and research analysis by industry experts.

The AI enterprises covered by this report are those enterprises that have the provision of AI products, services and related solutions as their core business. They can be divided into those that focus on AI technologies and those that focus on products/solutions. The former category includes providers and manufacturers of algorithms, basic hardware and voice and vision generic technologies and the latter category includes manufacturers and solution providers whose products/solutions include AI products and solution providers in various vertical industries (see Appendix 3).

- **AI Policy Data**

The AI keyword list generated from Clarivate Analytics' database and validated by experts is further supplemented and refined with new additions, validated by experts, from policy documents containing any of the keywords in the list in the Government Documents Information System of Tsinghua University School of Public Policy and Management, to form an expanded AI keyword list. Finally, the expanded AI keyword list is used for information retrieval to create an AI policy dataset for analysis, which includes 27 international policy documents (9 for the United States, 5 for the European Union, 5 for Germany, 4 for the United Kingdom, 2 for France, 1 for Russia, 2 for Japan, and 1 intergovernmental document for Germany and France) and 1,047 Chinese AI policy documents. The data are as of May 15, 2018 (see Appendix 5).

- **AI Public Perception and Education Survey**

The research on public perception of AI is mainly based on the survey conducted by Bytedance of users on its Toutiao news aggregation platform. The survey was conducted from May 9 to 13, 2017 and collected a total of 3,088 valid samples. In addition, Toutiao Index tracked the AI interest differences by industry, user and region from January 1 to December 30, 2017.

The AI education questionnaire was designed by CISTP and implemented via the WJX platform. WJX, which has a daily visitor traffic of more than 500,000, recommended the questionnaire to its visitors for completion. As of May 15, 2018, a total of 1,154 valid responses were collecte

AI S&T Output and Talent

02 AI S&T Output and Talent

2.1 AI Paper Output

Definitions of key indicators:

Highly Cited Paper: *Highly Cited Papers are papers that perform in the top 1% based on the number of citations received when compared to other papers published in the same ESI field[1] in the same year.*

Hot Paper: *Hot Papers are papers published in the last two years that have been cited enough times in the most recent bimonthly period to place them in the top 0.1%.*

Top Paper: *Top Papers refer to the sum of highly cited papers and hot papers.*

2.1.1 Paper Output: World and China

The trajectory of global output of AI scientific papers began to take an upward swing from the early 1990s and remarkably more steeply in the late 1990s and then slightly went downward in 2010 before continuing the upward movement stably afterwards. In recent years, there have been over 100,000 papers published on AI every year. Papers published in this field as a percentage of all papers published globally in the same period have shown a similar pattern, pointing to the fact that as researchers have taken an increasing interest in artificial intelligence, relevant research results being publicized and published have been increasing as well.

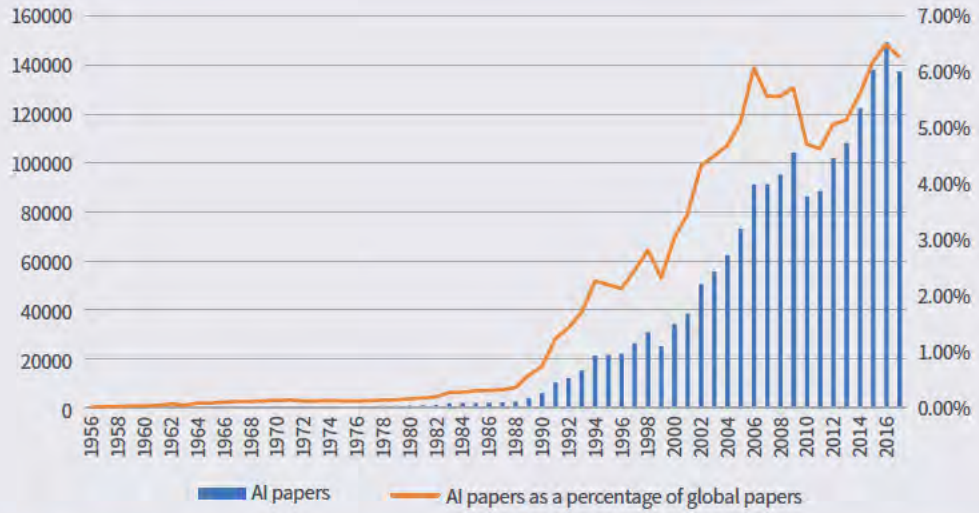


Figure 2-1 AI papers published and as a percentage of global scientific paper output from 1956 to 2017

It was found that 58.64% of AI papers were proceeding papers, showing that proceeding papers are important sources of AI research output. Articles were also significantly represented, accounting

[1] Journals included in the Web of Science Core Collection fall within 22 subject categories, i.e. ESI fields.

for 42.49% of all AI papers. Based on the above analysis, this report selected the AI-related proceeding papers, articles, reviews and book chapters published between 1997 and 2017 as the main basis for analysis [2].

In the past two decades, China (including Hong Kong and Macao) has made giant strides in AI scientific paper output, with papers published in the field increasing from more than 1,000 in 1997 to greater than 37,000 in 2017, and the percentage of the global total increasing from 4.26% in 1997 to 27.68% in 2017 (Figure 2-2).

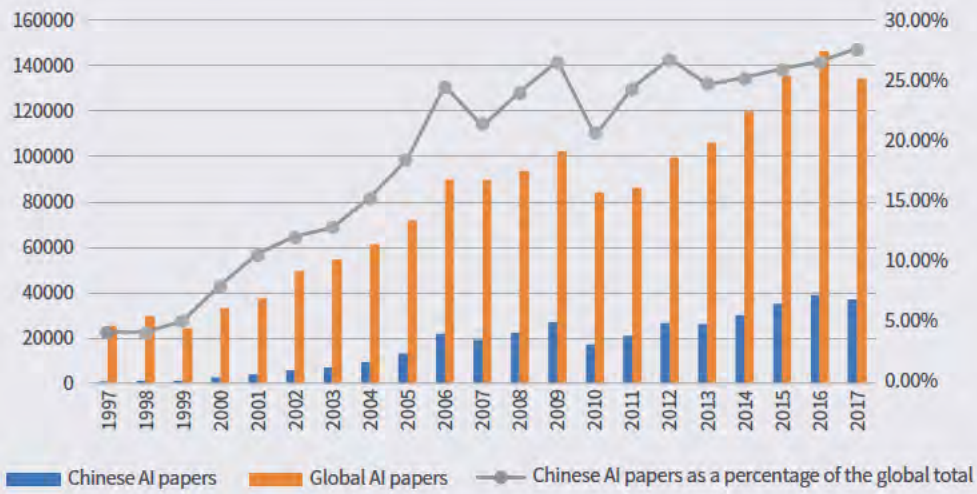


Figure 2-2 China's AI paper output and as a percentage of the global total from 1997 to 2017

As shown in the figure above, China's AI scientific papers experienced a certain decline in around 2007 and 2010 in terms of both quantity and percentage of the global total. China's output of articles and reviews has maintained an overall upward trend over the last 20 years, except a decline in 2007; in contrast, China's output of proceeding papers experienced remarkable fluctuations in a trajectory which was consistently upward before 2006 and began zigzagging afterwards, especially in 2010 when it dropped by nearly 50% from the previous year. The significant percentage of proceeding papers in all AI papers provides a partial explanation of the significant slide of paper output in 2010 in Figure 2-2. (Figure 2-3)

[2] Note: Proceeding papers and book chapters that were published in SCIE journals are also marked as articles and therefore correspond to two document types. As a result, the sum in the above figure is more than 100%.

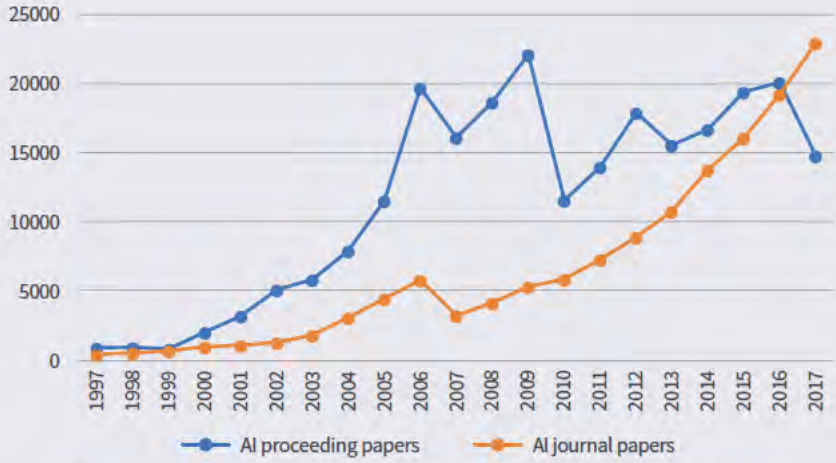


Figure 2- 3 Trend of China's AI paper output by document type

The last 20 years have seen an increasing number of countries and regions participate in basic research of AI in a race where China and the USA have ranked first and second, respectively, in terms of paper output, each with an output that is more than three times that of the United Kingdom in the third place (Figure 2-4). China and the USA are in the top echelon, followed by the United Kingdom, Japan, Germany, India, France, Canada, Italy, Spain, South Korea, Taiwan and Australia in the second echelon, and Iran, Brazil, Poland, Netherlands, Turkey, Singapore and Switzerland in the third echelon with rather strong output of AI papers.

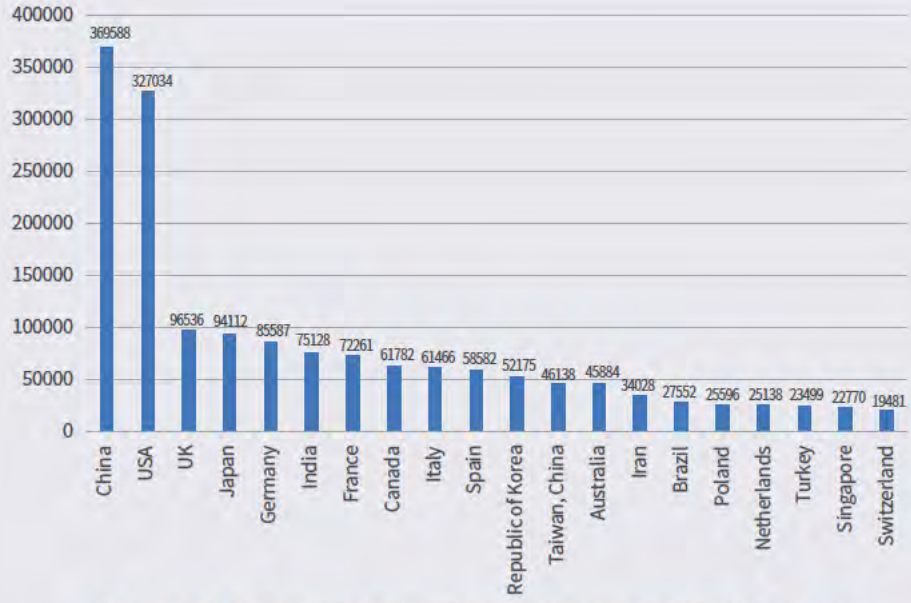


Figure 2-4 Top 20 countries/regions in AI paper output (1997-2017)

Judging from the development trajectory (Figure 2-5), the USA had been consistently in the first place in paper output before 2005, and ahead of other countries by a big margin. China's paper output

was only higher than that of India among the eight countries in 1997 but developed very fast and overtook the USA for the first time to take the first place globally in 2006. In spite of slight declines in 2007 and 2010 after that, China has remained in the lead and left the USA further behind. India, which was always at the bottom, has since 2011 picked up rapidly, and became the third largest country—after China and the USA—in terms of AI paper output in 2013, an advantage it had maintained to 2017.

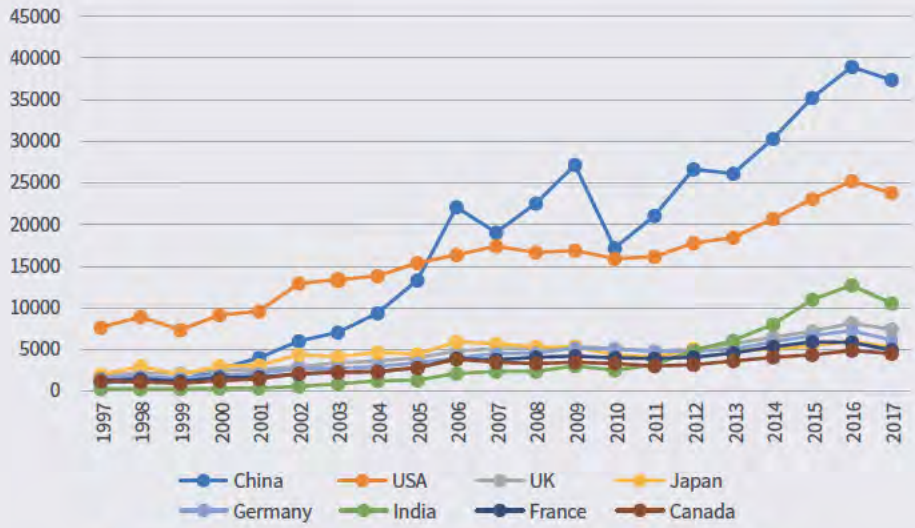


Figure 2-5 Trends of the Top 8 countries in AI paper output

In terms of institutions, Chinese Academy of Sciences (CAS), French National Center for Scientific Research (CNRS) and University of California System are the top three institutions to have published the greatest number of AI papers over the past two decades, each having more than 24,000 papers to their credit (Figure 2-6).

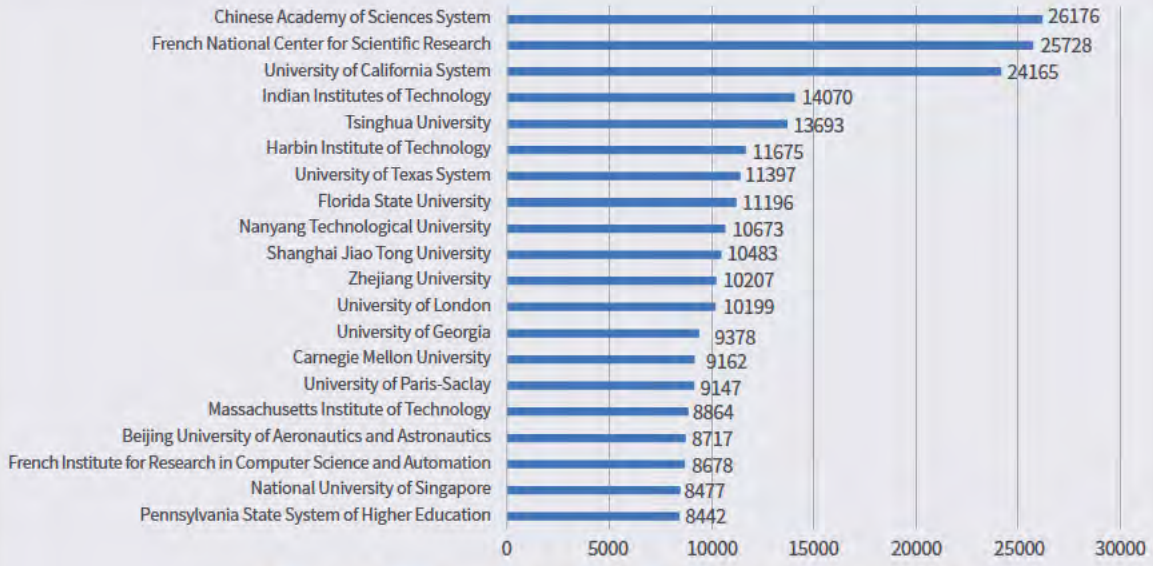


Figure 2-6 The world's top 20 institutions in AI paper output

Among the top 100 institutions in AI scientific output, there are 87 universities, 8 research institutions, 3 government agencies, and only 2 enterprises. The three government agencies are the U.S. Department of Energy, the U.S. Department of Defense and the National Aeronautics and Space Administration (NASA); and the two enterprises are IBM and Microsoft.

Figure 2-7 shows the top 20 research institutions in AI scientific output. Among them, CAS and CNRS were in the clear lead, with CAS' Institute of Software being also in the top 20. France, Germany and the USA featured prominently in this top 20 list, each with three research institutions gracing the list.

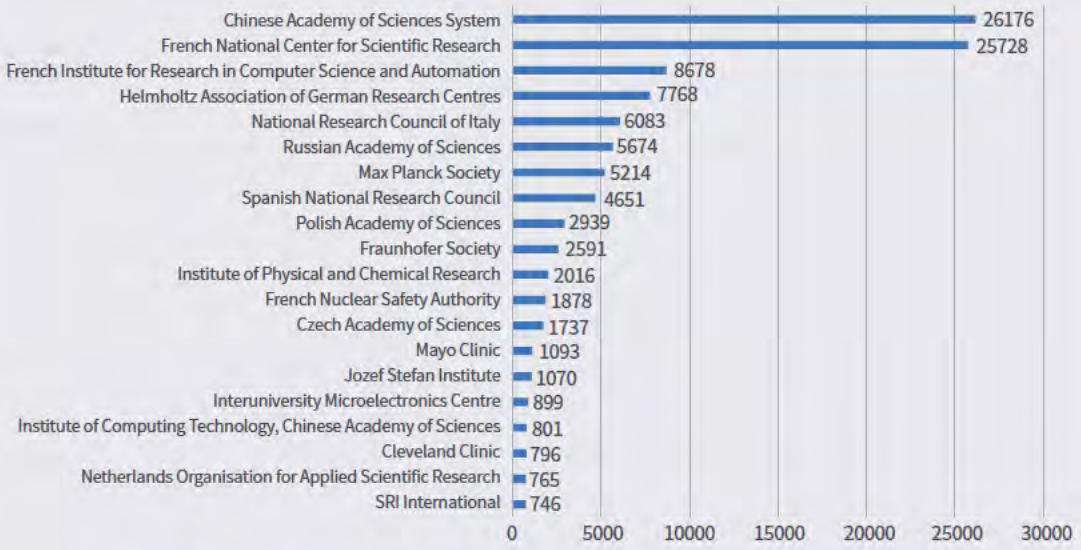


Figure 2-7 The world's top 20 research institutions in AI paper output

The top 10 government agencies in AI scientific output are all from the USA, including government departments such as Department of Defense and Department of Energy as well as funding institutions such as National Institute of Health and national laboratories, reflecting the USA's strong interest and active involvement in AI research at the government level (Figure 2-8).

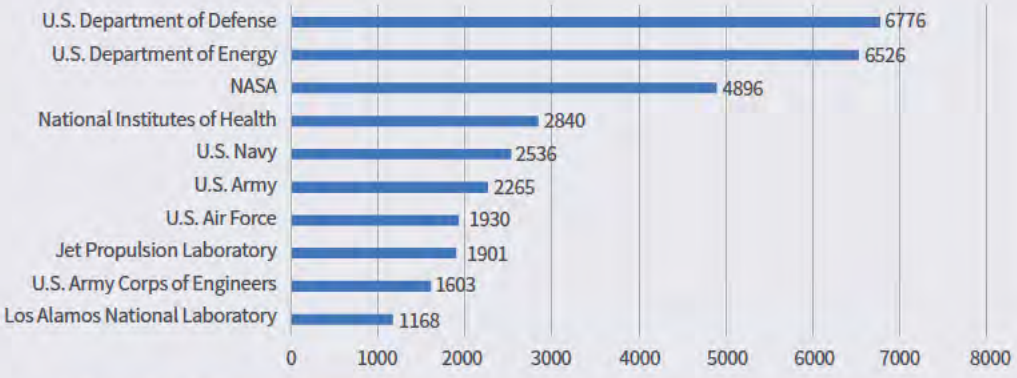


Figure 2-8 The world's top 10 government agencies in AI paper output

Many enterprises worldwide have also actively involved in basic research of AI over the last 20 years. Figure 2-9 shows the top 20 enterprises in AI paper publication, with IBM and Microsoft leaving others far behind in AI paper output. Companies such as Siemens, Samsung, Google and Intel have also yielded a significant number of AI papers.

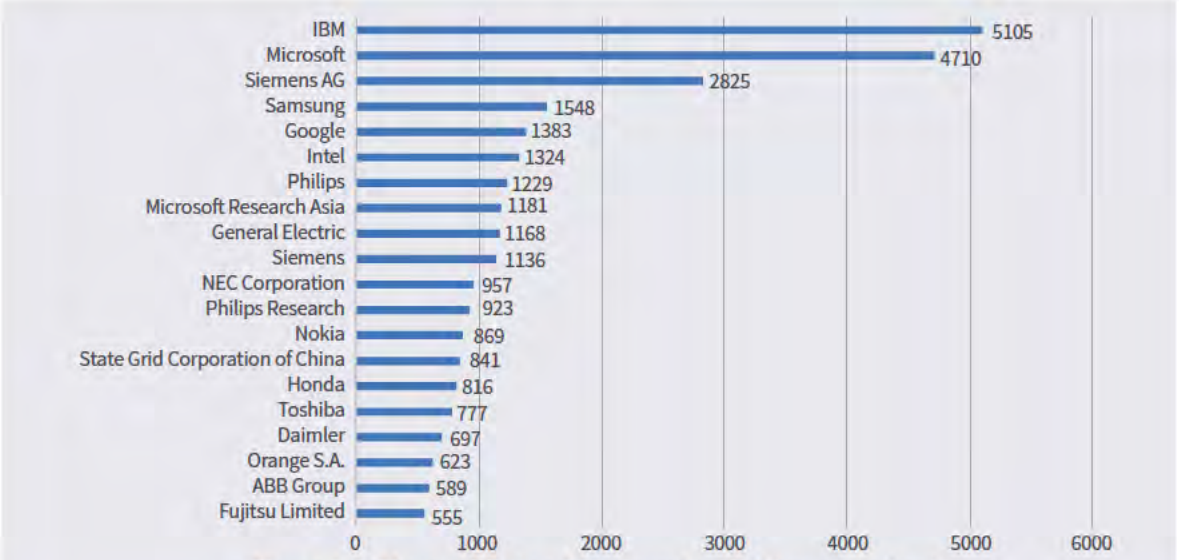


Figure 2-9 The world's top 20 enterprises in AI paper output

Many Chinese institutions have been very active in AI research over the last 20 years as well. The top twenty of them are shown in Figure 2-10. Chinese Academy of Sciences, the only research institution in the top 20 (the others are all universities), leads the list with more than 26,000 AI papers, followed by Tsinghua University, Harbin Institute of Technology, Shanghai Jiao Tong University and Zhejiang University, each having more than 10,000 papers to their credit. The top 20 list also featured three universities from Hong Kong - Hong Kong Polytechnic University, City University of Hong Kong and Chinese University of Hong Kong.

Figure 2-10 China's top 20 institutions in AI paper output

In terms of subject category[3], COMPUTER SCIENCE and ENGINEERING are the top two subject categories of AI research worldwide and in the top eight countries as well. AUTOMATION CONTROL SYSTEMS is the third-ranked subject category of AI research worldwide and in the top eight countries other than India whose third-ranked subject category of AI research is TELECOMMUNICATIONS. In addition, ROBOTICS, MATHEMATICS and IMAGING SCIENCE & PHOTOGRAPHIC TECHNOLOGY are also remarkably focused on by the top eight countries. The countries differ in their AI research strengths and priorities. Developed countries such as the USA, the United Kingdom, Japan, Germany, France and Canada have applied AI to NEUROSCIENCES & NEUROLOGY; India to ENERGY & FUELS because of energy shortage; and China to the manufacturing materials of energy management (battery system), robotics and other systems and components, leveraging its strengths in MATERIALS SCIENCE.

Table 2-1 Distribution of subject categories of AI research worldwide and in top 8 countries

Rank	Worldwide	China	United States	United Kingdom	Japan	Germany	India	France	Canada
1	Computer science	Computer science	Computer science	Computer science	Computer science	Computer science	Computer science	Computer science	Computer science
2	Engineering	Engineering	Engineering	Engineering	Engineering	Engineering	Engineering	Engineering	Engineering
3	Automation and control systems	Automation and control systems	Automation and control systems	Automation and control systems	Automation and control systems	Automation and control systems	Telecommu-nications	Automation and control systems	Automation and control systems
4	Robotics	Telecommu-nications	Robotics	Robotics	Robotics	Robotics	Automation and control systems	Robotics	Robotics
5	Telecommu-nications	Imaging science and photographic technology	Imaging science and photographic technology	Mathematics	Imaging science and photographic technology	Mathematics	Imaging science and photographic technology	Mathematics	Imaging science and photograph-ic technology
6	Imaging science and photographic technology	Robotics	Mathematics	Imaging science and photographic technology	Telecommu-nications	Imaging science and photographic technology	Energy and fuel	Imaging science and photographic technology	Telecommu-nications
7	Mathematics	Materials science	Telecommu-nications	Neurology and neuropsychol-ogy	Instruments and meters	Neurology and neuro-psychology	Mathematics	Telecommu-nications	Mathematics
8	Operations research and management science	Mathematics	Optics	Telecommuni-cations	Neurology and neuro-psychology	Telecommu-nications	Robotics	Physics	Neurology and neuro-psychology
9	Instruments and meters	Operations research and management science	Neurology and neuro-psychology	Computation-al Biology	Mathematics	Physics	Other tech-nology	Operations research and management science	Operations research and manage-ment science
10	Physics	Instruments and meters	Operations research and management science	Other technol-ogy	Physics	Biochemistry and molecu-lar biology	Materials science	Neurology and neuro-psychology	Energy and fuel

[3] Note: The Web of Science platform classifies research areas into five broad categories— Arts Humanities, Life Sciences Biomedicine, Physical Sciences, Social Sciences and Technology—which are further divided into a total of 154 subject categories (Refers to http://images.webofknowledge.com//WOKRS529AR7/help/WOS/hp_research_areas_easca.html)

2.1.2 High-impact Papers: World and China

The simple logical relations between articles (citing articles) and their references (cited references) provide the basis and background of the citation analysis. Citations underscore the value of previous research work to the current research and, therefore, papers that are more frequently cited are considered as having a higher impact[4]. Figure 2-11 shows the global distribution of top papers on AI, which highlights North America, West Europe and East Asia as the main sources of the top papers.

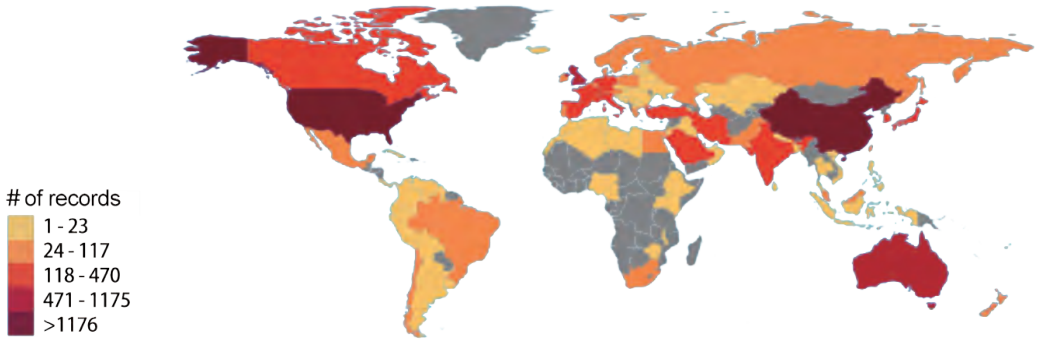


Figure 2-11 Global distribution of top papers on AI

Table 2-2 shows the quantities of highly cited papers and hot papers of the top 10 countries in AI paper output. China, the USA and the United Kingdom rank in the top 3, with Iran, the only western Asian country in the list, ranking eighth. In terms of their highly cited papers on AI as a percentage of their total papers on AI, all the top 10 countries beat the global average of 1%, with Australia ranking first in this indicator with 2.66%, followed by the United Kingdom and China whose percentages are both more than twice the global average. In terms of absolute figures, China, the USA and the United Kingdom retain their lead in hot papers as well. All the top 10 countries outperformed the global average of 0.1% in their hot papers on AI as a percentage of their total papers on AI, with Australia and China leading this indicator neck to neck with 0.7%, seven times the global average. Noteworthily, Australia, while not prominent in its total number of AI papers published in the last decade, performed prominently in the output of top papers. In addition, Japan and India, ranking 4th and 6th respectively in total AI paper output as shown in Figure 2-4, did not make into the top ten in terms of the output of top AI papers, in which indicator Japan ranks 19th and India 14th.

[4] Evidence Ltd. (2002) Maintaining Research Excellence and Volume: A report by Evidence Ltd to the Higher Education Funding Councils for England, Scotland and Wales and to Universities UK. (Adams J, et al.) 48pp.

Table 2-2 Top 10 countries in output of top papers on AI

	Highly Cited Papers	Percentage (%)	Hot Papers	Percentage (%)
China	2349	2.01	81	0.07
United States	2241	1.94	55	0.05
United Kingdom	811	2.17	23	0.06
Australia	472	2.66	13	0.07
Germany	431	1.57	12	0.04
Canada	397	1.73	10	0.04
France	354	1.46	6	0.02
Iran	271	1.28	5	0.02
Italy	253	1.12	7	0.03
Spain	247	1.03	4	0.02

Figure 2-12 shows the trends of the output of highly cited papers from the top 10 countries. It can be seen that the USA has been stable in the output of highly cited papers with a slight decline in recent years, versus the steady steep upward movement of China which overtook the USA for the first time in 2013 to rank first in the world. Australia, which has the highest percentage of highly cited papers on AI in its total papers on AI, has achieved a further modest growth in recent years. Iran, the only western Asian country in the top 10 list, has also registered a remarkable growth in the output of highly cited papers.

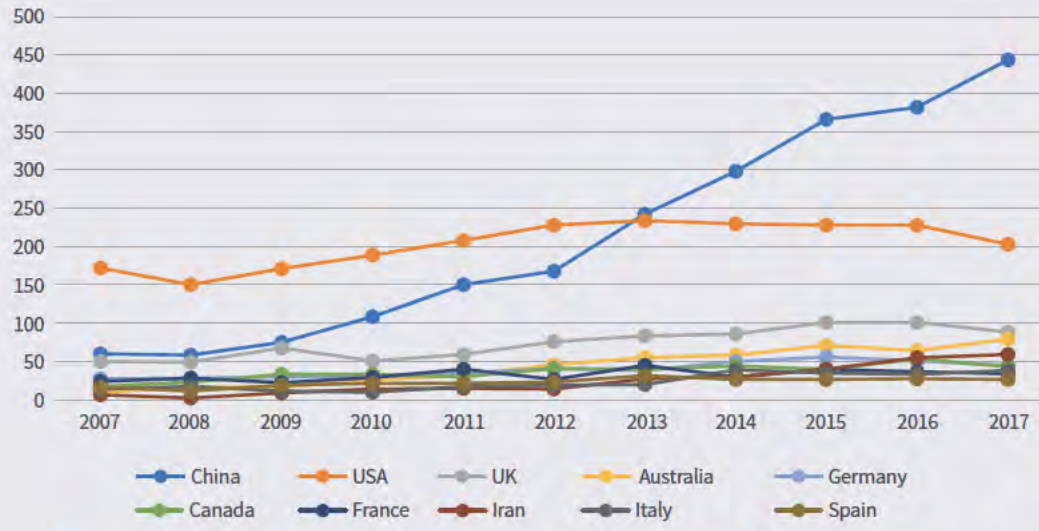


Figure 2-12 Trends of the output of highly cited AI papers of the top 10 countries

In the basic research of AI, global collaboration is indispensable. Figure 2-13 shows the collaboration graph of the top 10 countries with the greatest output of top papers on AI, where the size of a node represents the quantity of a country's output of top papers and the thickness of a line represents the

number of top papers from collaboration between the two countries connected by the line. It can be seen from the collaboration graph that China has published significant number of top papers in collaboration with such countries as the USA, the United Kingdom and Australia and that the USA has also published fairly large quantities of top papers in collaboration with the United Kingdom and Germany.

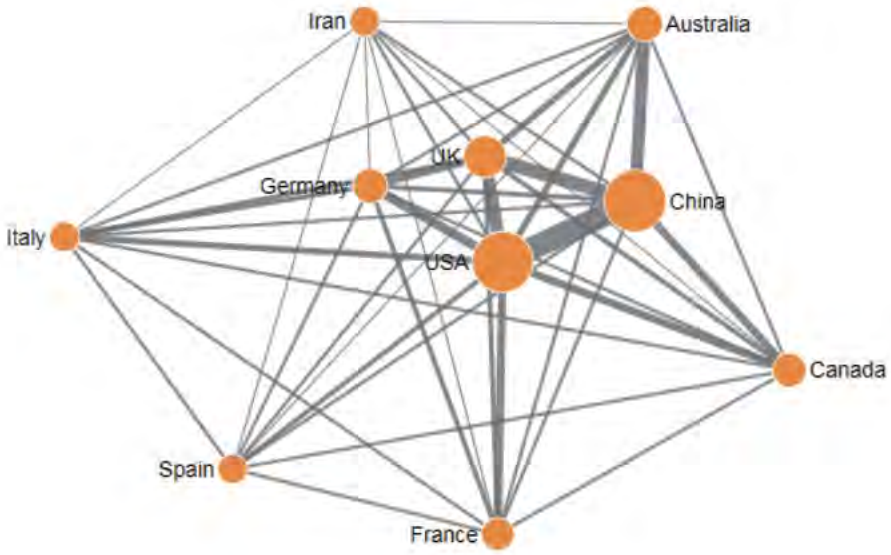


Figure 2-13 Collaboration network of the top 10 countries in the output of top papers on AI

Generally, papers yielded by international collaborative research tend to have a higher impact, as attested by Table 2-3 where international collaborative research papers on AI represent 23.42% of all AI papers but as high as 42.64% of all top papers on AI and even more than 50% of all top papers on AI of the top 10 countries with the greatest output of top papers on AI. The percentage is high at 53% for China and is even more than 80% for Australia and Germany.

As AI lends itself profitably to industrial application, a significant number of top papers was yielded by collaboration with enterprises. Compared to a global benchmark of 1.83% of industry collaborative papers as a percentage of all top papers, the percentage for the AI subject category is 3.7%, more than double the overall global benchmark. Among the top ten countries, France has the highest percentage of industry collaborative papers at 8.17%, versus more than 5% for Germany, the USA, the United Kingdom and Spain, and 2.55% for China.

Table 2-3 Representation of collaborative papers in top 10 countries' top AI papers

	Percentage of Internationally Collaborative Papers (%)	Percentage of Industry Collaborative Papers (%)
Reference Value of International Papers	23.42	1.83
Reference Value of International Top Papers	42.64	3.7
China	53	2.55
United States	53.94	6.99
United Kingdom	76.38	6.03
Australia	81.82	3.59
Germany	80.65	7.83
Canada	72.5	4.75
France	76.9	8.17
Iran	50.18	0.74
Italy	75.98	3.94
Spain	71.66	5.67

An institution's output of top papers reflects its influence in the field of research. Table 2-4 lists the top 20 institutions with the greatest output of top papers on AI, where University of California System in the USA ranks first with 337 highly cited papers and 6 hot papers, closely followed by Chinese Academy of Sciences and Harbin Institute of Technology in China. The USA occupies 7 spots in the top 20 list, followed by China with six, Singapore with two and Saudi Arabia, France, the United Kingdom, Iran and Germany with one each.

Table 2-4 The world's top 20 institutions with the greatest output of top papers on AI

Institution	Highly Cited Papers	Hot Papers	Country/Region
University of California System	337	6	United States
Chinese Academy of Sciences System	242	7	China
Harbin Institute of Technology	189	9	China
Harvard University	164	7	United States
King Abdulaziz University	136	6	Saudi Arabia
French National Center for Scientific Research	133	0	France
Southeast University	131	5	China
Nanyang Technological University	125	0	Singapore
University of London	122	2	United Kingdom
University of Texas System	115	2	United States
Massachusetts Institute of Technology	112	2	United States
Tsinghua University	110	2	China
City University of Hong Kong	106	1	Hong Kong
Stanford University	104	2	United States
U.S. Department of Energy	96	1	United States
National University of Singapore	93	0	Singapore
Islamic Azad University	91	1	Iran
Hong Kong Polytechnic University	88	1	Hong Kong
Max Planck Society	88	3	Germany
University of California, Berkeley	87	3	United States

Many enterprises have also yielded a remarkable number of high-impact papers. Microsoft, Microsoft Research Asia, and Google, have each published more than 20 top papers (Table 2-5).

Table 2-5 The world's top 13 enterprises with the greatest output of top papers on AI

Enterprise	Highly Cited Papers	Hot Papers
Microsoft	64	2
Microsoft Research Asia	27	1
Google	23	3
IBM	18	0
Siemens AG	13	0
Intel	10	0
Roche	8	1
Samsung	7	0
GlaxoSmithKline	7	0
Novo Nordisk	6	2
Toshiba	6	0
General Electric	6	0
Honda Motor	6	0

Table 2-6 lists Chinese institutions with the greatest output of top papers on AI, led by Chinese Academy of Sciences with 242 highly cited papers and 7 hot papers, followed by Harbin Institute of Technology, Southeast University of China, Tsinghua University and City University of Hong Kong in the top five. It merits noting that Liaoning University of Technology and Bohai University, though not high in total output, still made into the China top 20 list thanks to a high percentage of top papers.

Table 2-6 China's top 20 institutions with the greatest output of top papers on AI

Institution	Highly Cited Papers	Hot Papers
Chinese Academy of Sciences System	242	7
Harbin Institute of Technology	189	9
Southeast University	131	5
Tsinghua University	110	2
City University of Hong Kong	106	1
Hong Kong Polytechnic University	88	1
Huazhong University of Science and Technology	86	2
University of Electronic Science and Technology of China	77	4
Liaoning University of Technology	71	4
Northwestern Polytechnical University	67	5
Peking University	65	2
Northeastern University	65	1
Zhejiang University	64	2
Xi'an Jiaotong University	64	1
Shanghai Jiao Tong University	63	0
Central South University	60	1
Nanjing University of Science and Technology	58	1
South China University of Technology	57	5
Xidian University	55	1
Bohai University	53	0

2.1.3 Paper Citation: World and China

Authors, institutions and countries behind top papers on AI have made important contributions to AI development, which is carried forward by their citing articles that do further research on the technologies, data and theories put forward by the top papers, even though the citing articles themselves are not top papers.

Figure 2-14 shows the top 20 countries with the highest output of articles citing top papers on AI, with the USA outperforming China with more than 210,000 citing articles to take the first place, indicating the importance attached by the USA to subsequent research in the field.

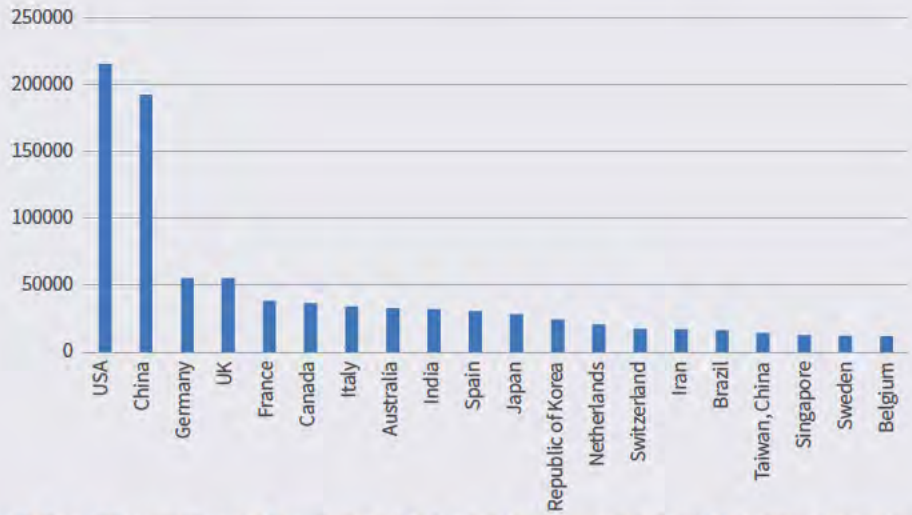


Figure 2- 14 Top 20 countries and regions with the highest output of articles citing top papers on AI

Figure 2-15 and Figure 2-16 show the top institutions with the highest output of articles citing top papers on AI worldwide and in China. Chinese Academy of Sciences, Tsinghua University, Shanghai Jiao Tong University and Zhejiang University lead the China list and are featured in the worldwide list as well.

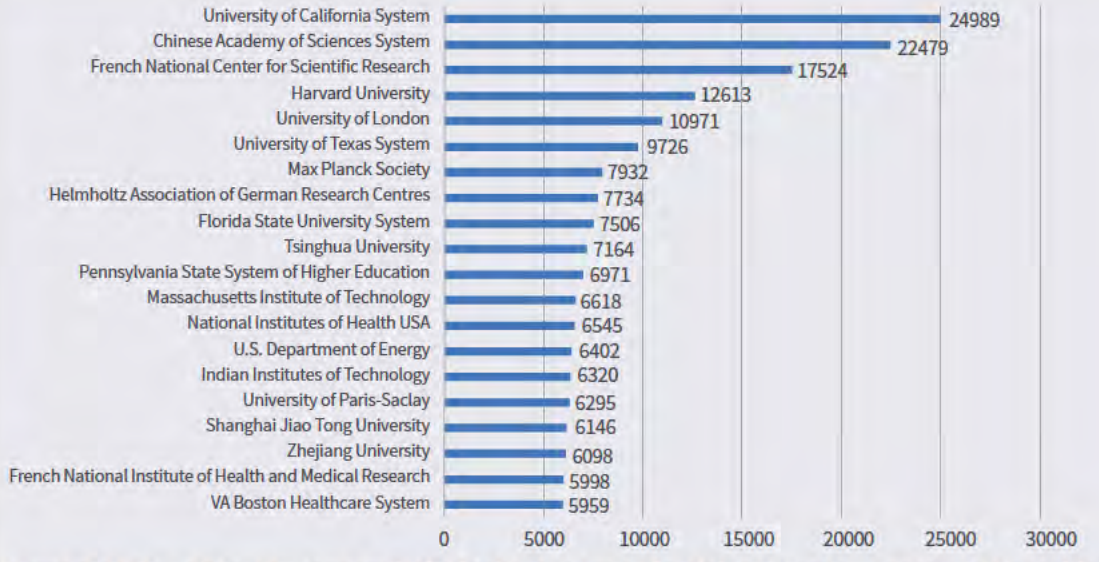


Figure 2-15 Top 20 institutions with the highest output of articles citing top papers on AI worldwide

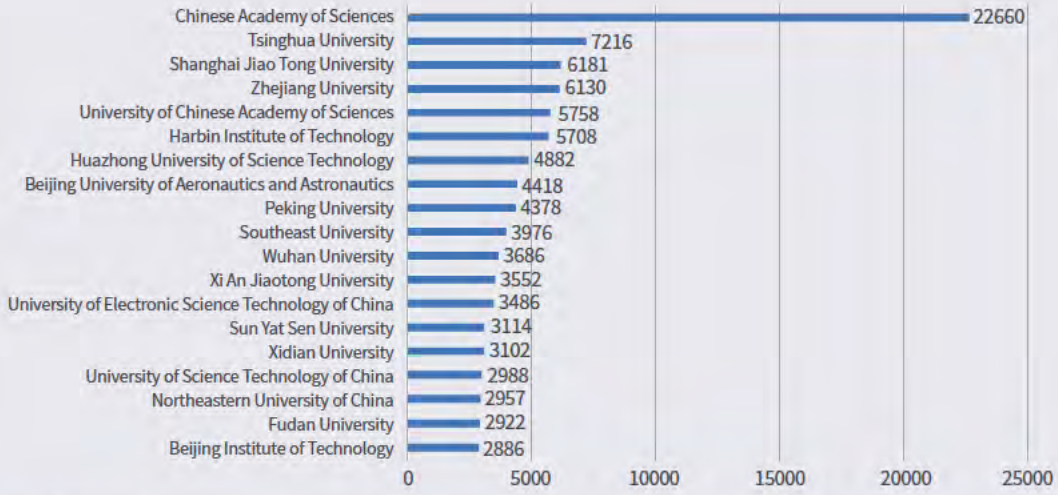


Figure 2-16 Top institutions with the highest output of articles citing top papers on AI in China

Figure 2-17 shows the top 20 subject categories with the greatest number of articles citing top papers on AI, with the top-ranked categories including ENGINEERING, COMPUTER SCIENCE, BIOCHEMISTRY MOLECULAR BIOLOGY, AUTOMATION CONTROL SYSTEMS, and NEUROSCIENCES NEUROLOGY, reflecting the interdisciplinary nature of AI research.

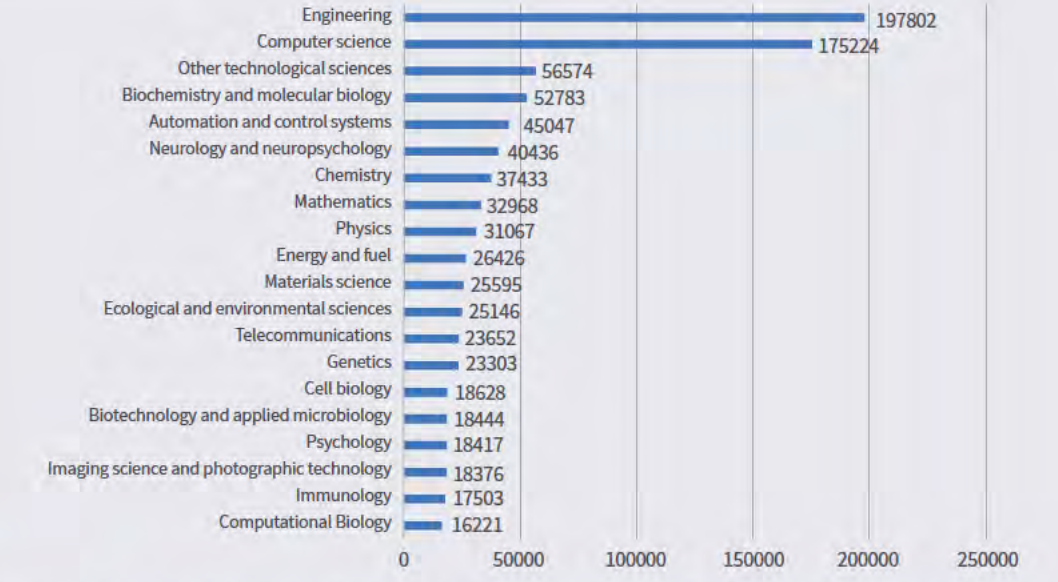


Figure 2-17 Top 20 subject categories with the greatest number of articles citing top papers on AI

Figure 2-18 and Figure 2-19 are overlay maps visually representing the trends of high-frequency keywords of top papers on AI worldwide and in China. The text analysis of high-frequency words is based on word co-occurrence, where the closer two words are to each other, the higher the frequency

of their co-occurrence is. The overlay maps feature words with a high frequency of co-occurrence, where words that are closer to red appeared more recently, and those that are closer to blue appeared earlier. The co-occurring keywords can provide valuable inputs for analysis of the evolving of hot areas of AI research. The figures indicate different focuses of global top AI papers and China's top AI papers in recent years, with the former focusing on a wide range of fields such as deep learning, neural network, adaptive control, optimization, smart grid and big data, while the latter on a fewer areas such as adaptive control, neural network, and big data.

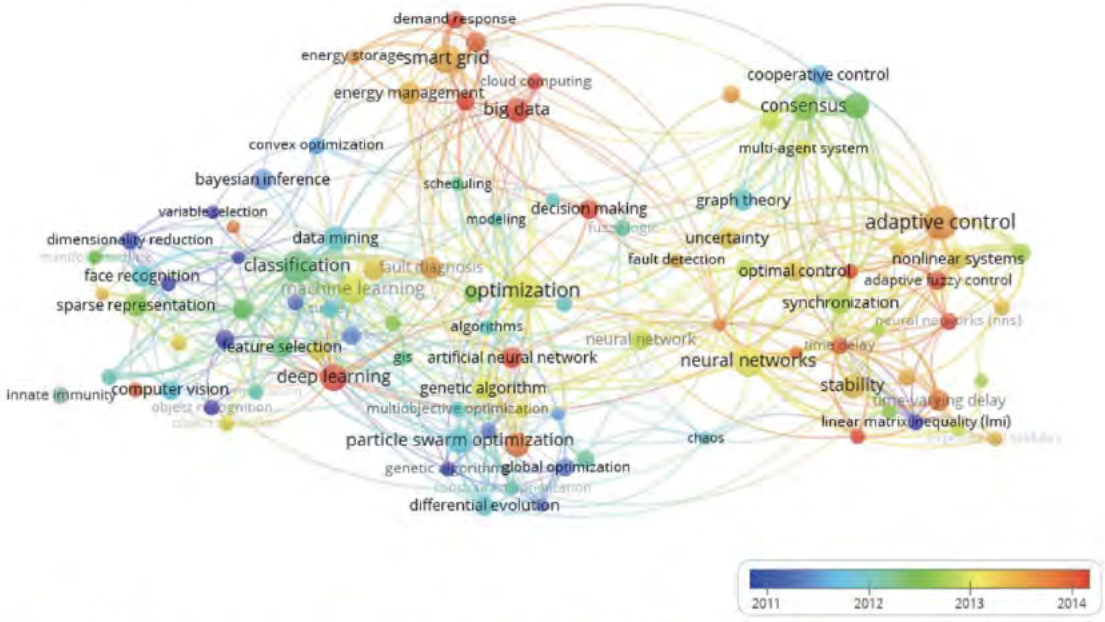


Figure 2-18 Keyword co-occurrence analysis of global highly cited AI papers from 2007 to 2017

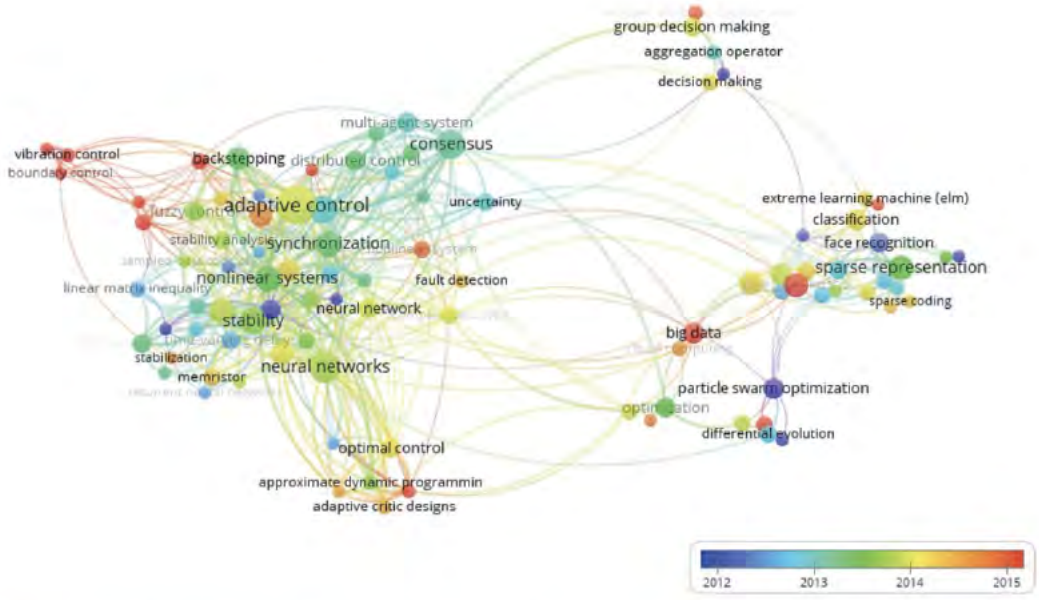


Figure 2-19 Keyword co-occurrence analysis of China's highly cited AI papers from 2007 to 2017

2.2 AI Patent Output

2.2.1 Global AI Patent Output

- **Trend of patent applications:**

Figure 2-20 shows the trend of patent applications in AI, indicating an overall upward trend on an application number consolidation basis over the last nearly 20 years, which peaked in 2016 with a total of more than 52,000 patent applications.

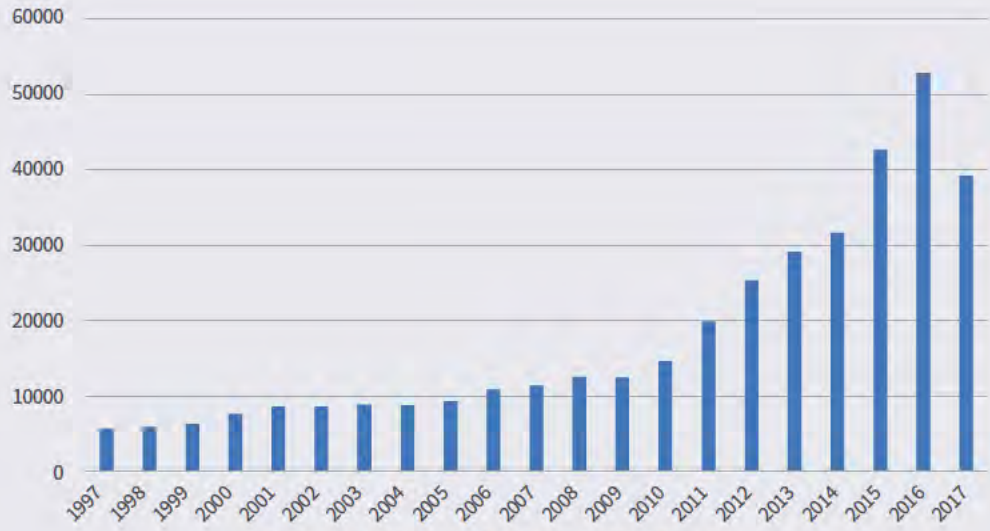


Figure 2-20 Trend of AI patent applications

- **Main assignees**

In DWPI database, the assignee of each patent document is designated with a four-letter code. The assignee code is generally based on the assignee's name. An analysis of the number of patents published by assignees revealed through Derwent assignee codes identified the companies that have the greatest number of AI patents, i.e. leaders in AI, including Chinese and foreign companies such as IBM, Microsoft, State Grid Corporation of China (SGCC) and Samsung (Figure 2-21).

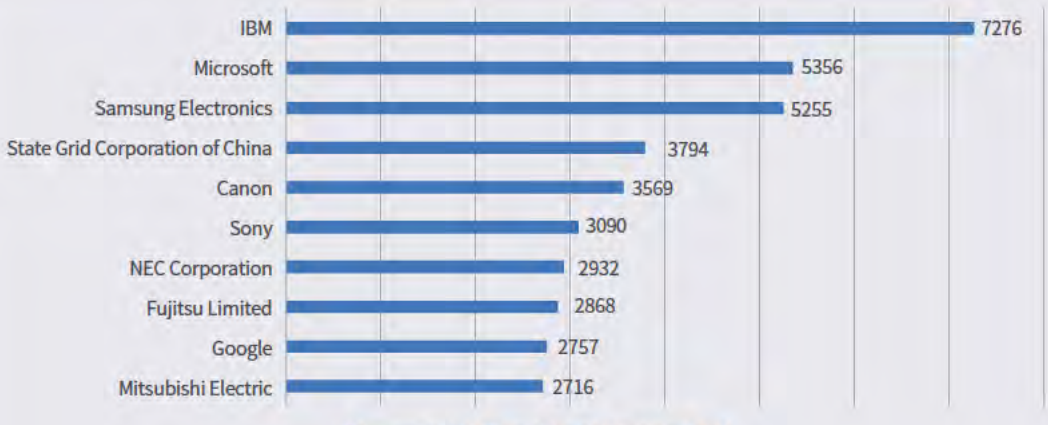


Figure 2-21 Top 10 assignees in AI

As shown by the competitive landscape of main assignees, IBM outperformed its closest competitor Microsoft by 36% in the number of patents, with its published patents accounting for 18% of the total published patents of the top ten assignees.

In terms of patent maintenance, SGCC has the highest percentage (87%) of valid patents in its total published patents among the top ten assignees. In contrast, as many as 40% of Sony's patents in AI has expired (Figure 2-22).

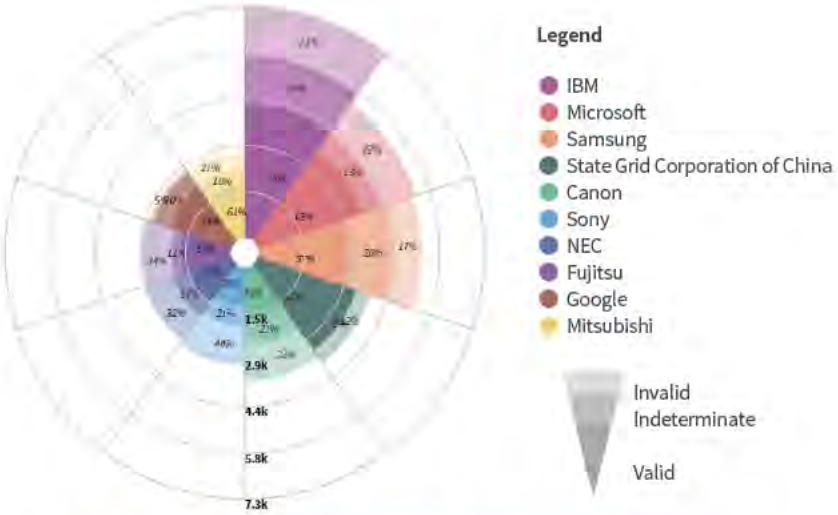


Figure 2-22 Competitive landscape of major assignees in AI

According to the analysis of main assignees, SGCC is the only Chinese company to secure a place in international competition in AI patents. As shown in Figure 2-23, SGCC's AI-related technological inventions focus on fields such as grid control, power distribution and utilization networks, smart substation transformer, wind farm and new energy, also with a remarkable interest in AI-related smart algorithms and robotics. According to interviews with experts, the quick increase of AI patents of SGCC in recent years is attributable to the following three main reasons: First, grid operations and management involve the collection and analysis of different types of data, which provide excellent use scenarios for AI technologies such as image processing, voice recognition and big data analysis. Secondly, SGCC not only has full life-cycle data of its massive assets and rich user data but also has massive operations data across wide regions and time frames. On top of those, it has completed its transformation of digitalization and information, and its operation has achieved automation to a large extent, which provides great conditions for making grid operations even more intelligent. Thirdly, SGCC has a clearly defined project management system, and its AI projects are managed with strict quantitative evaluation indicators.

Figure 2-23 SGCC's main areas of AI research

• Global distribution of AI patents

A further analysis of priority countries/regions identified originating countries/regions of AI technologies. As shown in Figure 2-24, China, the United States and Japan are the top three countries/regions of origin of AI technologies, whose AI patents account for 74% of the total published AI patents.

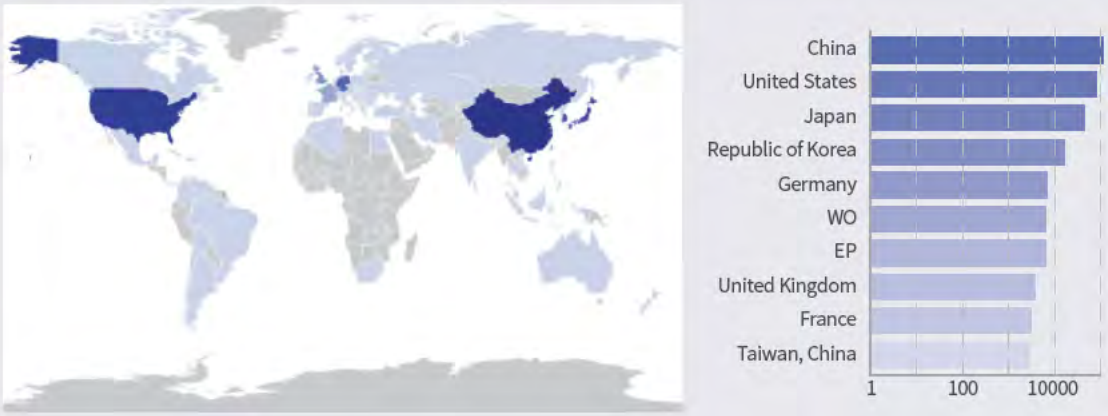


Figure 2-24 Distribution of countries/regions of origin of AI technologies

Analysis of countries/regions with published AI patents identified countries/regions where AI technologies have gained further development. As shown in Figure 2-25, China ranks first in the comprehensiveness of patented AI technologies, while the United States has the highest patent grant rate.

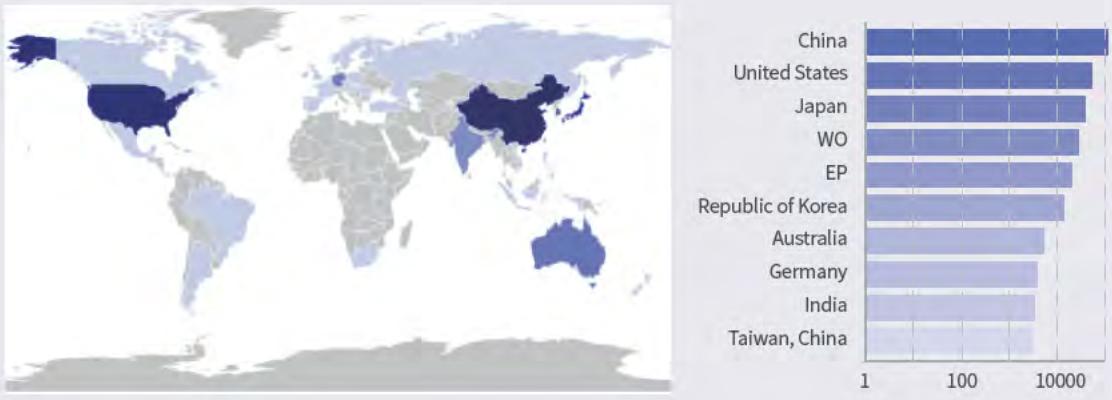


Figure 2-25 Global distribution of AI patents

- **Fields of patented AI technologies**

ThemeScape within Derwent Innovation, which performs statistical and textual analysis of the semantic similarity of patent texts and presents its findings visually in a map, can provide a vivid thematic panorama of an industry or technological field.

Figure 2-26 is a ThemeScape map of patented AI technologies. As shown in the figure, patent applications focus on fields including voice recognition, image recognition, robotics, and currently most popular deep learning (such as neural network, human-machine interaction, decision tree, and fuzzy logic). Figure 2-26 also shows the main application fields of AI technologies, such as energy, communication and vehicles.

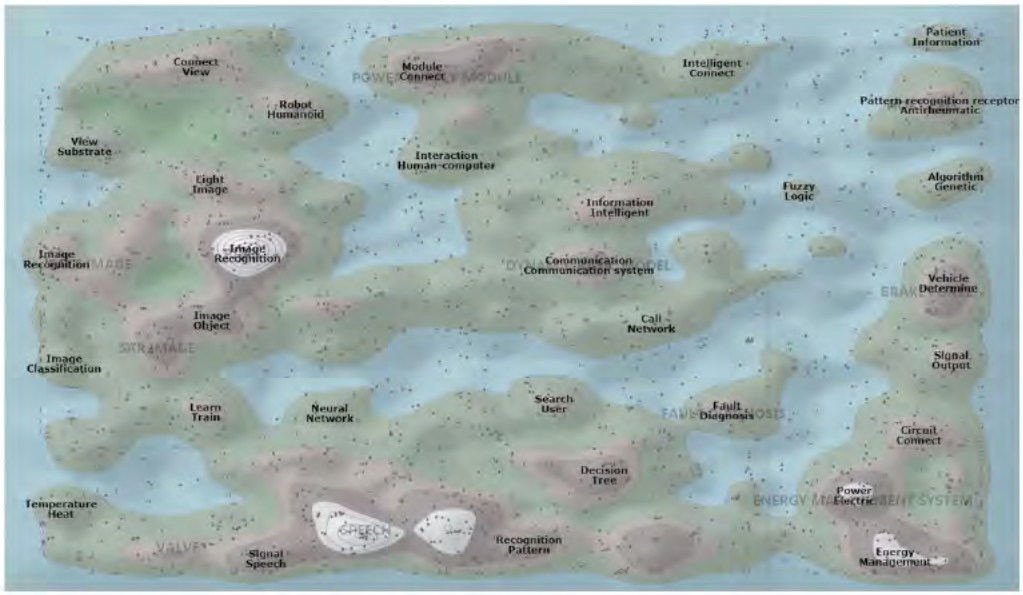


Figure 2-26 The ThemeScape of AI patents

2.2.2 China's AI Patent Output

- **Distribution of major assignees**

This report analyzed China as the earliest priority country with records being deduplicated using the Derwent patent family mechanism. As a patent right is valid only in the regions where it is granted, one patented invention may have multiple published patent documents. In view of this fact, this report merged multiple patent documents of the same invention in a single patent family so that calculation reflects the number of actual inventions rather than the number of patents which may have duplicates. On this basis, the statistics of the number of inventions belonging to each assignee will provide a comprehensive picture of AI R&D in China (the earliest priority country/region: CN; years of publication 2013-2017). Shown in Figure 2-27 are the top 15 assignees from academia and the top 15 from the business world in terms of the AI patents held over the last five years, with the first list featuring universities such as Chinese Academy of Sciences, Zhejiang University, Xidian University, South China University of Technology, Tsinghua University, Hohai University, Southeast University, University of Electronic Science and Technology of China, Beihang University and Tianjin University, and all being more or less comparable, and the second list featuring companies such as SGCC, Baidu, Changhong, OPPO, Xiaomi and Midea (but differing drastically in terms of patents held, with SGCC holding far more than others). Overall, slightly more patents are from academia (52%) than from the business world.

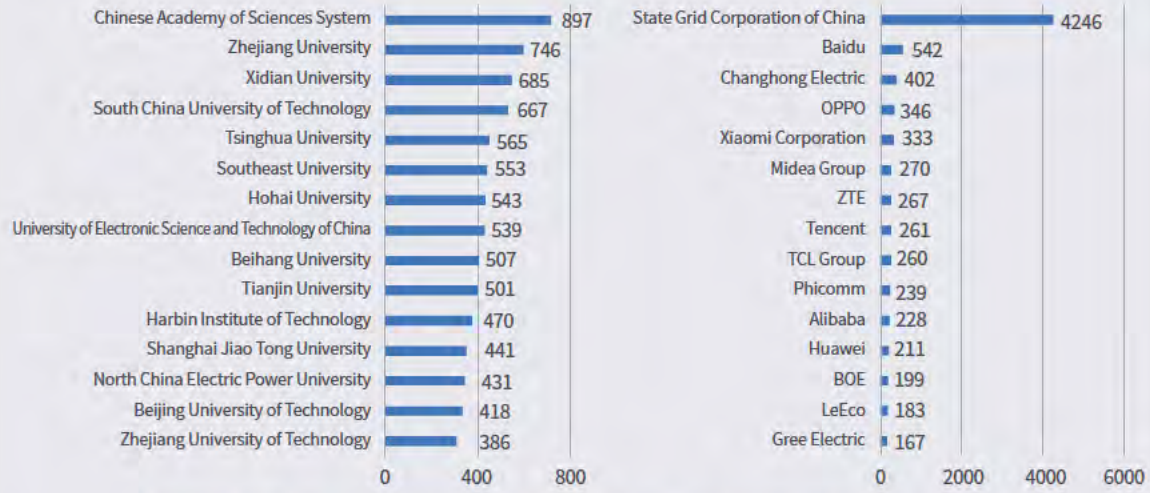


Figure 2-27 Top assignees from the academia and from the business world

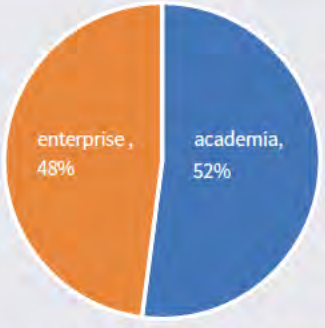


Figure 2-28 AI patents held by top 30 assignees by category

- **Distribution of key technological fields**

This report analyzed Derwent Manual Codes for AI and provides a picture of the fields and sub-fields of China's AI technologies patented in the last five years. As shown in Figure 2-29, AI technologies developed by China have focused on such fields as data processing systems and digital information transmission. Image processing and analysis (T01-J10B), in particular, has had more inventions patented (representing 16% of the total inventions) than in other sub-fields.

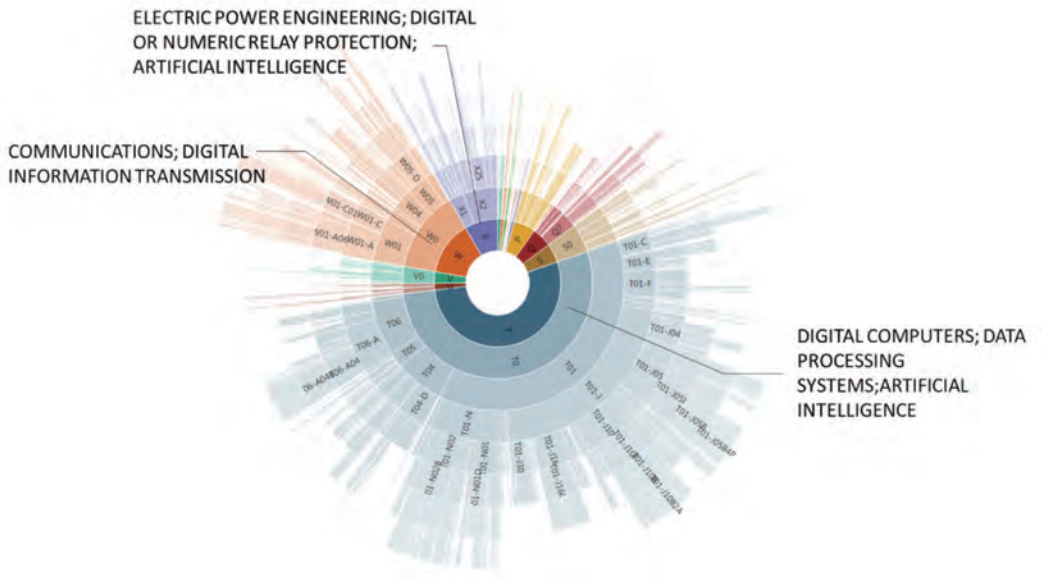


Figure 2-29 Distribution of patented inventions in AI (Derwent Manual Codes)

2.3 AI Talent

Definitions of Main Indicators:

International AI talent: *Researchers possessed of creative research ability and technical expertise in their research area and active in AI research with innovative outcomes. Innovative outcomes refer to issued patents and/or published English papers. "Active" refers to the creation of innovative outcomes in the last ten years.*

Top international AI talent: *International AI talent with leading research ability. To ensure access to and measurement of assessment indicator data, this report adopts the h-index widely recognized in the academic community as the indicator of research ability and qualify researchers whose H-index score ranks among the top 10% of international AI researchers as top international AI talent.*

Chinese AI talent: *Researchers possessed of creative research ability and technical expertise in their research area and active in AI research with innovative outcomes. Innovative outcomes refer to issued Chinese patents and/or published papers in Chinese or English. "Active" refers to the creation of innovative outcomes in the last ten years.*

2.3.1 Global AI Talent Distribution

- **Distribution by regions**

International AI talent is highly concentrated in several countries including the United States, China, India, Germany and the United Kingdom. By the end of 2017, the international AI talent pool

had 204,575 people, densely distributed in North America, Western Europe, Northern Europe, East Asia, South Asia and West Asia. At the country level, AI talent is concentrated in a few countries, with the top ten countries representing 61.8% of the global total.

China ranks second with an AI talent number that is 65% of the United States'. The United States takes the lead with as many as 28,536 AI talents, representing 13.9% of the global total; followed by China in the second place with 18,232, representing 8.9%; India in third place with 17384; Germany in fourth place with 9,441; and the United Kingdom in fifth place with 7,998. In terms of city distribution, the top five cities of AI talent as a percentage of the national total is 10.5% for the United States, 20.0% for China, 14.9% for India, 17.3% for the United Kingdom, and 23.3% for Germany.

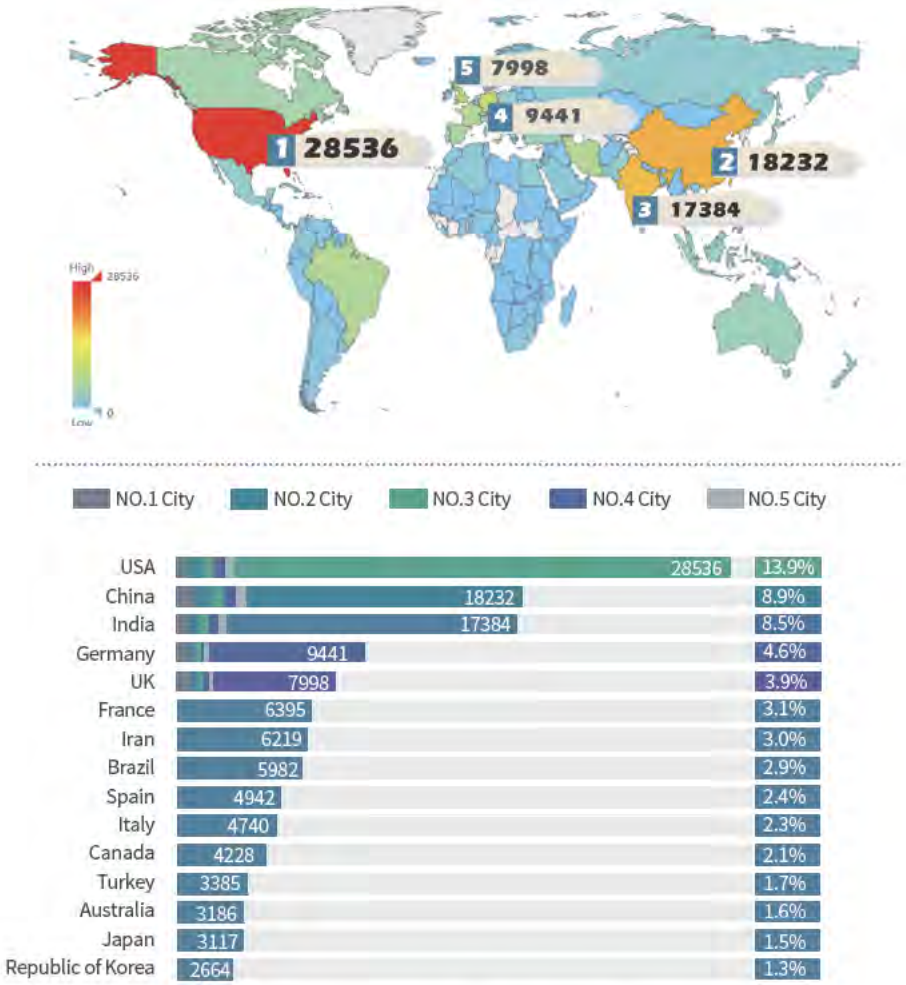
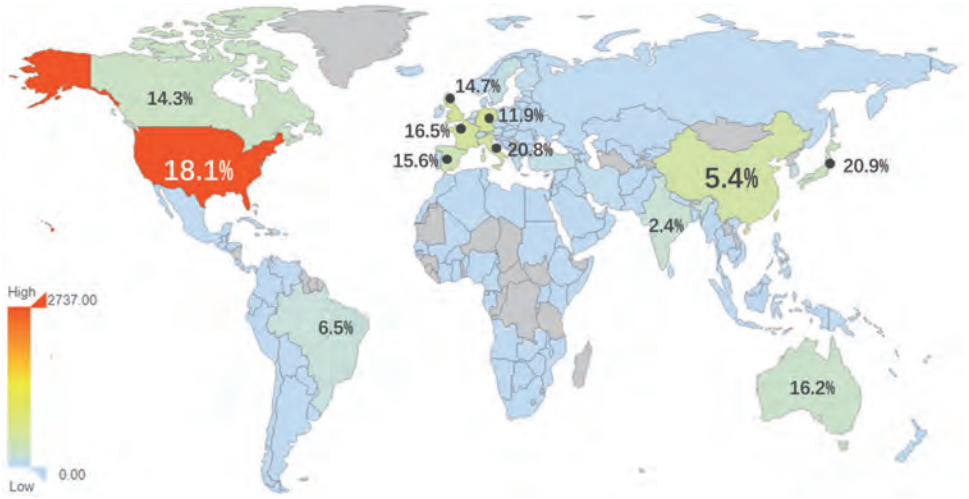


Figure 2-30 Global distribution of AI talent

Top international AI talent is concentrated in a handful of developed countries including the United States, United Kingdom, Germany, France and Italy. By the end of 2017, the top international AI talent pool had 204,575 people, densely distributed in North America, Western Europe, East

Asia and South Asia. At the country level, top AI talent is concentrated in a few countries, with the top ten countries representing 63.6% of the global total, with a slightly higher concentration than that of all AI talent (61.8%).

Developing countries such as China are underrepresented by top AI talent. The United States maintains its safe lead with 5,158 top AI talents, representing 25.2% of the global total, 4.4 times of the number of the United Kingdom in second place. The United Kingdom, and Germany in third place, France in fourth place, and Italy in fifth place, are at comparable levels. China ranks 6th with 977 top AI talents at a rather low level, especially in comparison with its all AI talent in second place globally. Developing countries like India (ranking third in all AI talent) and Brazil (8th) are also in the same situation, whose rank in terms of top AI talent falls to 11th and 13th, respectively.



Country	Number of top AI talent ÷	Number of total AI talent =	top AI talent as a percentage of all AI talent in each country
USA	5158	28536	18.1%
UK	1177	7998	14.7%
Germany	1119	9441	11.9%
France	1056	6395	16.5%
Italy	987	4740	20.8%
China	977	18232	5.4%
Spain	772	4942	15.6%
Japan	651	3117	20.9%
Canada	606	4228	14.3%
Australia	515	3186	16.2%

Figure 2-31 Global distribution of top AI talent (top AI talent as a percentage of all AI talent in each country)

- **Distribution by universities**

International AI talent is concentrated in universities. Universities host a total of 147,914 international AI talents, accounting for 72.3% of the total, versus 31,123 in research institutions such as national academies of sciences and research centers and 6,488 in for-profit business entities.

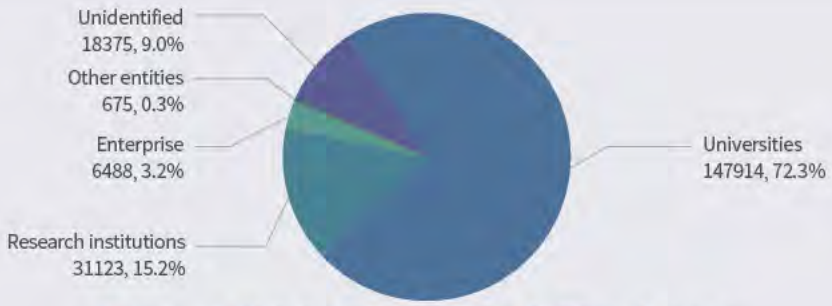


Figure 2-32 Global AI talent by type of affiliated entities

Universities that have a high intensity of International AI talents are concentrated in China, with Tsinghua University having the greatest number of international AI talents. Thanks to its large research force and master's and doctoral degree programs, Tsinghua University leads universities around the world with 822 international AI talents, followed by Shanghai Jiao Tong University in second place with 590; Vellore Institute of Technology in third place with 526; Beihang University in 4th place with 525; and Carnegie Mellon University in 5th place with 523. Massachusetts Institute of Technology, Stanford University and Georgia Institute of Technology rank 14th, 17th and 18th, respectively.

Tsinghua University	822	China	Nanyang Technological University	418	Singapore
Shanghai Jiao Tong University	590	China	Xi'an Jiaotong University	400	China
Vellore Institute of Technology	526	India	University of Science and Technology of China	382	China
Beihang University	525	China	Massachusetts Institute of Technology	368	USA
Carnegie Mellon University	523	USA	National University of Singapore	367	Singapore
Zhejiang University	506	China	University College London	365	UK
Huazhong University of Science and Technology	465	China	Stanford University	364	USA
Peking University	463	China	Georgia Institute of Technology	358	USA
Wuhan University	446	China	Harbin Institute of Technology	353	China
Beijing University of Posts and Telecommunications	443	China	Imperial College London	334	UK

Figure 2-33 International AI talent by affiliated university

However, there is no Chinese university in the top ten universities by the number of top international AI talent. In this indicator, Stanford University takes the lead with 79, followed closely by Massachusetts Institute of Technology, University College London, University of Washington and University of São Paulo. Tsinghua University ranks 15th and Shanghai Jiao Tong University 33rd, falling steeply from their positions in terms of all AI talents.

Stanford University	79	USA	University of Oxford	49	UK
Massachusetts Institute of Technology	72	USA	Sapienza University of Rome	47	Italy
University College London	67	UK	University of Cambridge	45	UK
University of Washington	60	USA	ETH Zurich	43	Switzerland
University of São Paulo	60	Brazil	Tsinghua University	42	China
University of Michigan	55	USA	University of California, San Francisco	42	USA
University of Toronto	53	Canada	University of Southern California	42	USA
University of California, San Diego	51	USA	Catholic University of Leuven	41	Belgium
University of California, Berkeley	51	USA	Karolinska Institute	40	Sweden
University of California, Los Angeles	49	USA	Yale University	40	USA

Figure 2-34 Top international AI talent by affiliated university

- **Distribution by research institutions**

The Chinese Academy of Sciences is the world's largest institution in terms of AI talent. The Chinese Academy of Sciences, with its vast system and affiliated research institutes, has as many as 1,244 AI talents, taking the clear lead globally. NASA ranks second globally with 103. Centre for Research and Technology Hellas ranks third with 67, followed by Toulouse Institute of Computer Science Research in 4th place with 64 and Bulgarian Academy of Sciences in 5th place with 63.

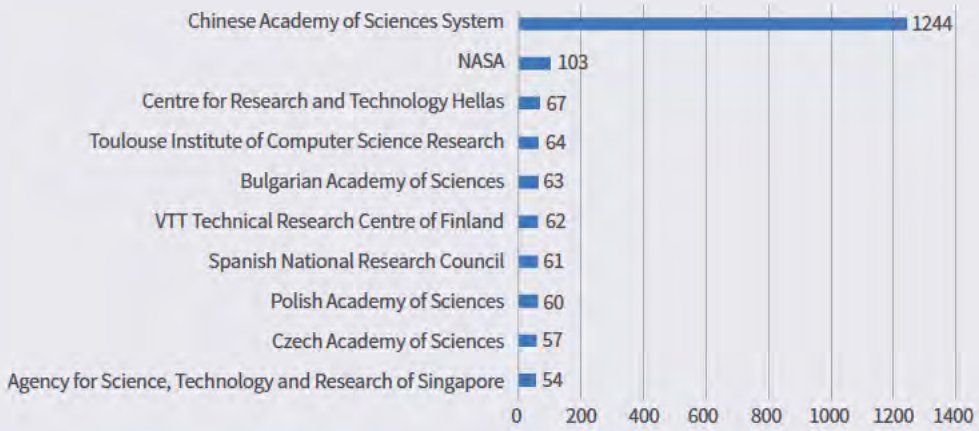


Figure 2-35 World's top 10 research institutions by AI talent

In terms of the number of top AI talents, Chinese Academy of Sciences still has a shining performance. It ranks first globally with 88, followed closely followed by National Research Council of Italy and French National Center for Scientific Research.

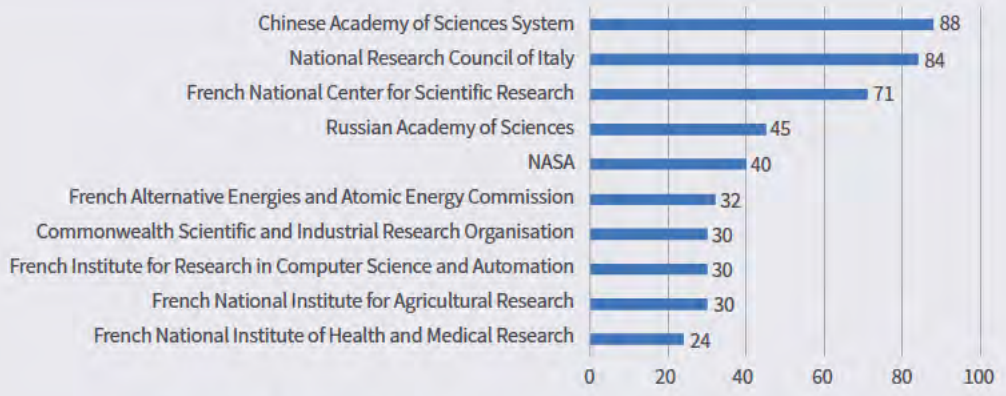


Figure 2-36 World's top 10 research institutions by top AI talent

- **Distribution by enterprises**

Enterprises with a high intensity of International AI talents are concentrated in the United States. Huawei Technologies is the only Chinese company to make into the top 20. In the business world, international AI talents are mainly employed by computer hardware and software development companies. The related industries in the United States started in the mid 20th century and their leading companies such as IBM, Microsoft and Google wield a wide global influence and represent the top three companies in the world in AI talent. Well-known American companies such as Intel, General Electric, Hewlett-Packard, Honeywell, Cisco, Qualcomm, and Apple are also on the list.

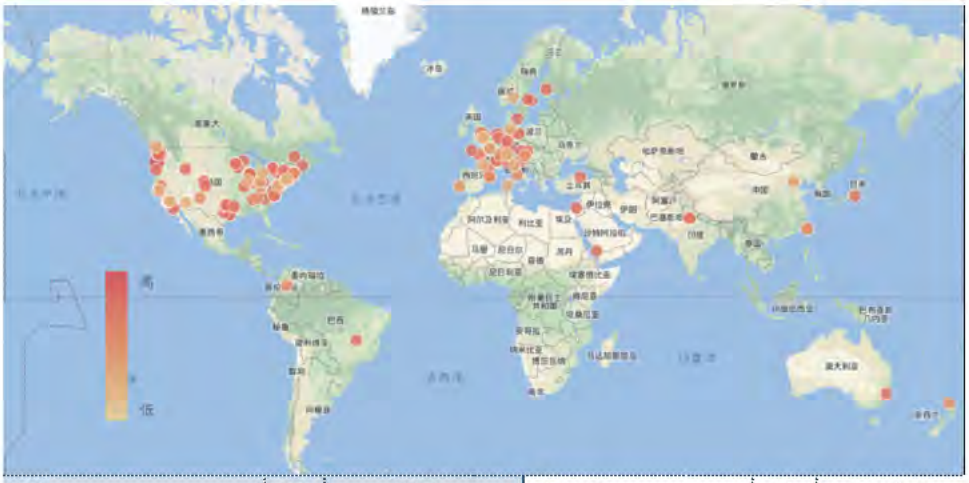
Three German companies—Siemens, SAP and Bosch, being all large manufacturers—break into the top 20 list. India has two companies on the list—Tata Consultancy Service and Cognizant, being mainly IT service providers. The Republic of Korea, the Netherlands, China, Ireland and Italy each have one company on the list.

IBM	538	USA	Hewlett-Packard	62	USA
Microsoft	341	USA	Accenture	59	Ireland
Google	256	USA	SAP Research	58	Germany
Tata Consultancy Service	189	India	Robert Bosch	56	Germany
Siemens	176	Germany	Cognizant	55	India
Samsung	142	Republic of Korea	MITRE	55	Italy
Intel	142	USA	Honeywell International	53	USA
Philips	118	Netherlands	Cisco	51	USA
General Electric	87	USA	Qualcomm	47	USA
Huawei	73	China	Apple	46	USA

Figure 2-37 International AI talent by affiliated enterprise

IBM has the largest top-tier AI talent force among enterprises globally. IBM leads the corporate world by a big margin with 83 top AI talents, followed by Intel with 39, Google with 32 and Microsoft with 31.

Overall, American internet companies have a clear edge. There is no Chinese company in the top ten, with only Huawei making into the top 20.



IBM	83	USA	Ericsson	11	Sweden
Intel	39	USA	ABB	10	Switzerland
Google	32	USA	Roche	10	Switzerland
Microsoft	31	USA	Sanofi	9	France
Siemens	22	Germany	AstraZeneca	9	Sweden
Philips	18	Netherlands	Novartis	9	Switzerland
Samsung	16	Republic of Korea	Pfizer	9	USA
General Electric	15	USA	Merck	8	Germany
Eli Lilly	12	USA	Nokia	8	Finland
Qualcomm	11	USA	Huawei	7	China

Figure 2-38 Top international AI talent by affiliated enterprise

- **Distribution by research areas**

International AI talent is mostly devoted to AI algorithm development, especially such hot areas as machine learning, data mining and pattern recognition. Specifically, there are 70,031 people devoted to machine learning, 68,736 to data mining, 53,241 to pattern recognition, 32,619 to computer vision, 21,794 to feature extraction and 13,404 to artificial neural networks.

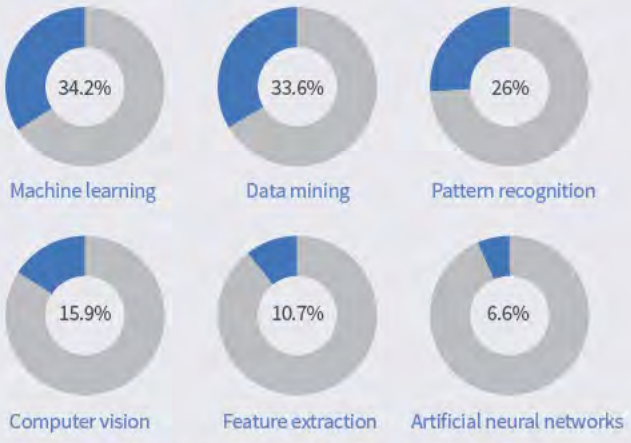


Figure 2-39 International AI talent by research area

2.3.2 China's AI Talent Distribution

In this report, Chinese AI talent refers to researchers having published Chinese patents or papers in Chinese or English over the last ten years, and their distribution, therefore, is more or less different from the distribution of international AI talent with English papers or patents only.

- **Distribution by regions**

Chinese AI talent is tilted towards the eastern region. By the end of 2017, China had 201,281 AI talents with a dense concentration in the eastern region. Eastern provinces had 126,120 AI talents, or 62.7% of the national total, versus 37,514, or 18.6%, for the central region, and 37,362, or 18.6%, for the western region. Beijing has a clear edge and ranks first nationwide with 27,355 AI talents. Jiangsu Province ranks second with 19,293, followed by Shaanxi with 12,878 in third place, being the only province in the western region to rank among the top ten. Hubei was closely behind with 11,773, followed by Shanghai with 10,592. Overall, Beijing and Jiang-Zhe-Hu (Jiangsu, Zhejiang and Shanghai) represent the two AI talent centers in the eastern region, with Hubei being the AI center of the central region and Shaanxi being the AI center of the western region.

Compared to the number of AI talents, there is not much regional difference in academic performance. Beijing ranks first with an average H-index of 9, followed by Shanghai in second place with 8, and Zhejiang, Hunan and Tianjin, each with 7.

Figure 2-40 Distribution of Chinese AI talent

Among the cities, Beijing leads other cities by a big margin and is followed by Xi'an, Shanghai, Wuhan and Nanjing. As China's cultural center, Beijing has a high AI research intensity, with its AI talent force accounting for 13.5% of the national total. In the second echelon are Xi'an, Shanghai, Wuhan, and Nanjing, each with an AI talent force of over 10,000. In the third echelon are Changsha, Guangzhou, Chengdu, Harbin and Hangzhou, each with over 5,000.

Figure 2-41 Chinese AI talent by city

- **Distribution by universities**

China's AI talents are mainly concentrated in universities. There are 179,349 AI talents in universities nationwide, representing 81.3% of the national total, versus 19,422 in research institutions, or 8.8%, and 13,065 in enterprises, or 5.9%, slightly higher than the global average of 3%.

Figure 2-42 Chinese AI talent by affiliated entity type

Among the universities, Zhejiang University ranks first with 2,273 AI talents. Harbin Institute of Technology is in second place with 2,252. Shanghai Jiao Tong University is closely behind in third place with 2,211, followed by Northwestern Polytechnical University with 2,102 and Tsinghua University with 1,996. Compared to the commitment of international AI talent, there are significant changes in the overall ranking places, which show that Tsinghua University and Shanghai Jiao Tong University are in the lead nationwide in both international AI talent and top international AI talent, while Zhejiang University and Harbin Institute of Technology outperform in the number of AI talents active in China's domestic academic community.

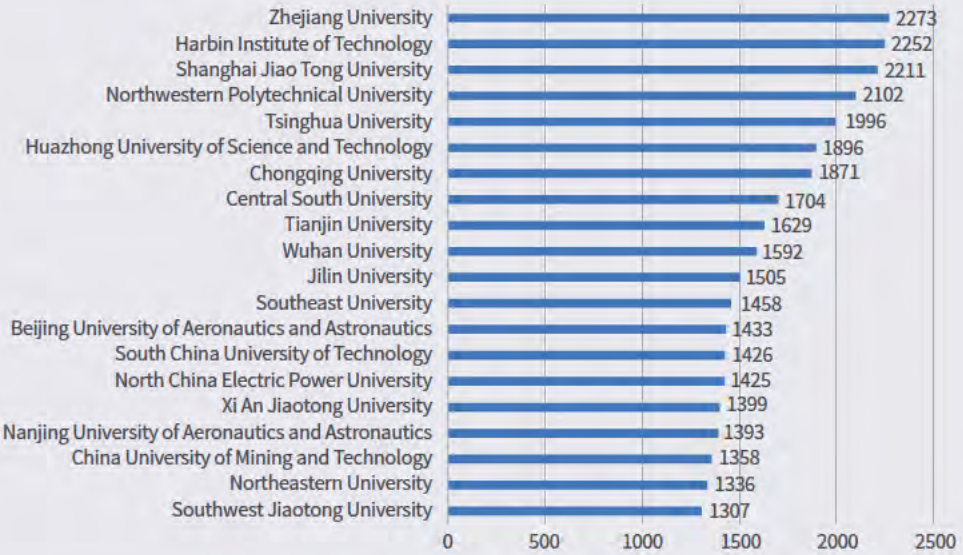


Figure 2-43 Top 20 Chinese universities by AI talent force

- **Distribution by research institutions**

The Chinese Academy of Sciences (CAS) System has the largest AI talent force in China. CAS has a total of 4,832 AI talents, with top-ranked members including Changchun Institute of Optics, Fine Mechanics and Physics (191), Institute of Computing Technology (188) and Shenyang Institute of Automation (135).

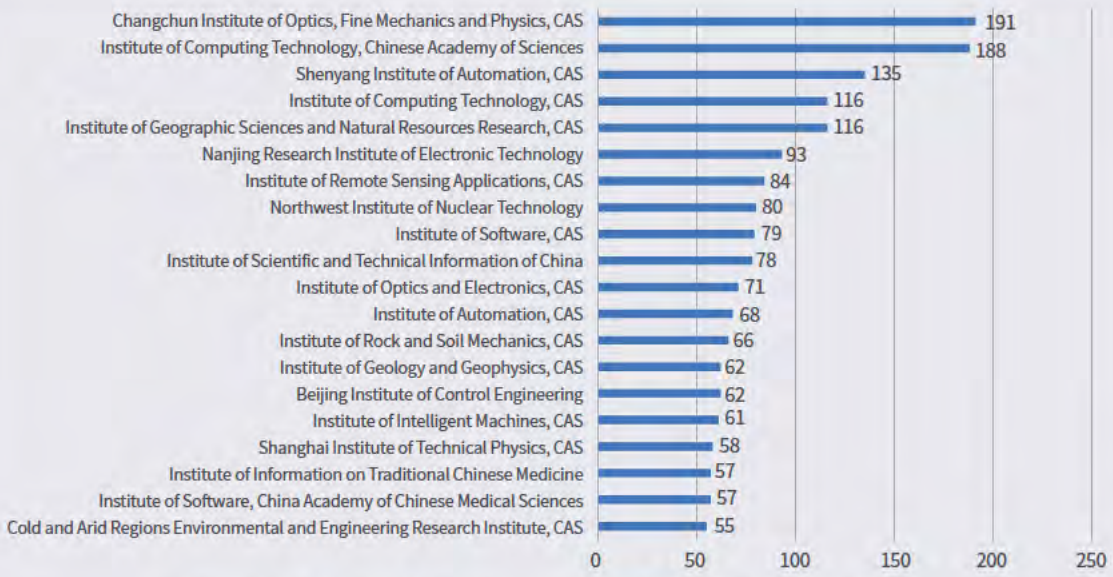


Figure 2-44 Top 20 Chinese research institutes by AI talent force

- **Distribution by research areas**

China's AI research areas are more dispersed. The top two research areas are genetic algorithm (42,706 AI talents) and neural networks (41,226), each representing more than 15% of the national total of AI talents. Other major research areas include fault diagnosis (25,161), data mining (23,976), BP neural networks (18,945) and support vector machine (18,783).

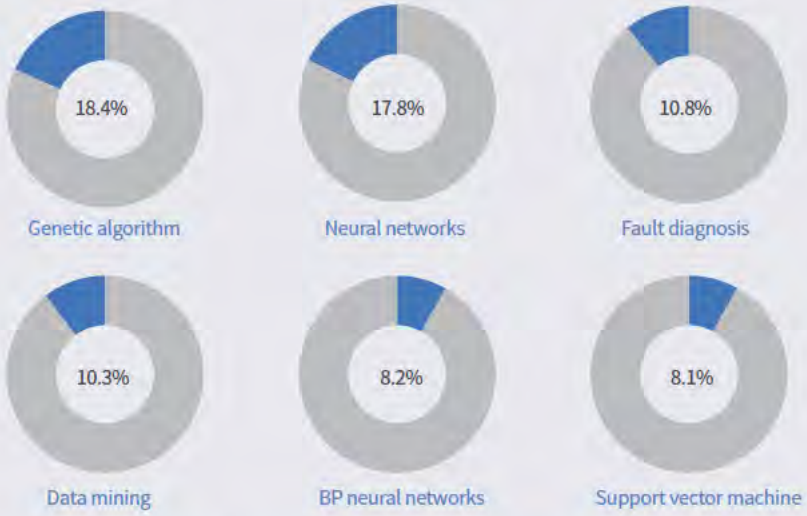


Figure 2-45 Chinese AI talent by research area

AI Industry Development and Market Applications

03 AI Industry Development and Market Applications

This chapter examines China's AI industry development from the perspectives of AI enterprises, venture capital investment, standard formulation, market size, and products and applications. In view of the wide applications of AI, AI enterprises in this report only include enterprises that have AI technologies or products as their core operations, as defined by the ICT industry monitoring platform of CAICT Data Research Center.

3.1 AI Enterprise Distribution

3.1.1 Regional Distribution of Chinese AI Enterprises

As of June 2018, there were 4,925 AI enterprises worldwide, with the United States having the greatest number at 2,028. China (excluding Hong Kong, Macao and Taiwan regions) came second with 1,011, followed by the United Kingdom, Canada and India.

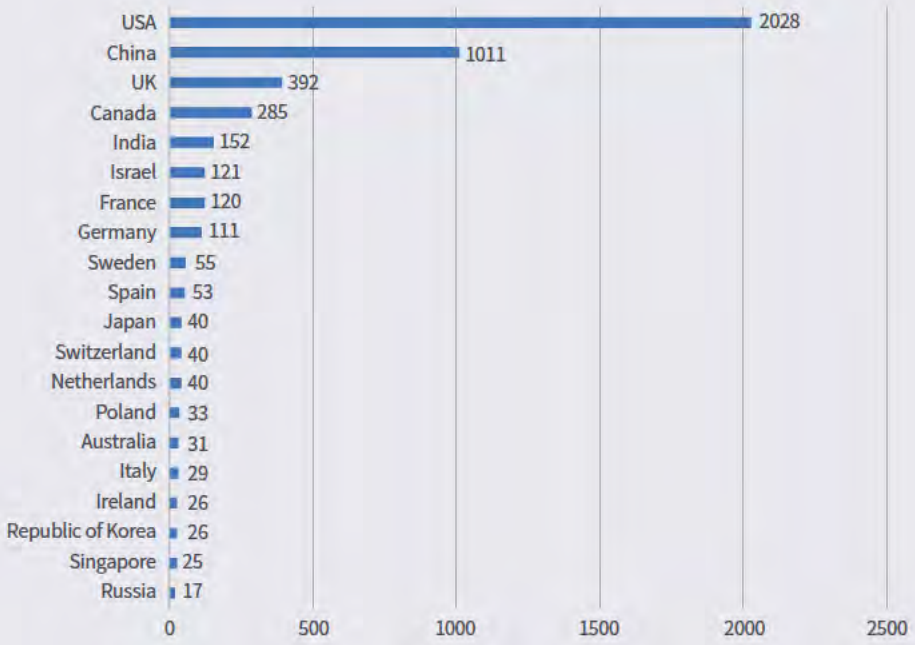


Figure 3-1 AI enterprises by country

The world's top 20 cities by the number of hosted AI enterprises include nine for the United States, four for China, three for Canada, and one for each of the United Kingdom, Germany, France and Israel. Among them, Beijing has the greatest number of AI enterprises in the world, followed by San Francisco and London. The other three Chinese cities on the list are Shanghai, Shenzhen and Hangzhou, respectively.

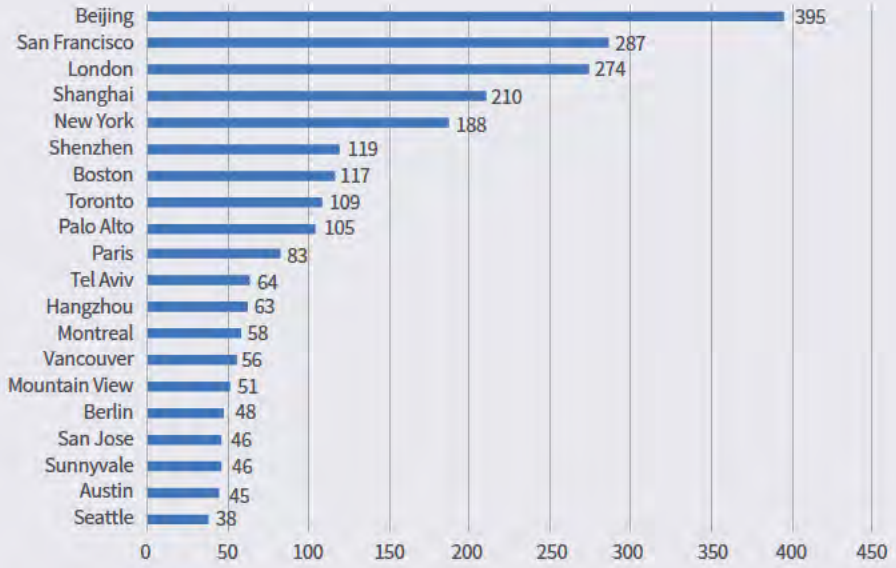


Figure 3-2 The world's top 20 cities by the number of hosted AI enterprises

In China, AI enterprises are mainly concentrated in Beijing, Shanghai and Guangdong. Beijing takes the lead with 395, far ahead of other regions. Zhejiang and Jiangsu provinces also have a fairly large number of AI enterprises.

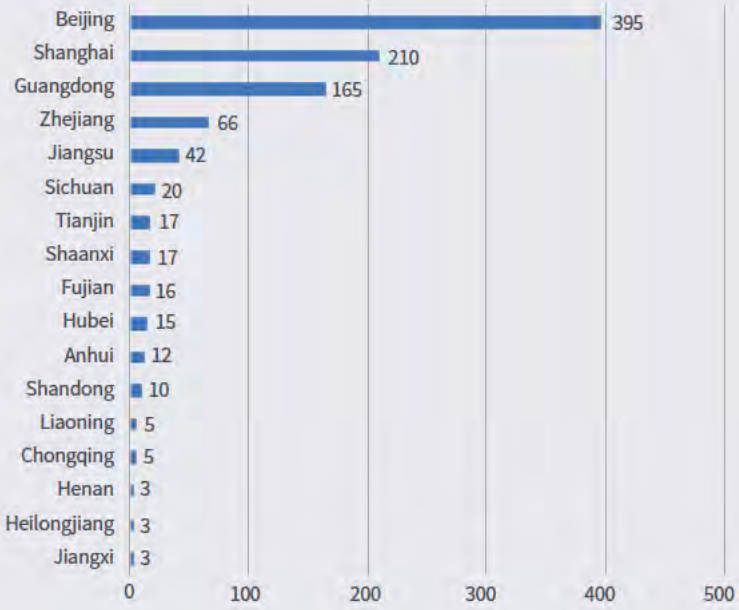


Figure 3-3 China's top provinces/municipalities by the number of hosted AI enterprises

3.1.2 Establishment Time of Chinese AI Enterprises

In terms of the time of establishment, most of Chinese AI enterprises were established between 2012 and 2016 and the growth peaked in 2015 with an addition of 228. After 2016, the growth of AI startups began slowing down.

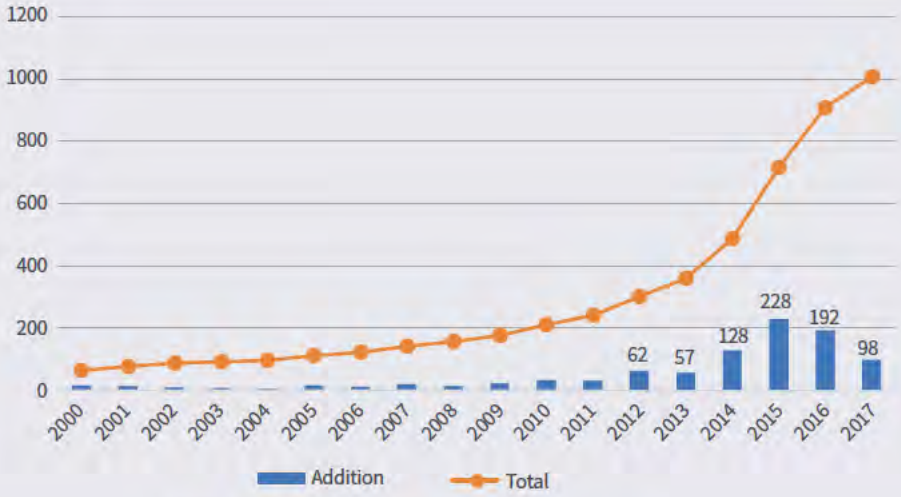


Figure 3-4 Growth of Chinese AI enterprises

Chinese AI enterprises have an average age of 5.5 years. Those in Beijing, Shanghai and Tianjin are younger than the national average. Those in Shandong and Liaoning, with many of them developed from well-established industrial robot and automation enterprises, are comparatively older.

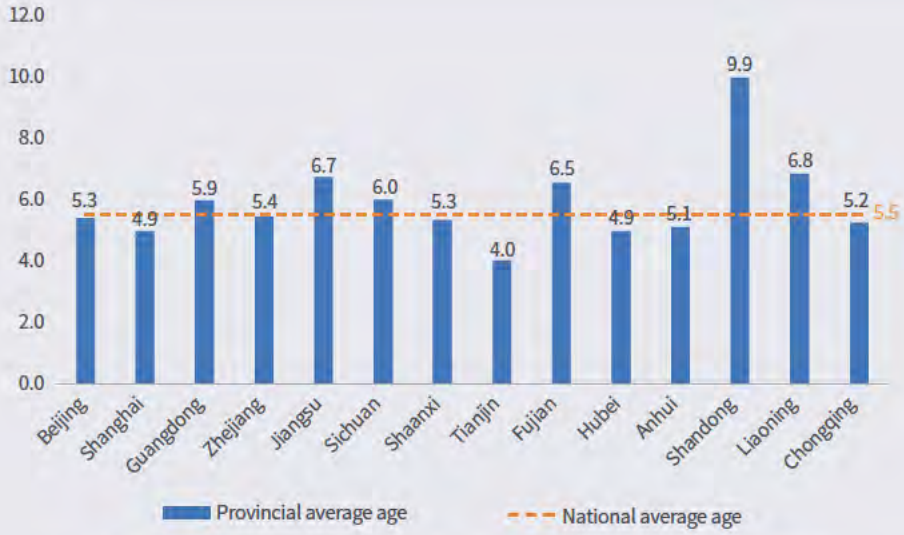


Figure 3-5 Average age of AI enterprises by province (unit: year)

3.1.3 Specialized Areas of Chinese AI Enterprises

Applied AI technologies mainly include voice technologies (speech recognition, speech synthesis, etc.), vision technologies (biometric recognition, image recognition, video recognition, etc.) and natural language processing technologies (machine translation, text mining, emotional analysis, etc.). With basic hardware included, the distribution of applied AI technologies of domestic and overseas AI enterprises is shown in Figure 3.6. Compared to their overseas counterparts, Chinese AI enterprises have a greater focus on vision and voice and are less focused on basic hardware.

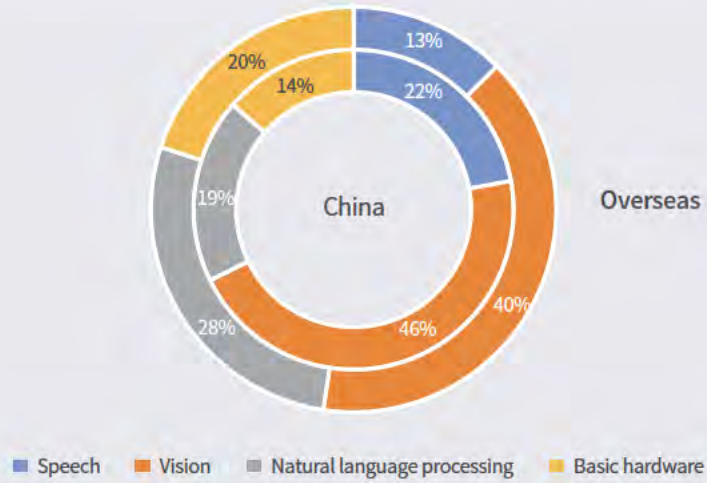


Figure 3-6 Distribution of applied AI technologies of AI enterprises in China and worldwide

The industry applications of AI include industrial robot, intelligent driving, drone, AR/VR, big data and data services, and various vertical applications (defined as "AI+" in this report). The distribution of industry applications of domestic and overseas AI enterprises is shown in Figure 3-7.

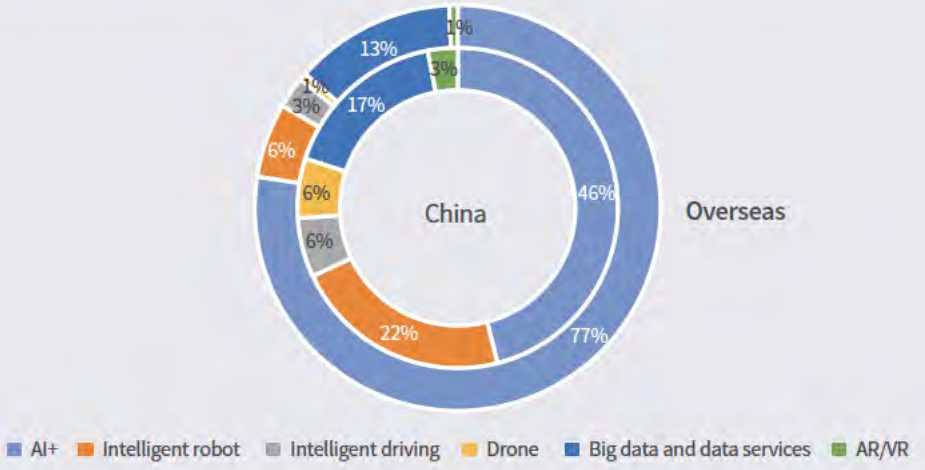


Figure 3-7 Industry distribution of domestic and overseas AI enterprises

It can be seen that domestic enterprises are more focused on terminal products such as intelligent robots, drones and smart cars, while foreign companies are more focused on the applications of AI in various vertical industries.

3.2 AI Industry Investment

3.2.1 Investment and Financing Scale of China's AI Industry

Since 2013, the global AI industry and the Chinese AI industry both have received steadily increasing investment. In 2017, global AI investment reached US$39.5 billion, including 1,208 investment transactions, with China alone posting US$27.71 billion of investment and 369 investment transactions. China's AI enterprises represented 70% of the global AI investment and 31% of global AI investment transactions.

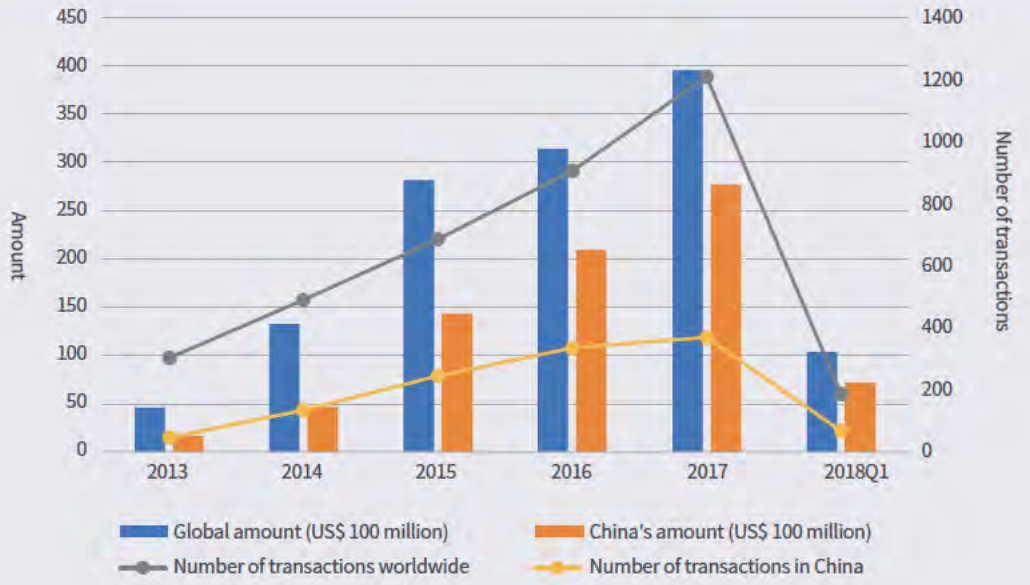


Figure 3-8 Trend of AI investment - worldwide and China

According to global investment and financing data for the period from 2013 to the first quarter of 2018, China surpassed the United States in financing scale to become the world's No. 1 destination of AI investment, though the United States kept its lead in terms of the number of investment transactions.

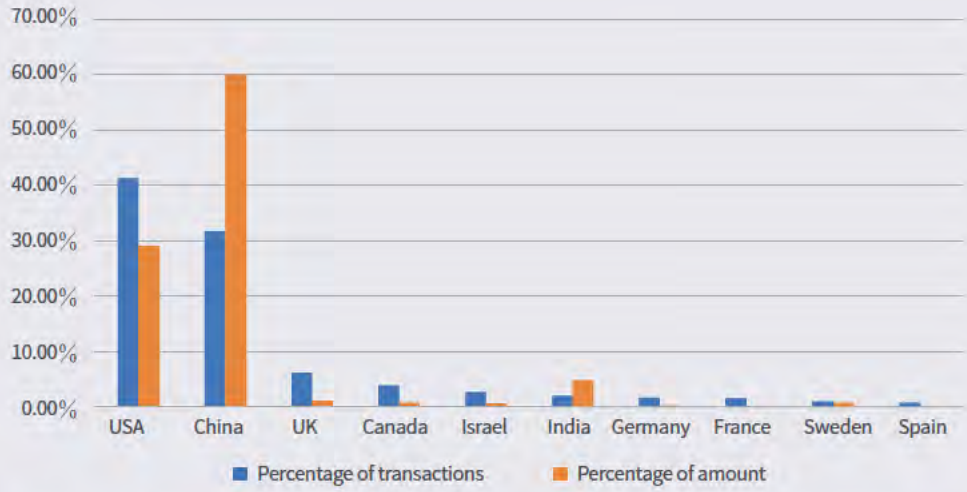


Figure 3-9 Distribution of global AI investment by country (2013 – Q1 2018)

3.2.2 Regional Differences of AI Industry Investment and Financing in China

Beijing led other provinces and municipalities in terms of financing amount and number of financing transactions. Provinces and municipalities including Shanghai, Zhejiang, Jiangsu and Guangdong also performed strongly. It merits noting that Guangdong, while receiving a comparatively less total amount of AI financing, had a high level of AI financing activity with its number of AI transactions being next only to that of Beijing and Shanghai. The AI financing amounts and numbers of AI financing transactions of the provinces are shown in Figure 3-10.

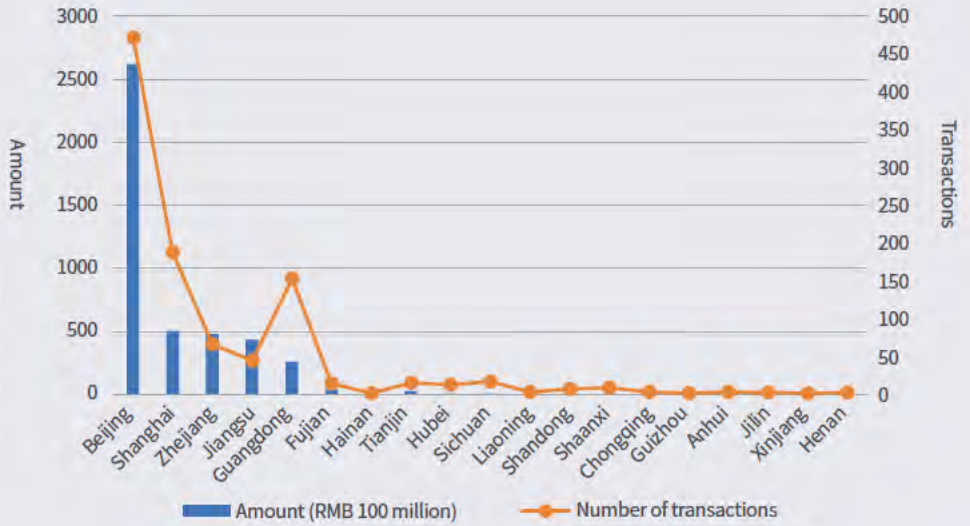


Figure 3-10 AI financing in China by region (2015 – Q1 2018)

3.2.3 Investment and Financing Round Changes in China's AI Industry

In terms of financing series, early-phase (Seed, Angel and Series A) financing as a percentage of the total AI financing began decreasing from 2015, indicating the increasing rationality of financing activity and the gradual maturing of the industry. The breakdown of domestic AI financing is shown in Figure 3-11.

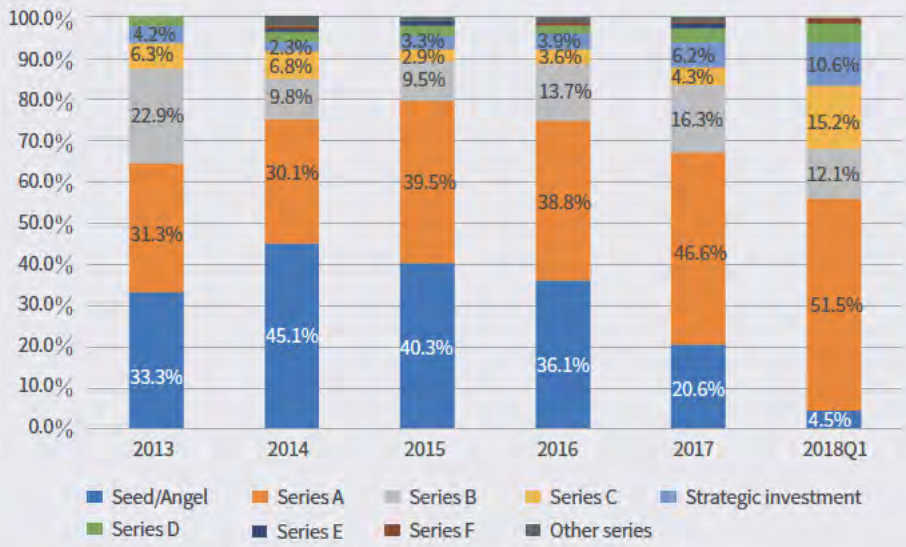


Figure 3-11 AI financing in China by series

3.3 Structure and Scale of The AI Market

3.3.1 Structure of China's AI Market

In 2017, China's AI market reached RMB23.74 billion, up 67% from 2016. The computer vision segment with technologies such as biometrics, image recognition and video recognition at its core was the largest segment, representing 34.9% of the market with RMB 8.28 billion.

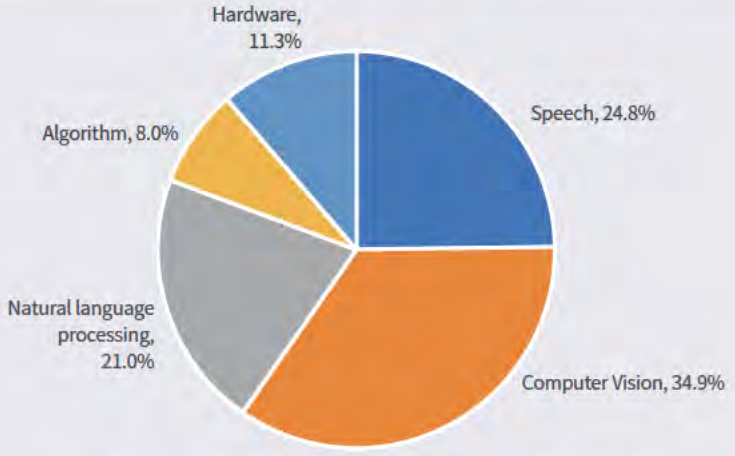


Figure 3-12 Structure of the Chinese AI market

3.3.2 Scale of China's AI Market

China's AI venture capital investment and financing fever began cooling off in 2017, but with the maturing of various AI technologies and their real-life applications, the AI market is expected to grow 75% to RMB 41.55 billion in 2018.

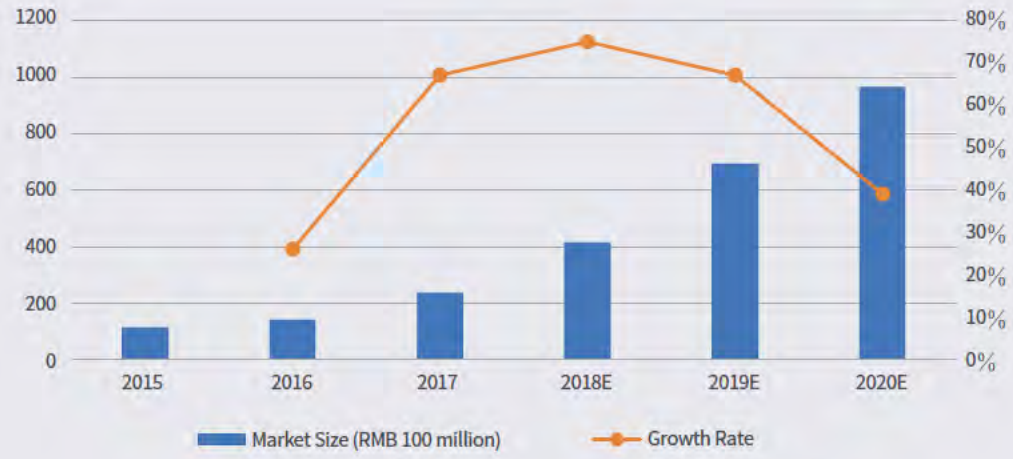


Figure 3-13 Size of the Chinese AI market 2015-2020

In 2018, the enhancement of machine learning and deep-learning algorithms will drive breakthroughs in computer vision, speech and related technologies. Core computing chips are also an important area where industry giants have made deployments, such as Google's upgraded TPU 3.0, NVIDIA's most powerful ever GPU, Chinese AI startup Cambricon's first cloud AI chip MLU100, and AI products rolled out by Chinese technology firms such as Alibaba, Huawei and Xiaomi which are expected to hit the market on a large scale soon. Against this backdrop, the AI industry will continue growing with accelerated integration with vertical industries.

3.4 AI Industry Standards

3.4.1 International AI Standards

With the development of the AI industry, international and domestic standardization organizations have started to work on AI standards Internationally, the joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC 1) has been engaged in AI standardization for more than 20 years. In the early stage, ISO/IEC JTC 1 has carried out relevant standardization in key areas such as AI terminology, human-computer interaction, biometrics, computer image processing, as well as in AI enabling technologies such as cloud computing, big data and sensor networks. ISO's work has been focused on AI standardization in areas including industrial robotics, intelligent finance and intelligent driving. IEC's work has been focused on AI standardization for wearable devices.

In addition, the Institute of Electrical and Electronics Engineers (IEEE) has focused on the research of AI ethics and approved seven IEEE standards. The U.S. National Institute of Standards and Technology (NIST) has conducted research in various AI areas including AI acquisition and analysis tools, future expert systems, AI-based collective production quality control, high-throughput material discovery

and optimization, and optimized applications of machine learning, but has not yet worked on or released any related standards.

3.4.2 Chinese AI Standards

In China, the Standardization Administration of China (SAC) has done standardization work in areas such as terminology, human-computer interaction, biometrics, big data and cloud computing and released a series of standards and norms (see Appendix 4 for details).

3.5 AI Products and Applications

With the continuous evolution and improvement of algorithms and computes, there have been more and more applications and products based on speech recognition, natural language processing and vision technologies. Typical ones include interactive products (such as smart speakers, smart voice assistants and intelligent in-vehicle systems), intelligent robots, drones and autonomous cars. In industry solutions, AI is even more widely applied and has been used in multiple vertical areas including healthcare, finance, education, security, business, and smart home.

3.5.1 AI-Powered Devices

As AI remains in the development stage and next-generation AI technologies such as machine learning and deep learning have been mainly confined to algorithms, mature AI devices are not very many. The following sections focus on three AI products that have been fairly mature and reached a certain market scale—smart speaker, smart robot and drone.

- **Smart speaker**

The AI interactive speaker market has seen a compound annual growth rate of 30% in recent years and is expected to grow from US$1.15 billion in 2017 to US$3.52 billion in 2021.

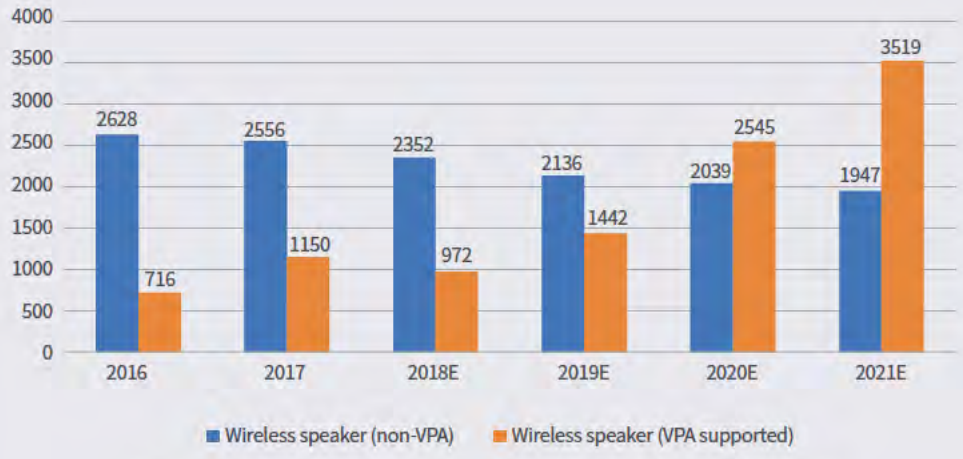


Figure 3-14 Global smart speaker market size (US$ 1 million)

Major products in the global smart speaker market are shown in Table 3-1.

Table 3- 1 Major smart speaker products in the market

	Vendor	Product Name
China	Baidu	Xiao Du
	Tencent	Tencent Tingting
	Xiaomi	Xiao AI
	Alibaba	Tmall Genie
	JD	Dingdong
Overseas	Amazon	Echo Series
	Google	Google Home Series
	Apple	HomePod
	Microsoft	Invoke

According to data released by research firm Canalys in May, Google had surpassed Amazon to lead the global smart speaker market. In the first quarter of 2018, Google sold 3.2 million smart speakers, representing 36.2% of the market. Amazon came in second place with 2.5 million Echo smart speakers sold, representing 27.7% of the market. China's Alibaba and Xiaomi came third and fourth, taking up a market share of 11.8% and 7.0%, respectively.

Table 3-2 Global smart speaker market share by vendor

Rank	Vendor	Q1 2017	Q1 2018	Y/Y growth
#1	Google (Home Series)	19.3%	36.2%	483%
#2	Amazon (Echo Series)	79.6%	27.7%	8%
#3	Alibaba (Tmall Genie)	-	11.8%	-
#4	Xiaomi (Xiao AI)	-	7.0%	-
Other Vendors		1.1%	17.3%	161%
Overall market (US$)		2.9 million	9 million	210%

Data source: Canalys

- **Intelligent robot**

Key technologies for intelligent robots include vision, sensing, human-computer interaction and mechatronics. From the application point of view, intelligent robots can be divided into industrial robots and service robots. Industrial robots generally include handling robots, palletizing robots, painting robots, and collaborative robots. Service robots can be divided into professional service robots and personal/home robots. Professional service robots include intelligent customer service, medical robots, logistics robots and receptionist robots; personal/home robots include personal virtual assistants, homework robots (such as home cleaning robots), children's educational robots, elderly care robots, and emotional support robots.

The structure of global intelligent robot enterprises is shown in Figure 3-15.

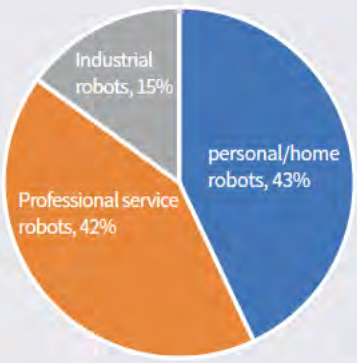


Figure 3-15 Global intelligent robot enterprises by type

According to data released by IFR in June 2018, the global robot market reached US$50 billion in 2017. The market posted 380,000 industrial robots sold in 2017, up 29% y/y. China has been the world's largest industrial robot market since 2013. In 2017, China posted 138,000 industrial robots in sales, followed by Korea with approximately 40,000 and Japan with approximately 38,000. In the Americas, the United States is the largest single market, selling approximately 33,000 industrial robots in 2017. In Europe, Germany is the largest seller with approximately 22,000 industrial robots sold. The top five countries - China, Korea, Japan, United States and Germany - combined to take up 71% of the global industrial robot market in 2017.

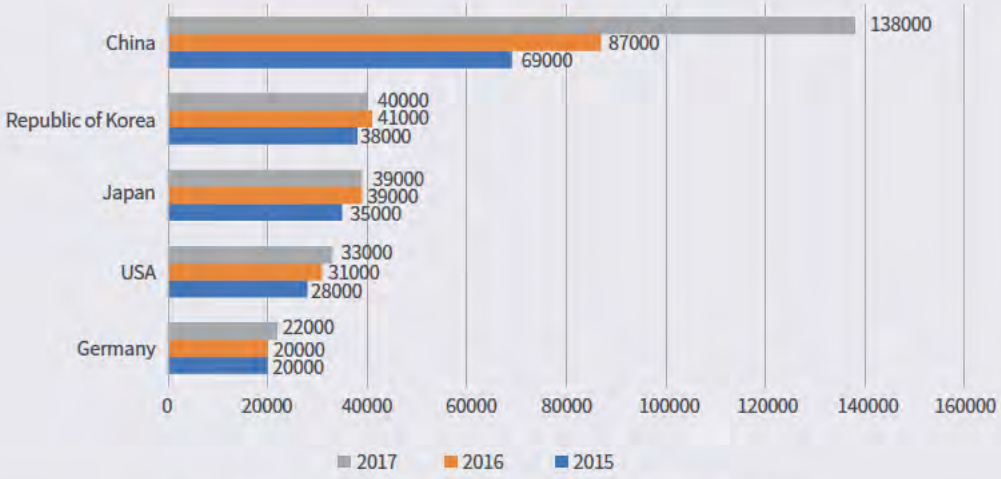


Figure 3-16 Industrial robot shipments in major markets

- **Drone**

At present, the drone market is mainly composed of consumer drones and commercial drones. Consumer drones are mainly used for entertainment scenarios such as aerial photography and tracking shots. Commercial drones have very wide applications

in many areas such as agriculture, forestry, logistics, security and patrol.

Consumer drones are generally priced below US$5,000 with a battery range of not more than one hour. Compared to consumer drones, commercial drones have a higher payload and longer flying time and are the most successfully applied in industrial fields. Commercial drones, small in shipments but high in prices, take up two-thirds of the revenue of the drone market.

Gartner predicts that the global drone market will reach US$7.3 billion with 3.13 million drones sold in 2018, up 28% from 2017.

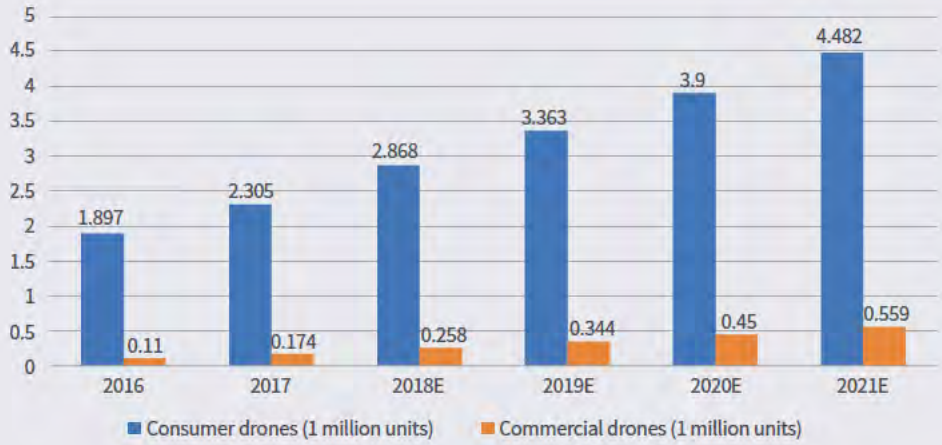


Figure 3-17 Global drone shipments from 2016 to 2021

DJI is the most influential drone manufacturer in China. It is focused on consumer drones but is also expanding in the commercial drone market. DJI is the clear leader in the global consumer drone market.

According to its financial data, DJI achieved RMB 17.57 billion in 2017, up 79.6% y/y. Data from drone market research firm Skylogic Research shows that DJI has taken up 50% of the North American market. For drones that cost between US$500 and US$1,000, DJI represented 36% of the market by units sold in North America in 2017. DJI also fetched 66% of the North American market for drones priced between US$1,000 and US$2,000, and 67% of the market in the US$2,000-US$4,000 range.

Besides DJI, other Chinese drone manufacturers such as EHANG, Zero Zero Robotics, Zerotech and XAG have also achieved rapid development and are fairly influential.

3.5.2 Industry Applications of AI

Compared to terminal products, AI has found more diversified applications in industrial fields. The following sections examine AI applications in smart healthcare, smart finance, smart security, smart home, and smart grid.

- **Smart healthcare**

As AI finds increasing real-world use, there have been quite a few success stories of AI rendering superior healthcare services. AI has been applied in many aspects of healthcare such as intelligent diagnosis and treatment, medical image analysis,

medical data management, health management, precision medicine, and new drug research and development.

Traditionally, doctors rely on their own medical knowledge and clinical experience to make a diagnosis according to symptoms and testing results. Today, they have got a super assistant in the form of a smart diagnosis and treatment system capable of "learning" specialized medical knowledge, "remembering" massive medical records and "reading" diagnostic imaging reports. IBM's Watson Health has furnished a compelling example with its ability to read 3,469 medical books, 248,000 papers, 69 therapeutic plans, results of 61,540 experiments and 106,000 clinical reports in only 17 seconds. Watson Health passed the U.S. Medical Licensing Exam in 2012 and has been deployed in multiple hospitals in the United States to provide assistant medical services. Currently, Watson Health can diagnose multiple cancers including breast cancer, lung cancer, colon cancer, prostate cancer, bladder cancer, ovarian cancer and uterine cancer.

- **Smart finance**

Smart finance is the integration of AI technologies and the financial system. AI applications in the financial sector mainly include AI financial advisor and intelligent financial fraud detection, among others.

AI financial advisor is now a common Fintech application scenario. An AI financial advisor, powered by machine learning algorithms, can automatically build investment portfolios according to a customer's investment goal, age, income, existing assets and risk tolerance to achieve their return target. In addition, the algorithms can automatically update investment strategies according to goal and market changes to maintain the optimal investment portfolio for their investment goals. Some major investment firms in the United States such as Betterment and Wealthfront have launched their AI-powered, low-priced financial advisor services which have been embraced and recognized by younger investors.

Traditional financial fraud detection systems rely heavily on rules that are complex and rigid and have become powerless in the face of continuously evolving and increasingly sophisticated fraud practices and techniques. Frauds based on forgery and impersonation have become common occurrences and caused massive losses to financial institutions and consumers. Chinese fintech companies represented by anti-fraud solution provider Maxent have developed AI-powered automatic intelligent anti-fraud technologies and systems that help enterprises build user behavior tracking and analysis and automatic anomaly detection capabilities to achieve controlled real-time identification of new fraud patterns.

- **Smart security**

Security is another area where AI has been successfully applied. AI-powered security involves algorithms and model training based on massive image and video data to provide comprehensive protection including early warning, effective response and post-incident handling.

At present, AI-powered security is mainly for police and civilian use. In the field of police use, applications in public security management are the most representative, where AI technologies are used to analyze in real time image and video content, collect human and vehicle information and identify criminal suspects, bringing substantial efficiency improvement and time savings. In the civilian use direction, AI enables intelligent building management and intelligent monitoring of industrial areas. Intelligent building management includes many AI-enabled applications such as face

recognition-based entry/exit management, theft identification and unauthorized access detection. In industrial areas, fixed cameras and patrol robots can be combined to implement real-time monitoring of all places and give alerts on potential hazards. Another important scenario of civilian use of AI is home security. A home security camera system, for example, is automatically activated when it detects no family member in the home and gives alarms and at the same time remotely notifies family members when it detects an intrusion. The system is automatically deactivated when any family member comes home for privacy protection.

Many Chinese security companies have developed their AI solutions and products. Traditional video surveillance companies such as Dahua, Hikvision and NetPosa have stepped up development of intelligent products. Companies that specialize in algorithms like SenseTime, Face++, CloudWalk and YITU Tech are focused on image processing areas such as face recognition and behavior analysis.

- **Smart home**

Smart home is an IoT-based home management system comprising hardware, software and a cloud platform. Integrating extensive functions such as home appliance control, human-machine interaction, interconnectivity of devices, user behavior analysis and user profiling, it brings the modern family with personalized services for greater convenience, comfort and security.

For examples, speech recognition and natural language processing technologies enable users to control smart home devices, such as curtains (windows), lights and TV sets by talking to them and telling them what to do; smart devices such as smart TV and smart speaker that are empowered by machine learning and deep learning technologies can learn about the user through their subscriptions or use history and recommend content according to their interests and preferences. In home security, biometric technologies such as face recognition and fingerprint recognition can be used to enable biometric door access, in addition to real-time camera monitoring and unauthorized intrusion detection.

In China, technology firm and device maker Xiaomi has established a complete system of R&D, manufacturing and selling of smart home devices, and its smart home ecosystem has had as many as more than 60 million connected devices. In addition, traditional home appliance makers Midea, Haier and Gree, leveraging their massive product lines and high market shares, have also actively pursued a smart home transition and pushed ahead with their smart device strategy.

- **Smart grid**

As power grids become increasingly extended, AI will become integral to their efficiency and adaptability. On the demand side, AI technologies will enable continuous monitoring of electricity usage of households and businesses through smart meters and sensors and electricity scheduling in a safer and more reliable, economical and efficient way.

On the supply side, AI technologies will help power grid operators or governments to optimize the energy mix, adjust the use of fossil energy sources, increase the production of renewable energy, and reduce the impact of renewable energy intermittency to the minimum. Energy producers will be able to manage energy output from different sources to continuously match supply with demand changes according to social, spatial and time changes.

In terms of line inspection, intelligent patrol robots and drones equipped with sophisticated sensors and detectors makes the inspection work more accurate, more efficient and safer. As for data diagnostics, intelligent patrol robots not only offer

more precise diagnosis than human eyes and all types of hand-held devices, but also support automatic operation round the clock, thus greatly expediting fault identification. Meanwhile, history inspection data can be analyzed to reveal hidden patterns and degradation trends of equipment and inform scientific formulation of maintenance and repair strategies. Drones fitted with high-resolution cameras capable of high-accuracy positioning and automatic detection can hover over power towers dozens of meters high, take photographs of them, and identify even the slightest disjunction. According to its official data, Guangdong Power Grid performs aerial power line inspection of over 180,000 km annually, equivalent to 4.5 times the earth's circumference, 85% of which is conducted by drones, representing the largest drone inspection workload in the world. Drone inspection has increased its overall inspection efficiency by 2.6 times.

AI Development Strategy and Policy Environment

04 AI Development Strategy and Policy Environment

This chapter compares and analyzes AI development from the perspective of international policy (United States, European Union, Germany, United Kingdom, France, Japan and Republic of Korea), China's national policy, and China's provincial-level government policy.

4.1 International AI Strategy and Policy

4.1.1 Key AI Policy Initiatives in Major Countries and Regions

In recent five years, countries have paid increasing attention and stepped up efforts to promote AI research and rolled out their national AI strategies and policies. The United States' AI policy documents include The National Artificial Intelligence Research and Development Strategic Plan; Artificial Intelligence, Automation, and the Economy; Preparing for the Future of Artificial Intelligence; and Artificial Intelligence White Paper.

The European Union has released policies and plans including Strategic Research Agenda For Robotics in Europe 2014-2020, Robotics 2020 Multi-Annual Roadmap, Gauging the Future of EU Research & Innovation, Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics, and Civil Law Rules on Robotics.

Germany has released Die neue Hightech-Strategie Innovationen für Deutschland (New High-Tech Strategy Innovations for Germany), Technik zum Menschen bringen-Forschungsprogramm zur Mensch-Technik-Interaktion ("Bringing Technology to the People" Research Program on Human-Machine Interaction), BMBF gründet Plattform "Lernende Systeme" (BMBF launches Platform for Learning Systems), Innovation Policy, and Präsentation zur Künstlichen Intelligenz (Presentation on Artificial Intelligence) co-prepared with France.

The United Kingdom has released RAS 2020 Robotics and Autonomous Systems, Industrial Strategy: Building a Britain Fit for the Future, Growing the Artificial Intelligence Industry in the UK, and Robotics and Artificial Intelligence: Government Response to the Committee's Fifth Report of Session 2016–17.

France's AI policy documents include For a Meaningful Artificial Intelligence—Towards a French and European Strategy and Präsentation zur Künstlichen Intelligenz (Presentation on Artificial Intelligence) co-prepared with Germany.

Japan has released two major AI policy documents—Japan Revitalization Strategy 2016 and Artificial Intelligence Technology Strategy: Report of Strategic Council of AI Technology.

Since 2013, China has released a series of AI and related policy documents, including State Council Guidelines on Promoting the Healthy and Orderly Development of the Internet of Things, State Council Notice on Issuing "Made in China 2025", State Council Guidelines on Promoting the "Internet+" Action, State Council Notice on Issuing the Action Outline for Promoting the Development of Big Data, Thirteenth Five-year Plan on National Economic and Social Development, and State Council Notice on Issuing the "Next Generation

Artificial Intelligence Development Plan" released in 2017, referred to in the media as "Year 1 of AI development in China", which identifies the development directions and priority areas of China's AI development.

Figure 4-1 provides a survey of AI strategies and policies released by the United States, European Union, Germany, United Kingdom, France, Japan and China since 2013. The United States' AI policies are geared to dealing with the general trend of AI development and the impact and changes it may bring to the national security and social stability in the long term, and maintaining the leading position of the United States as a technology superpower in AI development and its key areas (internet; computer software and hardware such as chips and operating systems; and finance, military and energy areas). The United States strives to take a full measure of the effects of AI-driven automation on the economy, examine the opportunities and challenges that AI will bring to employment, and come up with strategies to deal with them. The European Union and European countries represented by Germany, United Kingdom and France stress the ethical and moral risks of AI development and in policymaking focus on how to respond to the potential security, privacy, integrity and other ethical threats posed by AI to humankind. Japan's AI policies, launched rather recently, have been geared to establishing a fairly comprehensive AI research advancement mechanism with a view to leveraging AI to promote its "Society 5.0" building.

China's AI policies in the early phase were tilted towards the Internet and therefore applications-oriented and focused on such areas as computer vision, natural language processing, intelligent robots and speech recognition. Despite having built some advantages in these areas, China's AI development was less than balanced when compared to the AI deployments of the United States. Therefore, China's current AI strategy emphasizes systematic deployments at the national level with a view to, as stated in the report to the 19th CPC National Congress, "promoting further integration of the internet, big data, and artificial intelligence with the real economy", by emphasizing the establishment of an open and collaborative AI technology and innovation system, grasping AI's characteristic of high integration of technological attributes and social attributes, adhering to the "three in one" synergy of AI R&D, product application and industry fostering, and strengthening AI's comprehensive support for technological, economic and social development and national security.

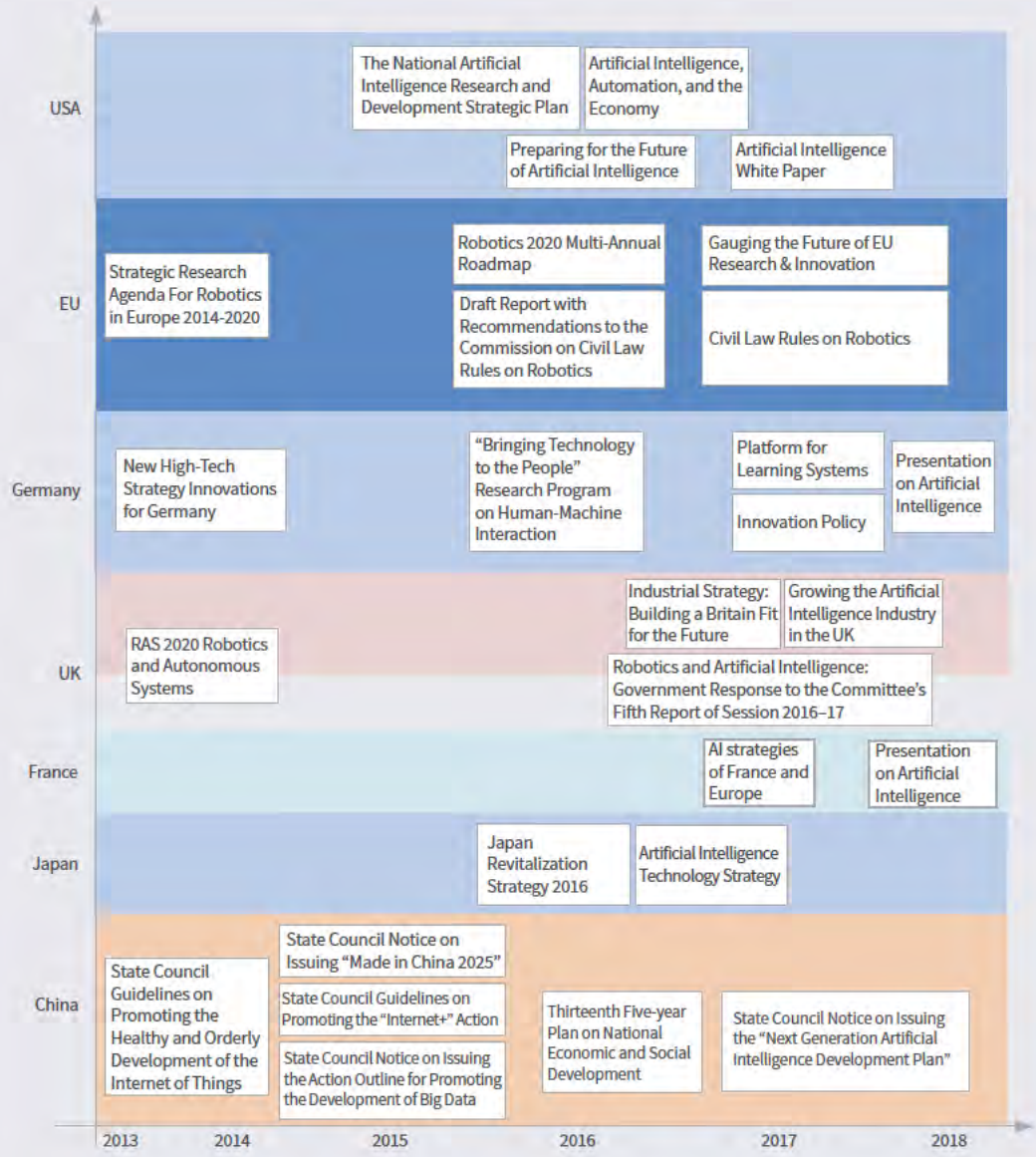


Figure 4-1 AI strategy and policy documents worldwide

4.1.2 Key AI Research and Application Areas in Major Countries and Regions

Because of significant differences among countries in their level of technological development and national conditions, their AI policies vary greatly in terms of priority areas of research and application.

Table 4-1 AI policies and priority areas worldwide

	Key research areas	Key application areas
USA	President Trump's FY2019 budget request was the first in American history to designate artificial intelligence and autonomous and unmanned systems as Administration R&D priorities. The Trump Administration's "Budget Blueprint to Make America Great Again" gives prioritized support to homeland security, military defense and medical care.	Homeland security: Face recognition, Flood Apex Program, wearable alarm system, etc. (The Department of Homeland Security has issued the Artificial Intelligence White Paper and Report on the Executive Summary of Emerging Technologies Strategy to the President (Draft)); Medical imaging (The Roadmap for Medical Imaging Research and Development has been released, which mentions the coordination between AI and medical imaging); National defense and military (Special Program Announcement for 2018 Office of Naval Research Basic Research Opportunity: "Advancing Artificial Intelligence for the Naval Domain")
EU	Data protection; network security; AI ethics; digital technology training; e-government	Supercomputer; data processing; financial economy; digital society; education
Germany	Human-computer interaction; cyber-physical system; cloud computing; computer identification; intelligent service; digital network; microelectronics; big data; network security; high-performance computing	Intelligent transportation (land, sea and air); healthcare; agriculture; ecological economy; energy; digital society
UK	Hardware CPU; identification	Underwater robotics; offshore engineering; agriculture; aerospace; mineral collection
France	Supercomputer	Ecological economy; gender equality (AI education for women); e-government; medical care
Japan	Robotics, brain-to-brain communication, sound recognition, language translation, social knowledge analysis, innovative network construction, big data analysis, etc.	Production automation, Internet of Things, medical health and care, space movement (automatic driving, unmanned delivery, etc.)
China	Key Generic Technologies System "1+N" Plan: "1" refers to the next-generation AI major S&T project which focuses on basic theories and key generic technologies; "N" refers to AI theoretical research, technological breakthroughs and product development and applications. Efforts are also outlined to strengthen interdisciplinary research and free exploration in the frontiers of artificial intelligence.	Smart manufacturing; smart agriculture; smart logistics; smart finance; smart commerce; smart home; smart education; smart pension; administrative management; judicial management; urban management; environmental protection Strengthening demonstration and application of AI technologies in key projects such as deep underwater space station, health security, smart city and smart agricultural machinery.

The Trump administration initially reacted slowly and indifferently to the rise of artificial intelligence, but this situation is undergoing changes. At the recently concluded "Artificial Intelligence for American Industry" summit, the White House announced the establishment of the Select Committee on Artificial Intelligence to examine U.S. priorities and investments on AI development. The R&D budget will focus on autonomous and unmanned systems, especially in such areas as homeland security and national defense. In application innovation, AI has been widely applied in different sectors in the United States such as homeland security, medical imaging, and national defense and military, with applications including face recognition and wearable alarm systems in homeland security and AI-powered medical imaging in medical care.

The European Union has attached great importance to AI and actively united its member states to conduct related legislative discussions. Most EU countries have joined the Horizon 2020 program and the SPARC robotics program in an effort to improve Europe's overall competitiveness through innovation in this field. Some EU countries, such as Italy and Finland, have not yet formed a unified government-level strategic policy, but their major universities and research institutions have undertaken their national research tasks in the field of AI. In general, the EU pays more attention to AI's impact on human society. Its research usually involves social sciences such as data protection, network security and AI ethics. At present, it has also invested considerably in digital technology training and e-government related research. In applications, the EU stresses AI-related basic research and has spent heavily on supercomputers and data processing applications in particular. The EU has also shown interest in in-depth AI applications in such fields as financial economy, digital society and education.

Germany, which launched its "Industry 4.0" program in 2013 leveraging its strong industrial infrastructure, has prioritized human-computer interaction, cyber-physical systems, cloud computing, computer identification, intelligent services, digital networks, microelectronics and big data, network security and high-performance computing. In AI applications, it has focused on intelligent transportation, healthcare, agriculture, ecological economy, energy digital society and other fields, involving all aspects of German society.

The United Kingdom is committed to the R&D of AI technologies in the fields of hardware CPU and identification. In applications, it has widely applied AI technologies in areas including underwater robotics, offshore engineering, agriculture, aerospace and mineral collection. Compared to the United States and Germany, the United Kingdom is more confined in both research and applications of AI but has greater specificity and depth with an emphasis on practicality. Meanwhile, the UK government has also emphasized AI talent development and invested heavily in technical colleges which have attracted many high-level specialists from universities.

France has allocated a lot of resources for R&D of AI-related supercomputers. In AI applications, it has focused on ecological economy, gender equality, e-government and medical care. When it comes to practicality, France has paid close attention to industries that are closely related to AI such as healthcare and autonomous cars and adopted a more cautious attitude towards investment in new AI research areas, with its R&D priorities concentrated in traditional fields.

Japanese society has always had a strong interest in robotics-related R&D and manufacturing. Japan has invested greatly in the fields of robotics, brain-to-brain communication, sound recognition, language translation, social knowledge analysis,

innovative network construction and big data analysis. In AI applications, Japan has focused on two lines: 1) traditional robot manufacturing and applications to achieve production automation, automatic delivery and large-scale IoT deployment in replacing workers; and 2) AI-powered medical care and autonomous vehicles to solve the country's increasing population ageing. It can be seen that Japan's AI R&D and applications are geared to solving specific real-world issues while reflecting its traditional cultural setting.

China's AI development is guided by the "1+N" planning system and has its focus on basic theories and key technologies while also supporting free exploration in interdisciplinary research. In applications, China has highlighted the important role played by AI in extensive fields including smart manufacturing, smart agriculture, smart logistics, smart finance, smart commerce, smart home, smart education, smart healthcare, smart pension, administrative management, judicial management, urban management, environmental protection and underwater space exploration. It can be seen that China's AI research and applications have been driven by the pursuit of sustainable economic and social development and cover wide research and application areas with a view to achieving comprehensive development of the AI industry.

4.1.3 AI Policy Advancement Agencies in Major Countries and Regions

The United States' AI policy steering agencies are the National Science and Technology Council (NSTC), the Office of Science and Technology Policy (OSTP) and the Office of Management and Budget (OMB). Through the joint efforts of the U.S. government and the private sector, the NSTC Subcommittee on Machine Learning and Artificial intelligence and the Select Committee on Artificial Intelligence were established to facilitate AI industry financing. In 2016, NSTC and NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD) jointly released the National Artificial Intelligence Research and Development Strategic Plan which states that NSTC is the principal means by which executive branches coordinate science and technology policy across diverse entities. NSTC oversees the working groups focused on different aspects of AI, and establishes clear national goals for Federal science and technology investments. This makes NSTC an important agency for AI investments.

The EU AI policy's two principal driving forces are the European Commission (EC) and the European Parliament Committee on Legal Affairs (JURI), which not only design AI development plans but also address issues that AI development may encounter. In 2013, the EC and euRobotics jointly launched the SPARC robotics program aimed at driving Europe's robotics development, promoting industry and supply chain development, and encouraging the development of robotic technologies. The JURI committee has proposed bills that emphasize research on legal issues relating to robotics and AI development and related issues such as ethics, safety and intellectual property protection. Subsequent agencies that have come to the AI scene include euRobotics, SPARC, European Robotics Technology Platform (EUROP) and European Robotics Network (EURON). Among them, euRobotics launched the SPARC robotics program and Horizon 2020 initiative and set forth a robotics development roadmap. Other agencies such as EUROP and EURON play an important organizing and coordinating role and promote AI research and industry development by integrating AI research institutes and researchers.

Germany's main AI policy steering agencies are the federal government, Federal Ministry of Education and Research (BMBF), Federal Ministry for Economic

Affairs and Energy (BMWi) and German Academy of Science and Engineering (acatech), which lead Germany's AI policy making and implementation. Among them, BMBF is directly involved in AI technology development, such as in the service robot project. BMWi supports six robotics projects and conducts research on robotic autonomous learning and behavioral decision-making models. Other mechanisms later introduced such as Industry 4.0 Platform in 2013, Platform for Learning Systems in 2017 and German-French Artificial Intelligence Joint R&D Center and German Research Center for Artificial Intelligence (DFKI) in 2018 are also important R&D instruments of Germany's AI policy.

The United Kingdom has put in place a well-functioning AI development ecosystem comprising researchers, developers and enterprises, where the main driving forces of AI policy are the Engineering and Physical Sciences Research Council (EPSRC), Royal Academy of Engineering, and subsequently established or introduced entities such as the RAS Leadership Council, the National Artificial Intelligence Research Center and the UK AI Council. The British government has hoped to make the UK an innovation center for artificial intelligence and to establish a partnership with the industry to promote artificial intelligence in various fields. In this context, the AI Council came into being. The council is a body of publicizing and promoting AI that comprises AI researchers and provides scientific data and reference for the government's AI reports. It conducted discussions on AI applications in the medical sector and has become an important factor in the UK government's AI policymaking.

France has made active efforts to advance AI innovation and R&D, leveraging the opportunities from the EU's robotics development. The main driving forces of France's AI policy making include the French Parliament, French Institute for Research in Computer Science and Automation, French Digital Council and Directorate General of Armaments (DGA). At the same time, France's AI research has also focused on the ethical issues relating to AI industry development, and this concern led to the establishment of an AI ethics committee to advance the country's AI strategy with a series of measures to establish a fair and sound assessment system to ensure that data is appropriately used and avoid any misleading use of AI.

In Japan, Prime Minister Shinzo Abe proposed the establishment of AI R&D targets and industrialization roadmap at the 5th Public-Private Dialogue towards Investment for the Future held in April 2016. After that, the Japanese government officially set up the Artificial Intelligence Technology Strategy Council that serves as a national-level general management agency that coordinates the Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry to jointly promote AI technology R&D and applications. Among them, the Ministry of Internal Affairs and Communications is mainly responsible for AI development in areas including brain-to-brain communication, sound recognition, language translation, social knowledge analysis and innovation network, with efforts led by the National Institute of Information and Communications Technology under it; the Ministry of Education, Culture, Sports, Science and Technology is mainly responsible for AI development in areas including basic research, innovation based on relevant S&T achievements, development of emerging next-generation basic technologies, provision of high-performance computing resources and talent development, with efforts led by Institute of Physical and Chemical Research under it; and the Ministry of Economy, Trade and Industry is mainly responsible for AI development relating to applied research, practical use and social applications of AI, standard assessment methods and techniques, and research on large-scale use of AI, with efforts

led by the National Institute of Advanced Industrial Science and Technology (AIST) under it.

In China, AI development has been in line with a three-step strategy introduced in 2017 in an effort led by the State Council, the Central Leading Group for National Science and Technology System Reform and Innovation System Construction and the Ministry of Science and Technology which are responsible for formulation and implementation of AI plans and projects and supported by the Office for Advancing AI Plans and the Advisory Committee on AI Strategy with research on relevant issues such as AI theories and technologies and related legal and ethical issues and regular publication of government white papers on AI. The Advisory Committee on AI Strategy was established in November 2017 with the release of the Next-Generation AI Development Plan in a significant move which marked China's commitment to promoting innovative applications of AI on a large scale, optimizing its systematic deployments of AI development, and turning AI into a major driver of China's industry upgrade and economic transformation and which, so to speak, ushered China's AI development into the stage of comprehensive implementation.

Table 4-2 Steering Forces of AI Policy Worldwide

Country	Driving Forces (Policymaking and Funding)	Agencies Subsequently Created or Added
USA	National Science and Technology Council (NSTC); White House Office of Science and Technology Policy (OSTP); Office of Management and Budget (OMB)	NSTC Subcommittee on Machine Learning and Artificial intelligence (formed to help coordinate Federal activity in AI); Networking and Information Technology Research and Development (NITRD) (formed to define the Federal strategic priorities for AI R&D, with particular attention on areas that industry is unlikely to address); Select Committee on Artificial Intelligence (formed to assist the NSTC to improve the overall effectiveness and productivity of Federal R&D efforts related to artificial intelligence (AI))
EU	European Parliament Committee on Legal Affairs (JURI); European Commission (EC)	euRobotics; SPARC; European Robotics Technology Platform (EUROP); European Robotics Network (EURON)
Germany	Bundesregierung (Federal Government); Federal Ministry of Education and Research (BMBF); Federal Ministry for Economic Affairs and Energy (BMWi); German Academy of Science and Engineering (acatech);	German Research Center for Artificial Intelligence (DFKI); 2018 German-French Artificial Intelligence Joint R&D Center; 2017 Platform for Learning Systems 2013 Industry 4.0 Platform;
UK	Engineering and Physical Sciences Research Council (EPSRC); Royal Academy of Engineering	RAS Leadership Council; National Artificial Intelligence Research Center; AI Council; Open Data Institute (ODI); Royal Statistical Society (RSS) Data Science Section; techUK; All-Party Parliamentary Group on Artificial Intelligence

Country	Driving Forces (Policymaking and Funding)	Agencies Subsequently Created or Added
France	French Parliament; French Institute for Research in Computer Science and Automation; French Digital Council; Directorate General of Armaments (DGA);	AI Ethics Committee; Planning to set up an environmental impact assessment platform to build a green value chain of AI
Japan	Public-Private Dialogue towards Investment for the Future	Artificial Intelligence Technology Strategy Council, serving as a national-level general management agency that coordinates the Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry to jointly promote AI technology R&D and applications
China	State Council; Central Leading Group for National Science and Technology System Reform and Innovation System Construction; Ministry of Science and Technology;	Office for Advancing AI Plans; Advisory Committee on AI Strategy (advancing project implementation through coordination of the Ministry of Science and Technology and other government authorities)

4.2 China's National AI Policy

4.2.1 China's National AI Policy Trend

Since the rise of AI research in China, the country has released a series of AI policies which have effectively promoted the stable development of AI technology and related industries. Searching the government documents database using keywords in the AI keyword list returned 202 central-level AI policy documents of China.

On August 8, 2016, the State Council issued the National Plan for Scientific and Technological Innovation During the Period of the Thirteenth Five-year Plan, which explicitly specified AI as the main direction of developing next-generation information technology, emphasized that the effort to build a modern industrial technology system should focus on "developing natural human-computer interaction, especially intelligent perception and cognition, virtual-physical integration and natural interaction, and semantic understanding and smart decision-making" and required "vigorously developing big data-driven human-like intelligence technologies and methods; making breakthroughs in human-centric human-machine fusion theories, methods and key technologies and developing related equipment, tools and platforms; and making breakthroughs in human-like intelligence based on big data analysis and achieving human-like vision, hearing, speech and thinking to support AI-driven industrial development and demonstrative applications in key sectors such as education, office and healthcare." At present, AI has become a core part of China's "Deep Blue" program geared to safeguard national security and strategic interests with strategic high tech. The report to the 19th CPC National Congress highlighted the commitment to "building China into a manufacturer of quality and develop advanced manufacturing and promoting further integration of the internet, big data, and artificial intelligence with the real economy", showing that AI has become a key national strategy and an important direction of China's industrial transformation. In the field of AI, China has rolled out a series of policy

documents including State Council Guidelines on Promoting the Healthy and Orderly Development of the Internet of Things, Made in China 2025, Robotics Industry Development Plan (2016-2020), State Council Guidelines on Promoting the "Internet+" Action, State Council Notice on Issuing the Action Outline for Promoting the Development of Big Data, Thirteenth Five-year Plan on National Economic and Social Development and State Council Notice on Issuing the "Next Generation Artificial Intelligence Development Plan". Among them, the Next Generation Artificial Intelligence Development Plan stated that the comprehensive AI advancement in terms of disciplinary development, theoretical modelling, technological innovation and software and hardware upgrade is triggering a chain reaction that will accelerate the change of economic and social development from digitalization and connectivity to artificial intelligence. Facing a complicated national security and international competition situation, China must adopt a global perspective and develop AI as a national strategy by making proactive systematic deployments and always maintaining the strategic initiative in international competition in the AI era to build new competitive edge, increase the development potential of the country, and effectively protect national security. Specific measures that have been outlined include thoroughly implementing the innovation-driven development strategy, accelerating the integration of AI with economy, society and national defense, improving innovation capabilities powered by next-generation AI technology, developing the intelligent economy, building an intelligent society, safeguarding national security, establishing an ecosystem where knowledge clusters, technology clusters and industry clusters are integrated based on positive interaction and talent, systems and culture support each other, anticipating and addressing potential risks and challenges, advancing AI-driven sustainable development, comprehensively increasing China's productivity, overall national strength and international competitiveness, and providing a powerful support for China's efforts to become an innovative nation and technology superpower and achieve the two centennial goals and the great rejuvenation of the Chinese nation.

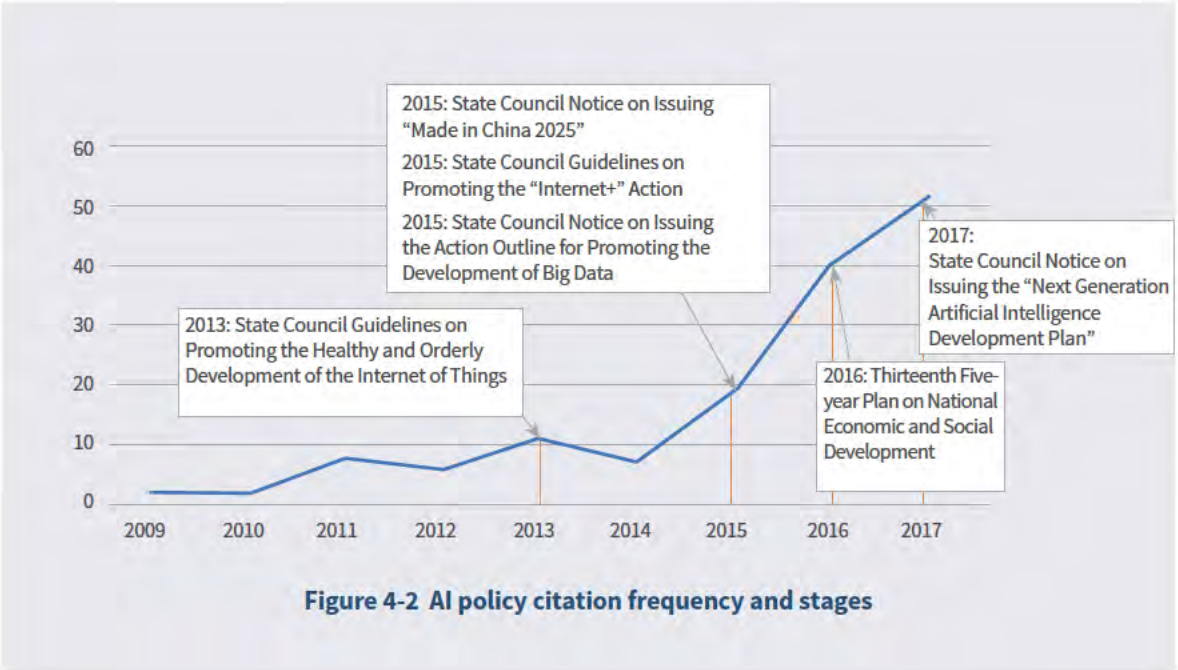


Figure 4-2 AI policy citation frequency and stages

China's AI policies can be divided into five stages according to the time of release of key AI policy documents: Stage 1 (before 2013), of potential development, where few policy documents were released and AI was not specified as a national priority; Stage 2 (2013-2015), of preliminary development, where the importance of AI began gaining recognition across all circles of society; Stage 3 (2015-2016), of rapid development, where a lot of policies documents were released and AI was elevated as a national strategy; Stage 4 (2016-2017), of stable development, where understanding of AI R&D and industry development was increasingly mature and policy documents came out stably; and Stage 5 (2017 to the present), of steady iteration, where all sectors have a more pragmatic understanding of AI and related policies are more specifically targeted.

4.2.2 Evolution of China's National AI Policy Themes

Corresponding with the release of key policy documents, each stage had remarkably different themes.

In Stage 1 (2009–2013), AI policy themes focused on IoT, information security, database, AI and infrastructure. In this stage, AI R&D and applications did not attract public attention and were mainly discussed in the academic fields, especially in computer science research.

In Stage 2 (February 2013–May 2015), the main AI policy keywords, in the descending order of frequency, included IoT, technical standards, infrastructure, big data and AI. In this preliminary stage of AI development, all circles of society gradually realized the importance of AI and policy adjustments were made that reflected increasing importance attached to technologies such as big data and infrastructure and emphasized the creation of standards in the early stage of AI development;

In Stage 3 (May 2015–March 2016), the main AI policy keywords included big data, infrastructure, IoT, cloud computing and data sharing. This stage saw rapid AI development in China, marked by the release of a large number of AI policy documents, the enshrining of AI development as a national strategy and the focus of AI policy keywords on infrastructure, especially on big data, cloud computing, data sharing and AI infrastructure. It can be seen that this stage saw the entry of AI into the big data era and related policies began attaching importance to mining and analysis of massive data;

In Stage 4 (March 2016–July 2017), the main AI policy keywords, in the descending order of frequency, included big data, AI, infrastructure, IoT and cloud computing. This stage represented a period of stable AI development in China, which saw an increasingly mature understanding of AI R&D and industry development and an increase of AI policy documents issued. The frequent mentioning of AI indicated a sharp increase of attention paid by all circles of life to AI, and relevant segments of the AI industry began experiencing rapid development.

In Stage 5 (July 2017–the present), the main AI policy keywords included AI, big data, information security, cloud computing and infrastructure. This stage experienced an AI fever and since then has seen a more pragmatic understanding of AI from all sectors of life and a greater specificity within produced AI policy documents. In this stage, AI, supported by technologies such as big data, cloud computing and information security as well as rapid development of relevant infrastructure, has become a national strategic industry.

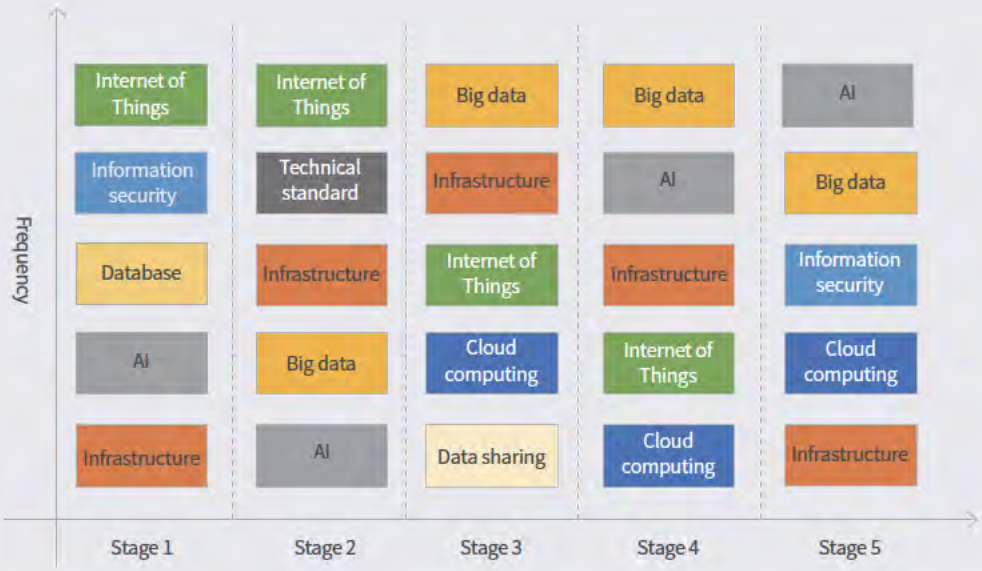


Figure 4-3 AI policy theme evolution

Keyword co-occurrence analysis is a common bibliometric method that uses the number of co-occurrence of two keywords in the same policy document as an indication of the degree of their relevance. Keywords can be clustered according to their co-occurrence relationships to identify core themes. On this basis, a keyword co-occurrence network can be created to identify the core themes in each stage.

- **Stage 1: before February 2013This stage**

marked the period of potential development of AI with policy keywords including IoT, technical standards, information security and infrastructure. This keyword distribution was closely related to the stage of social development at that time. In this stage, there had been a certain amount of infrastructure required by AI development, where remarkable progress had been made in such aspects as data collection, data mining, data sharing, database/data warehouse development. At the same time, this stage saw the rise of IoT in China, driven by significant breakthroughs in relevant fields including wireless intelligent sensor network communication technology, micro-sensors, sensor terminals and mobile base stations, and a complete industry chain had been formed in fields such as smart healthcare, smart logistics, smart transportation and smart agriculture. This stage, however, left many important things unattended such as intellectual property, intellectual rights protection, technical standards, information security and public security due to the absence of AI and IoT policies offering guidance on such matters.

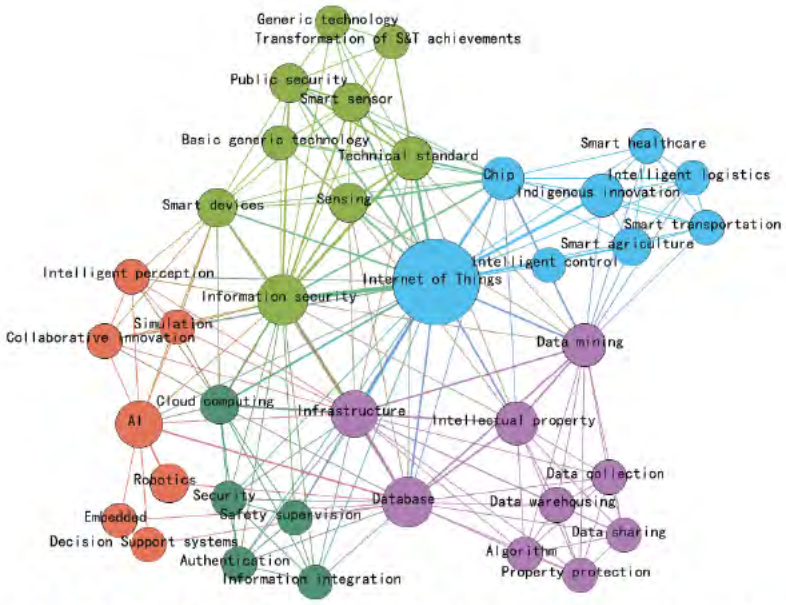


Figure 4-4 AI policy keyword co-occurrence diagram before February 2013

- **Stage 2: February 2013 – May 2015**

In this stage, which began with the release the State Council Guidelines on Promoting the Healthy and Orderly Development of the Internet of Things on February 17, 2013, IoT and technical standards remained core themes, but keywords such as AI, security regulation, big data and indigenous innovation began occurring more frequently. This stage saw China lay some groundwork in IoT technology development, standard formulation, industry fostering and industry application and saw big data technology gain application in IoT development, but AI policy keywords still focused on issues that remained unsolved such as difficulty in key technology R&D, yet-to-be-improved infrastructure, and information security threats. Meanwhile, it saw steady development in such fields as smart grid, smart city and smart device, with relevant AI research projects expecting to gain actual applications in public security and other fields and provide more advanced information processing and analysis capabilities.

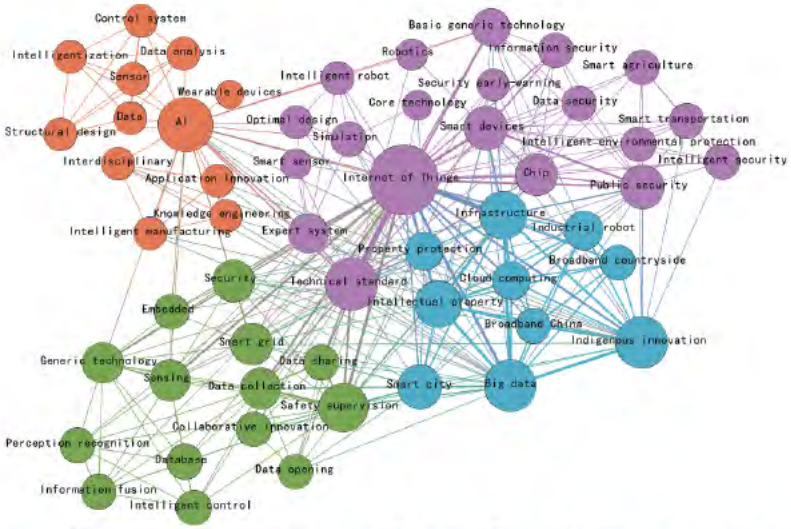


Figure 4-5 AI policy keyword co-occurrence diagram from February 2013 to May 2015

- **Stage 3: May 2015 – March 2016**

This stage saw the release of a series of important policy documents such as Made in China 2025, Robotics Industry Development Plan (2016-2020), State Council Guidelines on Promoting the "Internet+" Action, and State Council Notice on Issuing the Action Outline for Promoting the Development of Big Data, with basic technologies of AI such as big data, infrastructure, information security and IoT becoming core themes and AI disappearing altogether. This, however, did not mean that AI was fading away but that as increasing importance was attached to the foundation of AI development and as understanding of AI became more mature, the focus had been shifted to basic technologies and relevant real-world applications of AI (such as smart agriculture). This stage saw the rapid development of AI. In May 2015, the State Council issued Made in China 2025, in which it outlined comprehensive deployments to turn China into a manufacturing power. Smart manufacturing was designated as a key direction of Chinese manufacturing, and efforts were highlighted to accelerate integrated development of next-generation information technology and manufacturing technology, develop intelligent equipment and smart devices, advance production automation, and promote AI application in wide fields including smart home, smart devices, smart cars and robots. In July 2015, the State Council issued the Guidelines on Promoting the "Internet+" Action which explicitly identified AI as one of the 11 prioritized areas of development to form new industrial models and thus elevated AI to the level of a national strategy, ushering AI into the new era of "Internet+" and big data.

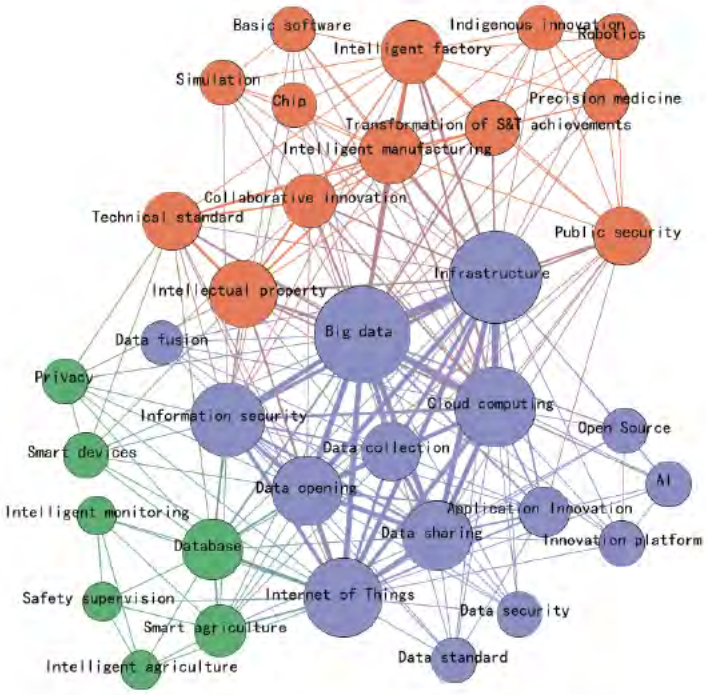


Figure 4-6 AI policy keyword co-occurrence diagram from May 2015 to March 2016

- **Stage 4: March 2016 – July 2017**

In March 2016, the Thirteenth Five-year Plan on National Economic and Social Development (Draft) was released which highlighted a commitment to making breakthroughs in AI. The keyword co-occurrence network for this stage became more complicated, though big data, AI, infrastructure, IoT and technical standards remained to be core themes, themes such as robotics, smart manufacturing and deep learning gained prominence. The background was that with the development of AI technology, all circles of life had an increasingly mature understanding of AI R&D and industry development and as a result paid more attention to AI's future applications (robotics, smart manufacturing, etc.) and enabling technologies (deep learning, etc.). The fact that high-frequency AI policy keywords continued to be big data and AI showed China's determination and attitude towards AI development in this stage. In this stage, development in key fields such as virtual technology, smart commerce and industrial robotics marked the gradual establishment and improvement of the AI industrial system, and at the same time, emerging technologies like IoT, cloud computing and big data gradually became strategic enablers of AI innovation and development.

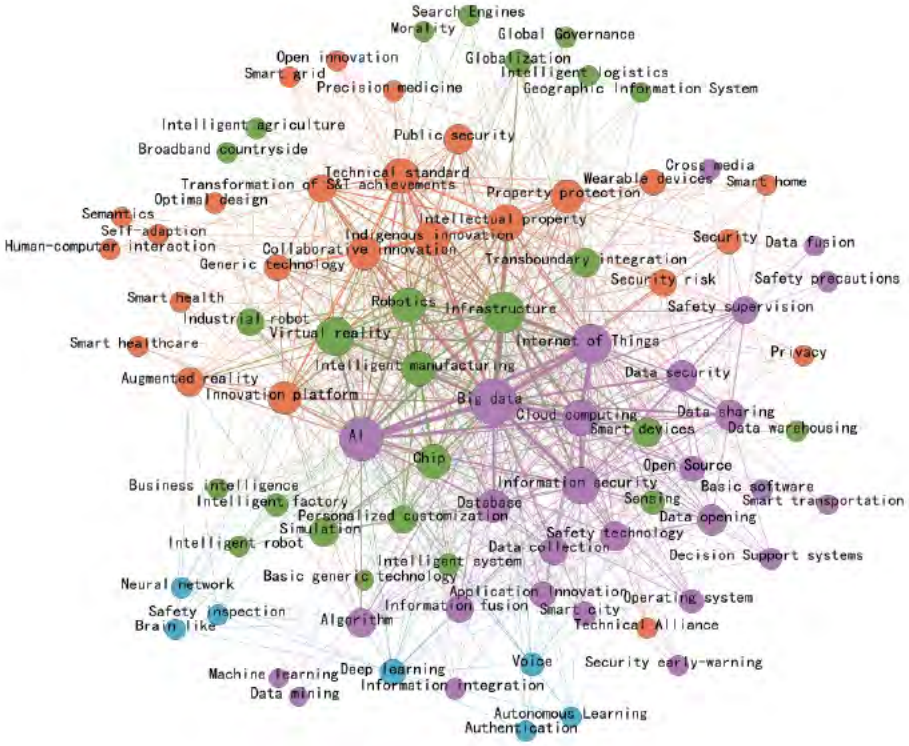


Figure 4-7 AI policy keyword co-occurrence diagram from March 2016 to July 2017

- **Stage 5: July 2017 – May 2018**

In July 2017, China released the State Council Notice on Issuing the "Next Generation Artificial Intelligence Development Plan", signifying the start of the advancement of next-generation AI. This stage saw AI become the No. 1 core AI policy keyword, followed by other prominent keywords such as intellectual property and intellectual rights protection. This stage experienced a fever of AI development and saw a more pragmatic and more internationally-contextualized understanding of AI

across society, leading to increasing attention paid to the intellectual property and intellectual rights protection relating to AI technologies. Policies in this stage were more targeted as well. In this stage, China placed a greater emphasis on building a safe intelligent society, with initiatives including developing efficient intelligent services, leveraging AI to improve public security, and promoting sharing and mutual trust in social interaction. Next-generation AI showed the characteristic of military-civilian two-way transformation which became a practical policy benefiting people by promoting integration-based innovation in six prioritized industries including manufacturing, agriculture, logistics, finance, commerce and home, marking the beginning of comprehensive AI development and applications in various sectors of the real economy.

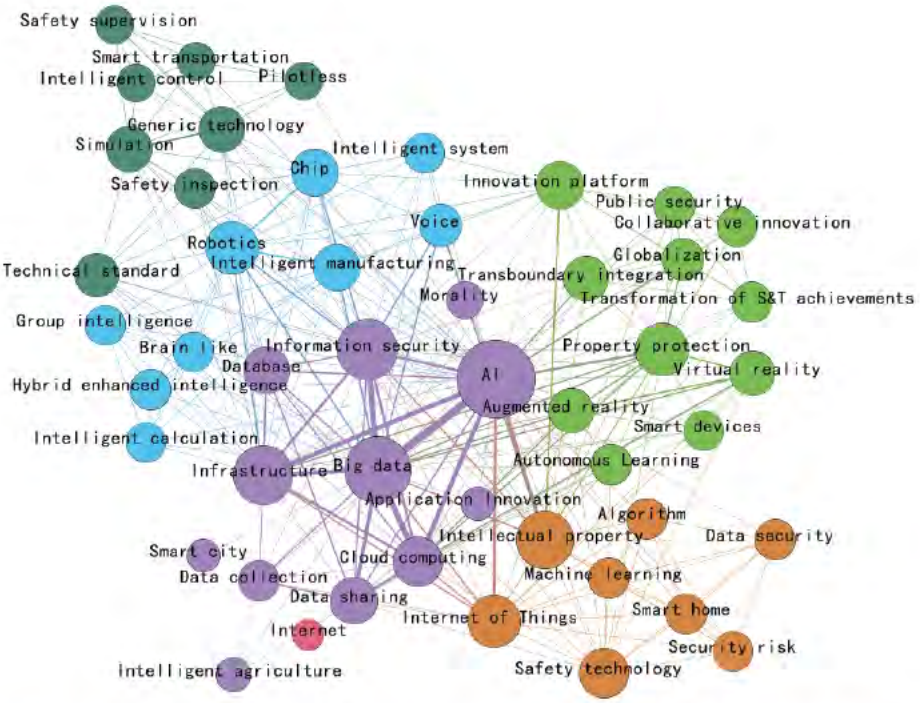


Figure 4-8 AI policy keyword co-occurrence diagram from July 2017 to May 2018

4.2.3 Citation Network Analysis of China's National AI Policy

In recent years, China's central government has issued a number of AI policies that are intertwined and cite each other. Figure 4-9 shows the citation network of China's central-level AI policy documents, where the individual policy documents vary in their relationship with other documents and their position in the citation network. Each code corresponds to a policy document. The table of contents of each document can be found on the website of the electronic version of this report.

According to the network graph, it can be seen that the AI policy at the center include the following: Thirteenth Five-year Plan on National Economic and Social Development, Made in China 2025, Outline of the National Medium- and Long-Term Program for Science and Technology Development (2006-2020), National Science, Technology and Innovation Plan for the 13th Five-year Plan Period, Outline of the National Strategy of Innovation-Driven Development, Interim Measures for the Management of Special Funds for the Development of the Internet of Things, Report to the 18th CPC National Congress, State Council issued the

Guidelines on Promoting the "Internet+" Action, State Council Notice on Issuing the Action Outline for Promoting the Development of Big Data, and State Council Guidelines on Promoting the Healthy and Orderly Development of the Internet of Things. These documents serve as core policy and programmatic documents in China's AI policy system and direct and influence the formulation of other AI policy documents. The AI policy citation network identifies several groups of documents that are closely related with each other and form relatively independent sub-networks in the overall network, which are marked in different colors and represent six core thematic areas of China's AI policies, namely, Made in China, IoT, Internet+, big data, innovation strategy, and technical research and development.

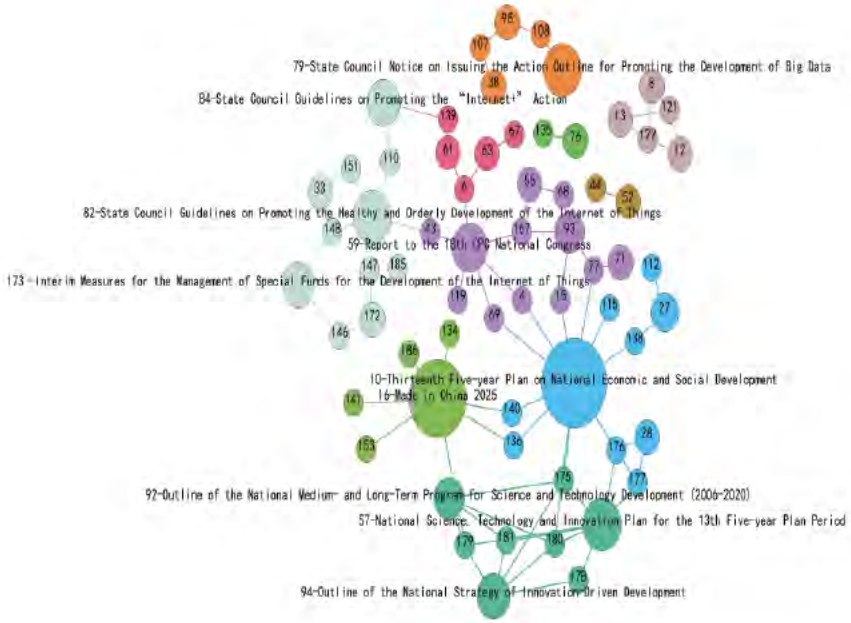


Figure 4-9 China's national AI policy citation network

4.3 China's Provincial-level AI Policy

A total of 845 provincial-level government AI policy documents were identified by searching the keywords in the AI policy keyword list. These policies were guideline documents formulated in a top-down approach in line with national AI industry plans and in the light of local conditions to steer local AI industry deployments. They led to a series of support policies and funds geared to strengthening AI technology R&D and product applications and promoting the integration of multiple fields such as healthcare, education, pension and culture to provide broad prospects for the AI industry development.

4.3.1 Number of Provincial-level AI Policy Documents

The first provincial-level AI policy came out in 2009 and since then, especially after the release of the State Council Guidelines on Promoting the Healthy and Orderly Development of the Internet of Things, a steadily increasing number of local government AI policies have been released every year.

Figure 4-10 Number of Provincial AI policy documents

After 2014, with the release of central AI policy documents including State Council Notice on Issuing "Made in China 2025", State Council Guidelines on Promoting the "Internet+" Action, State Council Notice on Issuing the Action Outline for Promoting the Development of Big Data and Thirteenth Five-year Plan on National Economic and Social Development, AI policy documents issued by local governments have grown exponentially. The number of such documents issued annually peaked in 2016 with 276. The recent release of the State Council Notice on Issuing the "Next Generation Artificial Intelligence Development Plan" has triggered a new round of release of local government AI policies.

Jiangsu, Guangdong and Fujian are the top three provinces by the number of AI policies issued in response to the national AI policies.

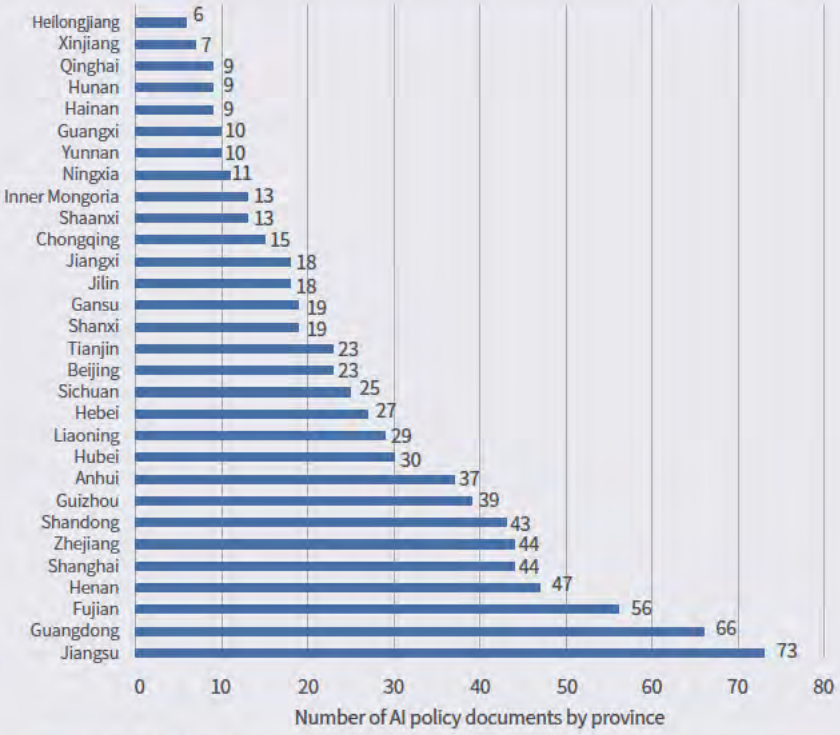


Figure 4-11 Number of provincial government AI policy documents

From the graph of the number of AI policy documents by province, it can be seen that three core regions of AI development have emerged—Beijing-Tianjin-Hebei, Yangtze River Delta, and Guangzhou-Hong Kong-Macao.

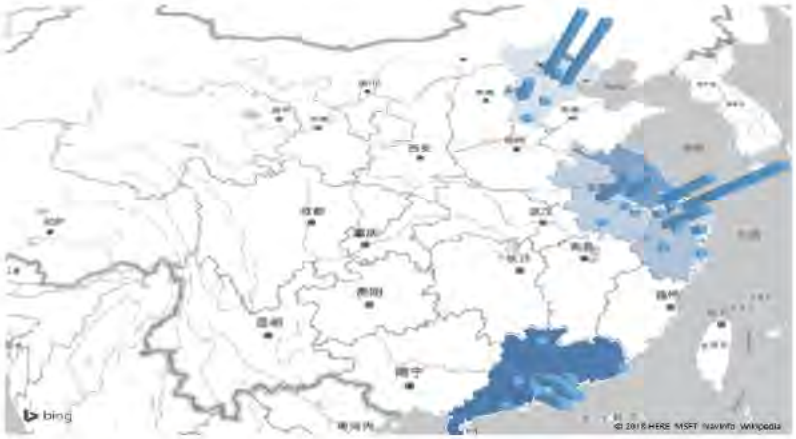


Figure 4-12 Top regions by the number of AI policy documents issued

Beijing-Tianjin-Hebei has many state-level scientific research institutions, numerous research institutes and many innovative industrial parks, and has gathered a large number of high-tech talents. Leveraging its unique advantages in knowledge resources, Beijing-Tianjin-Hebei has become the Asia Pacific's knowledge innovation center. By introducing industry development plans, creating R&D platforms and building industrial bases, Beijing-Tianjin-Hebei has not only driven the development of AI-related industries but also preliminarily formed several internationally competitive industrial clusters including autonomous driving, smart manufacturing, smart healthcare and public services.

The Yangtze River Delta region is represented by Zhejiang, Jiangsu and Shanghai. Jiangsu launched the "Jiangsu Brain Plan" to establish a national AI industry innovation base; Shanghai, located in the center of the Yangtze River Delta and relying on strong technical innovation resources, has built an "AI development cluster" in Xuhui district and established the "National Engineering Laboratory for Brain-like Intelligence Technology and Application"; and Zhejiang launched an AI town development plan to build the China (Hangzhou) AI Town in Future Sci-Tech City in Hangzhou, which is home to the Zhijiang Lab supported by leading research forces from Zhejiang University and Alibaba Group.

The Guangdong-Hong Kong-Macao region, represented by Guangzhou, Shenzhen, Hong Kong and Macau, has also seen local governments issue multiple AI policy documents, including Guangzhou Consensus on Artificial Intelligence and Support Plan of Foshan Municipality on Promoting Robotics Applications and Industry Development. Shenzhen, though not possessed of the knowledge resource advantages of Beijing and Shanghai, has built a high-tech industrialization platform and

become a frontier of China's efforts to respond to AI and other high-tech challenges by leveraging international trade liberalization and enabling quick marketization, productization and wide application of emerging technologies. Hong Kong, as an international financial, information and trade center, has become China's AI technology and product market-based transformation center by leveraging its professional financial talent forces and mature legal system. The government of Macao SAR signed a Strategic Cooperation Framework Agreement on Smart City Development with Alibaba Group to apply Alibaba's leading AI technologies to Macao's city development and build the world's largest city AI system.

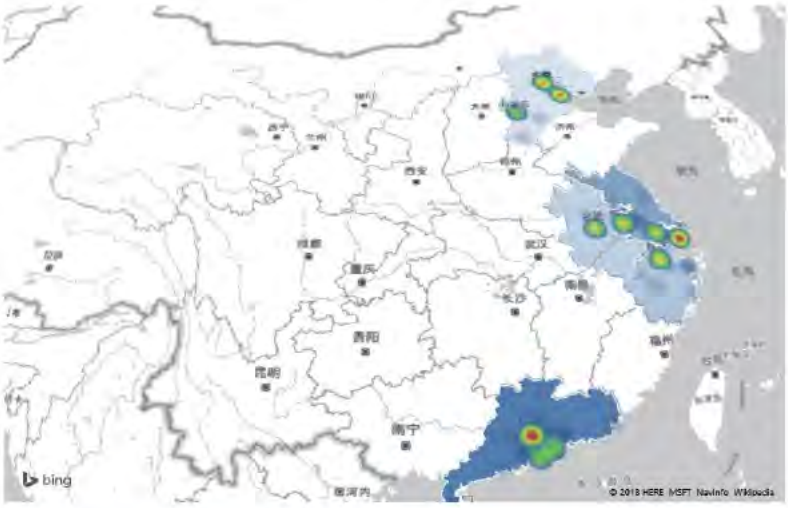


Figure 4-13 AI development trends in Beijing-Tianjin-Hebei, Yangtze River Delta and Guangdong-Hong Kong-Macao

4.3.2 Citation Relationship of Provincial-level AI Policies

AI policy documents issued by China's provincial governments in recent years have been intertwined with mutual citation of each other. Figure 4-14 shows the citation network of China's provincial-level AI policy documents, where the individual policy documents vary in their relationship with other documents and their position in the citation network. The table of contents of each document can be found on the website of the electronic version of this report.

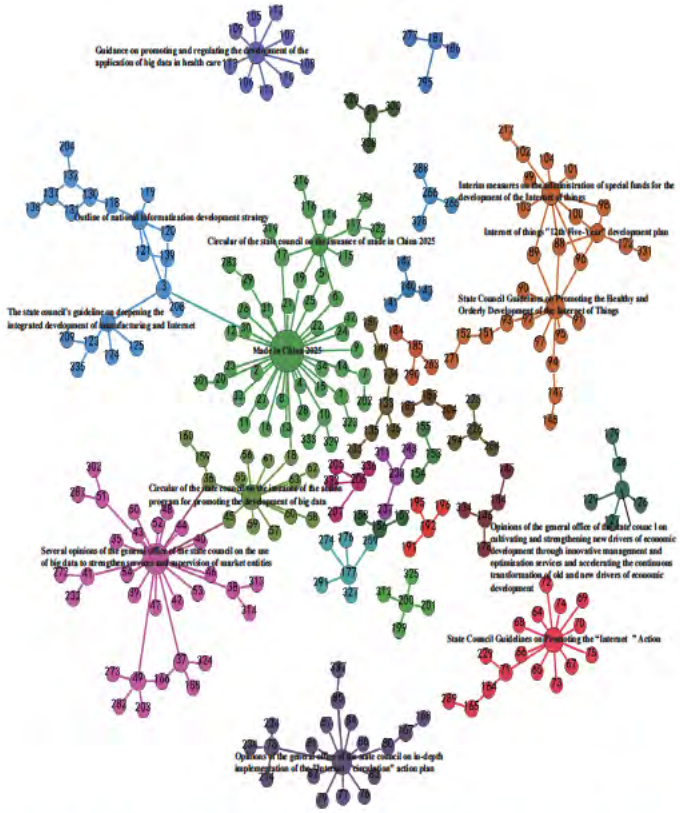


Figure 4-14 Graph of provincial policy documents citing central policy documents

It can be seen from Figure 4-14 that policy documents represented by the Opinions on In-depth Implementation of the "Internet + Circulation" Action Plan and the Guidelines on Promoting the “Internet+” Action and their corresponding provincial-level citing policies form simple first-level citation networks with no further policy derivatives, so that each network assumes a single-core single-level star-like structure. The snowflake-shaped networks are core citation networks represented by Made in China 2025 which is a single-core multi-center multi-level network with a single document serving as its main center. A citing policy of the core policy that is cited with a higher frequency in a subordinate network becomes a sub-center of the entire network which consists of a number of clusters. It can be seen from the graph that Made in China 2025 is a programmatic document in China’s AI development and connects to other policy clusters through citing policies and thereby directly or indirectly connects most provincial-level AI policies and plays an irreplaceable guiding role in the entire AI industry development process.

4.3.3 Theme Analysis of National and Provincial-level AI Policies

- **Keyword co-occurrence analysis of national and provincial AI policy documents**

Figure 4-15 shows the keyword co-occurrence of national and provincial AI policy documents, which provides an intuitive picture of the relevance of national and provincial AI policy documents in goals and contents. Keyword co-concurrence analysis finds that provincial AI policy documents are consistent with central AI policy documents in terms of both direction and content. Specifically, the State Council Notice on Issuing the “Next Generation

Artificial Intelligence Development Plan" released in July 2017 explicitly specified a three-step policy of AI development. In line with this policy, local governments such as Shanghai, Beijing, Zhejiang, Anhui, Guizhou and Jiangxi formulated their own AI policies. Overall, these local government AI policies were basically consistent with the national policies in goals and contents. The policy contents focused on three aspects, i.e. industry, technology and application. To be specific, they focused on machine learning, smart chips and cloud storage in industry; IoT, big data, AI and smart manufacturing in technology; and geographic information system, smart grid, smart agriculture, information security and precision medicine in application.

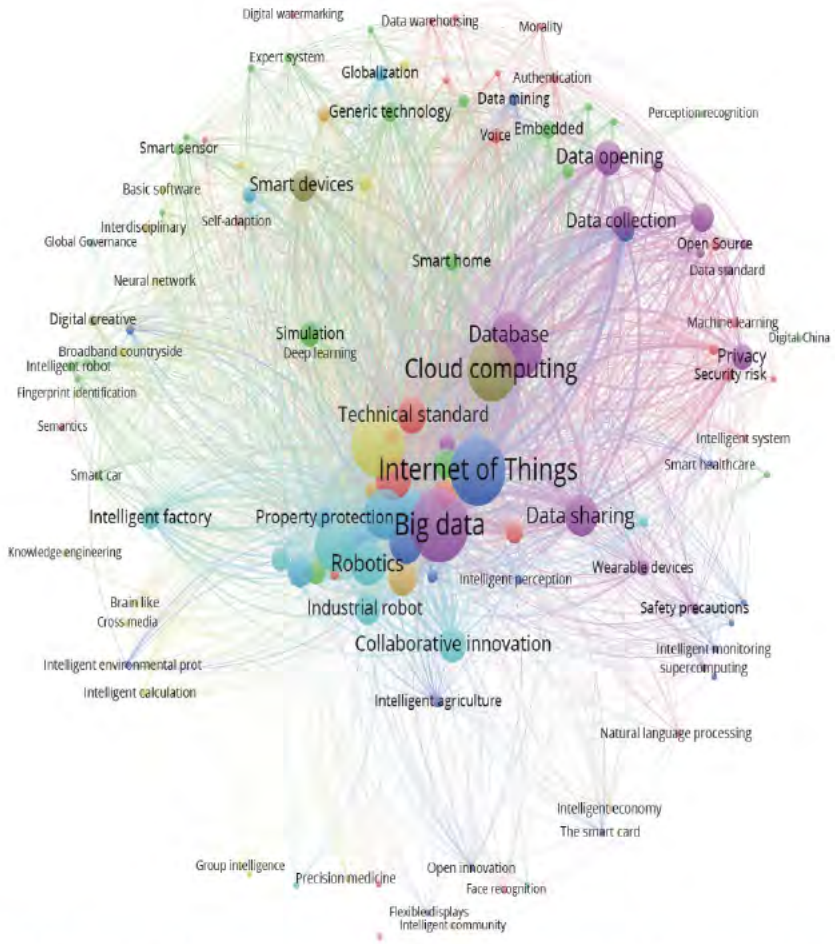


Figure 4-15 Keyword co-occurrence of national and provincial AI policy documents

• Keyword co-occurrence analysis of provincial AI policy documents

Figure 4-16 shows the keyword co-occurrence of provincial AI policy documents, which examines the AI policy priority areas of those provinces whose AI industries are closer to implementation. As shown by the graph, AI has had a solid foundation of development in such areas as unmanned systems, security, smart home, wearable engineering and smart robotics with smart analysis, decision, sensing and control capabilities and enabling technologies in fields including environmental monitoring, home security, medicine and health,

and energy management. All the provincial AI policy documents have been geared to making advancements in AI enabling technologies and mechanisms such as big data, IoT, indigenous innovation, intellectual property, research result transformation and data sharing and promoting the integration of AI with different industries with the emphasis on indigenous innovation and data sharing and the application of AI in wide fields including transportation, geography, economy and security regulation to accelerate AI development and uptake for the benefit of all citizens.

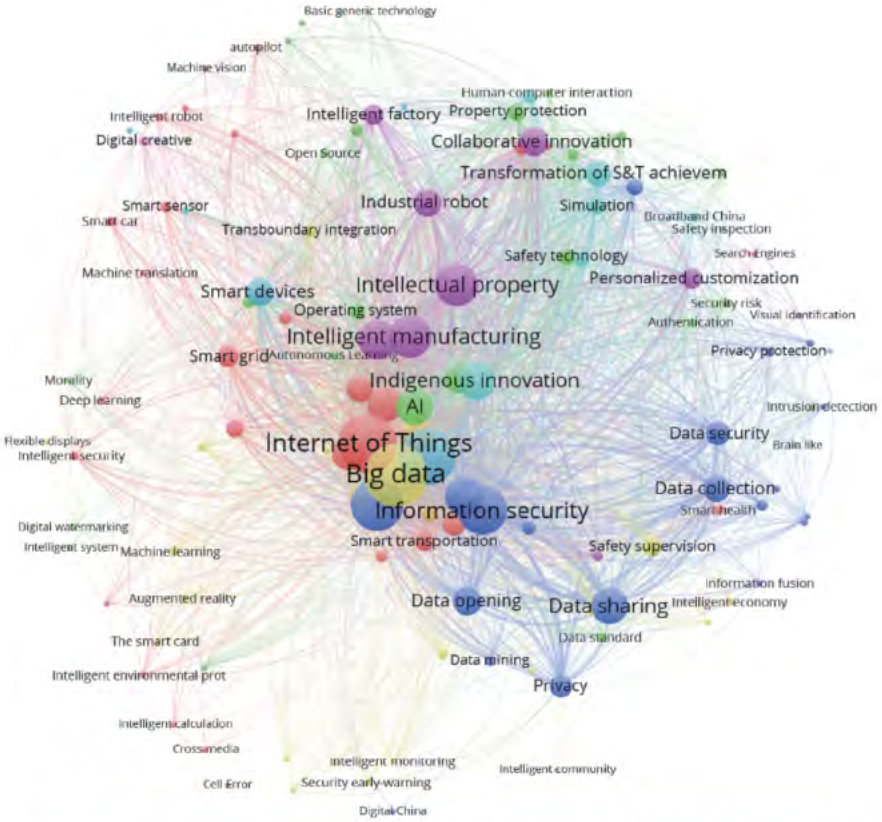


Figure 4-16 Keyword co-occurrence of provincial AI policy documents

While aligning with national AI strategic plans, local government AI policies had their own characteristics and priorities due to their local conditions, as illustrated by the top three provinces in terms of AI policy documents issued, with Jiangsu focusing on infrastructure, IoT and cloud computing; Guangdong on infrastructure, smart manufacturing and robotics, showing a great interest in AI applications; and Fujian on IoT, big data, innovation platform and intellectual property rights. A closer look at these differences explains that Jiangsu is more concerned with basic R&D of AI, especially basic AI technologies such as cloud computing and big data; Guangdong, a strong manufacturing province with the ability to quickly productize technologies, is more concerned with the applications of AI in fields such as manufacturing and robotics while working on basic AI technologies like big data and cloud computing; and Fujian, whose priority area of AI development is IoT, has leveraged its IoT industry alliance platform and Mawei IoT industry base to build a nationally leading IoT sensing and identification industry cluster.

05 Public Perception and General Impact of AI

5.1 Public Perception of AI

The flourishing of AI is profoundly changing people's lives. Half a century ago when AI was sprouting, most people would not expect that humans and machines would be so close. In fact, the discussions about human-machine relations have quickly gone beyond the academic world. From top-down design at the national level to the penetration into various sectors, AI is becoming a powerful engine driving disruptive changes.

From 2016 to 2017, AI received 286.3% more attention and became the most trending science topic of the year. [1]High technologies that can improve the life of ordinary people tend to have a higher reputation and influence. According to Toutiao Index monitoring for the first quarter of 2018 (Figure 5-1), analysis of article views, comments and sharing identified March 14 as the peak date in the quarter in terms of the amount of attention received by AI. The passing away of the famous UK physicist Stephen Hawking attracted massive attention from users and triggered many commemorative activities online.

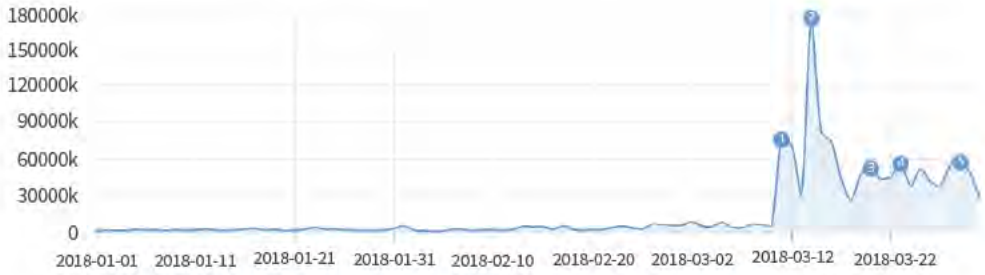


Figure 5-1 Public attention on AI related topics in Q1 2018

5.1.1 Survey of Public Perception of AI

Toutiao conducted a survey of its users from May 9 to May 13, 2017, which collected a total of 3,088 valid responses. According to the survey, only 6.23% of the respondents were ignorant of AI, and the rest knew about it from news (80.27%) and movies (37.25%).

[1] AI Impact Report, Toutiao.

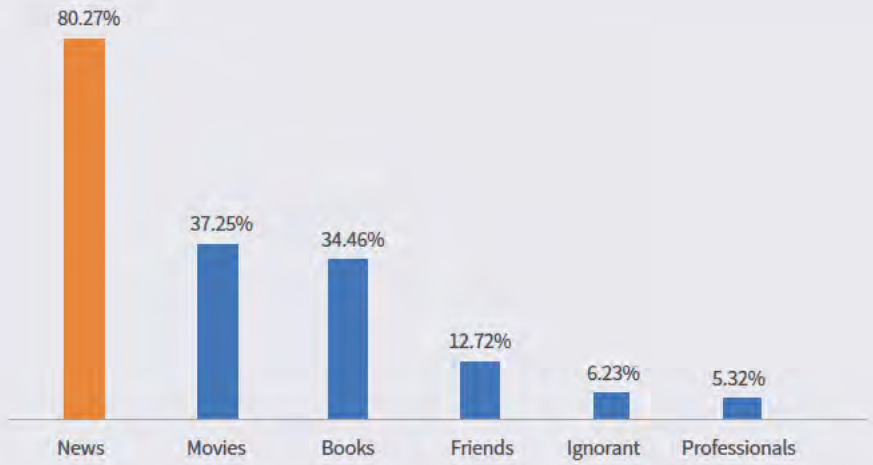


Figure 5-2 AI awareness by channel

AI has penetrated everyday life, but not all are aware of it or its effects. Although there was a high level of AI awareness, only 41.58% reported that they had used AI products, with 40.74% stating that they had never used any AI products, and 17.68% saying that they were not sure what makes a product an AI product.

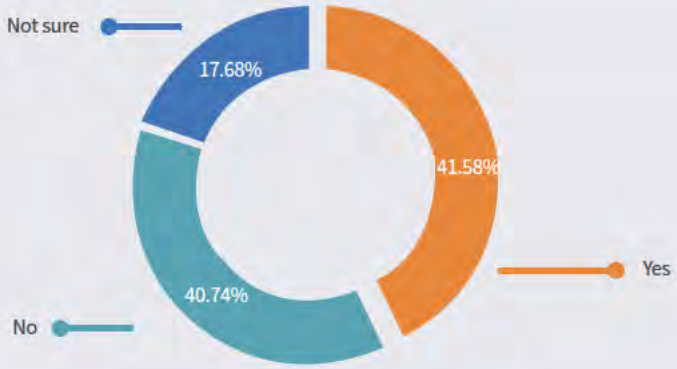


Figure 5-3 Awareness of AI product use

According to the survey, respondents were most interested in how AI development will affect themselves, with the top three questions being: What jobs will be replaced by AI? (46.14%) What harms will AI cause? (43.61%) Will AI become a subject capable of legal and moral awareness and civil conduct? (40.36%) All the three questions have negative implications, indicating that despite a supportive attitude towards AI development, people want to know more about the direct risks that AI might bring. For the question, "what worries you the most about AI", the top three concerns were

"AI losing control and causing social crises" (selected by 54.9% of respondents), "AI making wrong decisions or judgments" (46.01%), and "AI losing control and causing personal injuries" (45.81%), respectively.

With respect to the expectation of AI development, 53.15% of respondents expressed support of the in-depth and comprehensive development of AI, with more than 60% of respondents in provinces including Xinjiang, Shanxi, Guizhou, Anhui and Shandong expressing support. Respondents who held a conservative attitude accounted for 28.68%, who believed that AI development should be confined to those relatively low-risk projects. The rest included 15.77% who did not oppose AI but believed that the pace of development should slow down and 2.4% who opposed AI development.

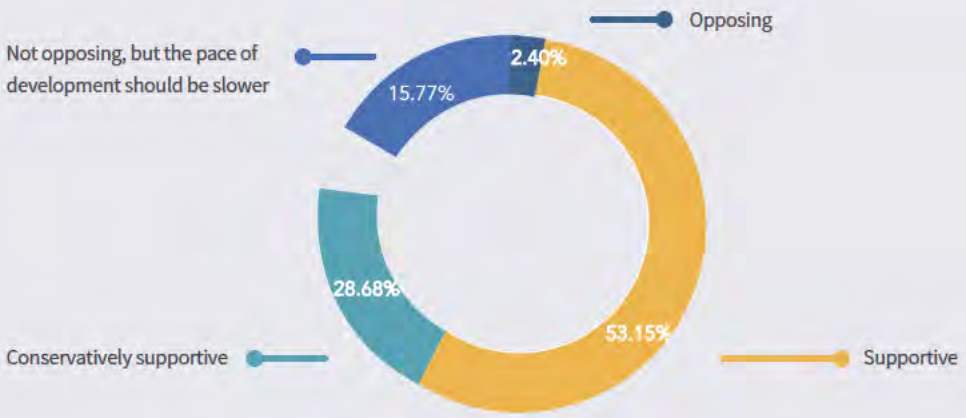


Figure 5-4 Expectation of AI development

5.1.2 Differences in Public Interest in AI

- **Industry differences**

The key to AI deployment is the rich variety of its application scenarios. In the current stage, AI has been applied in fairly wide areas, with the most common and familiar forms including autonomous cars, intelligent assistants, recommendation engines and multi-language translation. AI will find more and greater-depth applications at work and in everyday life in the future.

According to Toutiao Index data, the top four sectors of AI application in 2017 were finance, transport, education and healthcare, respectively.

In terms of the attention received for AI application, the financial sector came first, followed by transportation, education and healthcare.

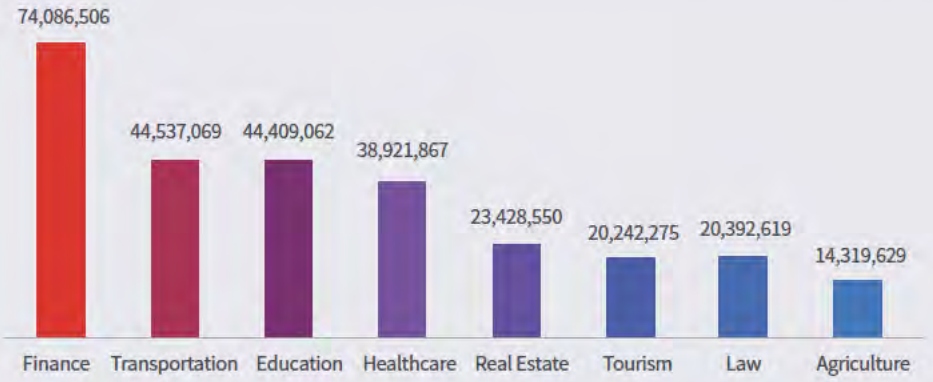


Figure 5-5 Top eight sectors of AI application by attention received

* Data explanation: The popularity index indicates the amount of attention received by a keyword. It is a weighted value based on a number of indicators such as views, comments, sharing and favoriting.
* Data monitoring time: January 1 – December 30, 2017

• Age and gender differences

The data collected from January 1 to December 30, 2017 were analyzed against the two indicators of age penetration and gender penetration, where age penetration is the number of views of articles containing AI keywords by users in an age group divided by the number of views of all articles by users in the age group, and gender penetration is the number of views of articles containing AI keywords by users of a gender divided by the number of views of all articles by users of the gender. According to data, users over 30 are more interested in AI, with the top group being the 31-40 age group, followed by the 41-50 age group. In terms of gender difference, male users are significantly more interested in AI than female users.

Users over 30 are more interested in AI, with male users showing a significantly greater interest in AI than female users

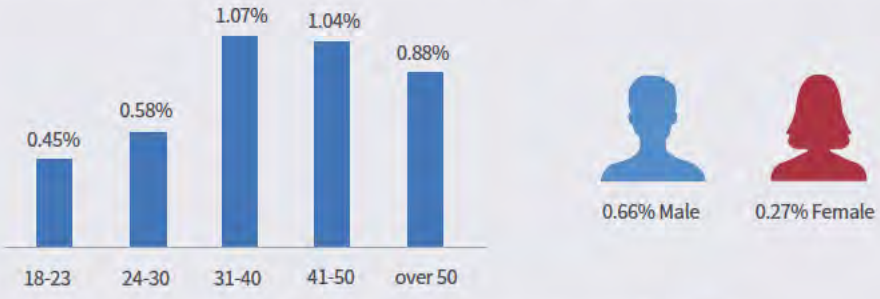


Figure 5-6 Interest in AI by age group and gender

• Regional differences

Regionally, the data was analyzed against the regional penetration indicator, where regional penetration is measured by dividing the number of views of articles containing AI keywords with the number of views of all articles in the region. The analysis identified Shanghai, Beijing, Hubei, Guangdong and Zhejiang as the top five regions in terms of the interest shown by local users in AI (Figure 5-7). In terms of cities, users interested in AI are mainly distributed in super first-tier and first-tier cities including Beijing, Shanghai, Shenzhen, Guangzhou, Hangzhou, Chengdu and Wuhan (Figure 5-8).

Top 5	Region	Regional Penetration
1	Shanghai	0.77%
2	Beijing	0.75%
3	Hubei	0.62%
4	Guangdong	0.61%
5	Zhejiang	0.61%

Figure 5-7 AI regional penetration

Figure 5-8 Interest in AI by cities

5.1.3 Public Attitudes towards AI

User comments on hot AI-related articles collected by Toutiao Index from 2016 to 2017 were analyzed to show the changes in user attitude to AI. The analysis identified a shift of user attitude from enthusiastic endorsement to reflection on potential negative implications of AI, reflecting a gradually rational attitude towards AI (as shown in Figure 5-9).

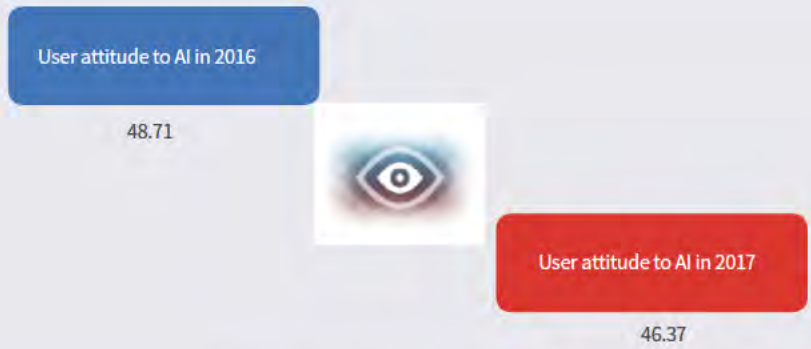


Figure 5-9 Attitude towards AI

* Data description: The user attitude analysis was conducted with technical support from partner Kismet Technology.
* User attitude description: User attitude is analyzed based on over 10,000 hot comments on AI-related articles, where a higher score indicates a more positive attitude towards AI.
* Data monitoring time: January 1 – December 30, 2017

Figure 5-10 Changes in user attitude towards AI revealed by user comments from 2016 to 2017

* Data description: The user attitude analysis was conducted with technical support from partner Kismet Technology.
* Data monitoring time: January 1 – December 30, 2017

Data collected from 2016 to 2017 revealed attitude shifts marked by decreasing optimism and anger and increasing anxiety, excitement and fear.

5.2 General Impact of AI on Society

With the full development of AI and the greatly increased labor productivity it brings, people will be able to live a richer and more colorful life and, as they are liberated from manual labor and even conventional intellectual labor, devote more energy to creative activities for fuller development of humankind and human society. Currently, the rapid development of AI technology has transformed many sectors including retail, agriculture, logistics, education, healthcare, finance and commerce and reshaped how production, distribution, exchange and consumption take place. According to data from IDC[2], the coming five years will see AI be applied in more industries and bring substantial efficiency improvements—82% for education, 71% for retail, 64% for manufacturing and 58% for finance.

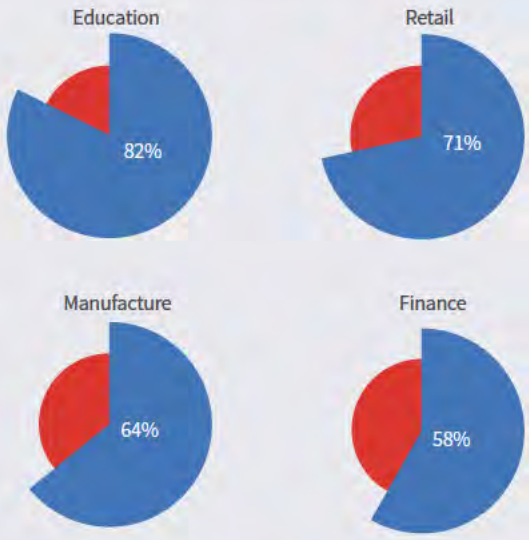


Figure 5-11 Efficiency improvement brought by AI to major industries

AI has been recognized by a broad spectrum of people ranging from technologists to sci-fi authors and from intellectual elites to the general public as the most disruptive and transformative ever innovation in human history and a technology capable of profoundly changing the world with far-reaching implications that cannot be exactly estimated. A large number of visionary people, including Norbert Wiener, the father of automation, recently deceased world-renowned scientist Stephen Hawking, Yuval Noah Harari, author of Sapiens: A Brief History of Humankind, and Tesla founder Elon Musk have warned that the quick development of AI, while bringing great conveniences to people, will pose huge potential risks and even challenge the existing social values and the value of the human race itself. They urge people to rethink the relationship between humans and machines and the future of humankind, and to ensure such AI systems are made as safe as possible before being deployed widely.

[2] IDC China: Artificial Intelligence White Paper: Towards the AI Era Led by Information Flow, 2017

5.2.1 AI's Impact On Education and Employment

The ultimate purpose of developing AI is not to replace humans but make humans smarter, where education will play a key role. By increasing productivity, AI liberates humans from mechanical, repetitive or dangerous labor and allows them to have more time at their disposal and focus more on developing and improving their potential of innovation, thinking, aesthetic appreciation and imagination. From the perspective of knowledge acquisition, with reduced mandatory labor and increased discretionary time, people will be able to acquire more soft knowledge that is closely related to human emotions and cannot be easily converted to data that can be processed by AI and therefore is more difficult to be learned or grasped by machines.

The intrinsic nature of education determines that personalization will be a basic direction of education. The talents needed in different periods vary greatly. In the AI era, personalized learning and communication and collaboration on different dimensions will become the main methods of learning, and students can get more personalized learning content support. At present, AI applications in education are mainly focused on the following areas: adaptive (personalized) learning, virtual teaching, educational robot, science and technology education based on programming and robotics, and situational education based on VR/AR. Learning in ways that are working to individual students will not only increase learning efficiency but also help keep a high level of interest in learning. In-depth applications of AI in education are not for the purpose of replacing teachers but to make teaching more efficient and fulfilling for teachers. Furthermore, in the AI-enabled educational system, there will be much higher requirements on students' ability to import and export information and learn independently, and the development of innovation skills will also become an important direction.

With the replacement of humans by machines for an increasing amount of onerous work or manual labor as technological development steadily advances, humans will face unprecedented challenges while enjoying the benefits of this replacement. In fact, more and more people are already worrying about their jobs being taken by AI or the prospect of their eking out a living in the shadow of AI. According to an estimate of the likelihood of jobs being replaced by AI in China, the coming 20 years will see approximately 76% of the working force being impacted by AI, or 65% if only the non-agricultural working force is considered[3]. At the same time, however, AI will also create new jobs. According to a survey, Chinese technology firms will expand their AI team by an average of 20% annually, and this demand for AI specialists will grow further. An expert from the Education and Examination Center of MIIT said that the demand for AI specialists in China will likely increase to five million in the coming several years.[4]

It can be safely averred that as AI transforms industries and consumption, some jobs will become things of the past and at the same time AI will incubate a series of new jobs. On the other hand, the human-machine relations will be restructured with the emergence of a new job market where non-routine cognitive jobs will be difficult to replace and have higher requirements on innovation skills, deep thinking and imagination.

As mechanization and intelligent automation give rise to a new employment landscape, vigilance needs to be exercised with respect to ensuing issues such

[3] Chen Yongwei, "How AI Will Impact Employment", Journal of Northeast University of Finance and Economics, No. 3, 2013
[4] AI: Job Destroyer or Job Creator
http://www.xinhuanet.com/tech/2018-02/26/c_1122452172.htm

as rising unemployment, widening wealth gap and social instability. The impact of AI will be continuous and so will its multifaceted impact on education and employment. Therefore, it is necessary to explore the educational and employment mechanisms that match and adapt to the technological revolution.

5.2.2 AI's Impact on Privacy and Security

Today, personalized experience has been emphasized in many consumption scenarios as personally and situationally relevant services gradually become one of the main directions of AI-driven innovation. With information access increasingly based on social media and user attention being more and more fragmented, service providers will strive to create more flexible and convenient consumption scenarios and provide better user experiences. Meanwhile, the development and maturing of speech recognition, face recognition and other capabilities derived from machine learning algorithms will allow businesses to get an unprecedented understanding of customers based on customer profile analysis and provide more satisfying experiences through precisely targeted and differentiated services. On the other hand, this ability, while promising an enormous business value, will pose some challenges to the existing regulatory framework and public security.

The virtual online space makes it easy for the collection and sharing of personal data and greatly facilitates the storage, analysis and exchange of information including identity IDs, health information, credit records, and location and movement information. However, at the same time, this makes it more difficult to determine how personal information was leaked and the degree of leakage. Examples include how to define the ownership of patients' electronic medical records and personal information in AI-supported smart healthcare, how to regulate hospitals' acquisition and use of patients' private data, and the copyright of AI-generated works. The open industry ecosystem will also make it difficult for regulatory authorities to determine the objects of regulation and blur the boundaries of laws.

The wide use of AI will bring about a radical change in human-machine relations in the form of a new mutually embedded relationship as human-machine interaction becomes increasingly complex. The unpredictability and irreversibility of the blurring of time and space and of virtual reality and reality will likely trigger a series of potential risks. Unlike information leakage that is often neglected by people, AI may be used by people with a secret agenda for fraud and other criminal activities, such as impersonation fraud on social media based on data profiling of personal information illegally obtained and security breach with information including image, video, audio and biometric information based on AI-enabled learning and simulation, as demonstrated by the hacking last year of iPhone's face ID system. In terms of potential risk, many things such as drones, autonomous cars and intelligent robots are vulnerable to intrusion and unauthorized control for fraudulent or other criminal purposes.

5.2.3 AI's Impact on Social Equality

As AI R&D and applications make giant strides, a series of value issues have gradually surfaced. At present, there are still a lot of internet illiterates and old-timers who are defined as “outsiders” in the AI era which has even higher requirements on people’s educational level and technology literacy[5]. As AI technology advances, the digital divide will widen even further and translate into a divide in access to services and benefits. In the AI era, it will become

[5] Sun Weiping. “Reflection on the Value of AI”, Philosophical Researches, No. 10, 2017

even more difficult for the “outsiders” to access convenient intelligent information services and scarce service resources.

For human society, AI technology should be for the benefit of all in accordance with the principle of equality and has the benefits and conveniences it brings accessible to as many people as possible. At the Beneficial AI conference held in Asilomar in the United States in early 2017, the “Asilomar AI Principles” were emphasized, i.e. developing AI in a way that is safe, transparent, responsible, accountable, contributable to society and for the benefit of the majority of people. [6]The best way to promote harmonious and positive human-machine relations is to make public services benefit all regions, all industries and all groups equally. Therefore, amid rapid AI development, it is necessary to think and come up with methods of using AI to improve basic public service platforms to steadily narrow the digital divide, build an efficient, developed and livable intelligent society, advance social inclusiveness and sustainable development, and create a beautiful future where the benefits of technology are enjoyed by all citizens.

5.3 Survey of China's AI Education

5.3.1 Current Situation of China's AI Education Development

As an interdisciplinary emerging technology field, AI involves various disciplines such as computer science, mathematics, neuroscience, statistics, electronic information engineering and automation. The basic courses in the field of AI mainly include basic computer courses such as programming language, algorithm design and data structure, as well as basic mathematics courses such as probability and mathematical statistics, numerical analysis and mathematical planning, and also courses related to engineering and natural sciences and humanities.

Since the Ministry of Education approval of the "Intelligent Science and Technology" undergraduate program at Peking University in 2004, higher education in AI has attracted more and more attention from universities. By July 2017, there had been as many as 36 universities approved by the Ministry of Education to offer the "Intelligent Science and Technology" undergraduate program, in addition to 79 programs related to AI[7]. Universities including University of Chinese Academy of Sciences, Xidian University, Nanjing University, Chongqing University of Posts and Telecommunications, Hunan University of Technology, Changchun University of Science and Technology, Tianjin University and Nankai University have established their AI colleges.[8]

In terms of undergraduate education, the Next Generation Artificial Intelligence Development Plan issued by the State Council in 2017 clearly pointed out that it is necessary to “improve the AI discipline structure, establish the AI specialty, and promote AI as a first-level discipline”, and requires AI pilot universities to establish their AI colleges as soon as possible. The Argumentation Report on Intelligence Science and Technology as a First-level Discipline issued by Chinese Association for Artificial Intelligence (CAAI) made the suggestion that the first-level discipline Intelligence Science and Technology” be divided into five second-level disciplines including “brain cognition”, “machine perception and pattern recognition”, “natural language

[6] Duan Weiwen. “Value Examination and Ethical Regulation in the AI Era”, Journal of Renmin University of China, No. 6, 2017
[7] Data source: “Call for AI as a first-level discipline”, Guangming Daily http://epaper.gmw.cn/gmrb/html/2017-07/28/nw.D110000gmrb_20170728_1-06.htm
[8] Data source: Nankai University and Tianjin University inaugurate AI colleges on the same day, focusing on robotics and brain cognitionhttps://www.thepaper.cn/newsDetail_forward_2133192

processing and understanding", "knowledge engineering" and "robotics and intelligent systems", with courses including basic specialized courses (such as "cognitive mechanism of brain, neural network, computational cognition, interactive cognition, memory cognition, introduction to artificial intelligence, robotics and machine ethics) and other specialized courses (such as cognitive physics, memory and reasoning, natural language processing and understanding, uncertainty in artificial intelligence, machine translation, emotional robots, intelligent robots, image cognition, machine learning, data mining and knowledge mapping).

In postgraduate education, the Next Generation Artificial Intelligence Development Plan required "increasing the quotas of doctoral and master's candidates in AI and related disciplines". It encouraged universities, on their existing basis, to expand the content of AI specialized education to form the new "AI+X" hybrid specialized training model with a greater focus on the integration of AI with other disciplines such as mathematics, computer science, physics, biology, psychology, sociology and jurisprudence. At present, China's AI teaching and research activities are concentrated in computer science, electronic information and automation faculties/departments of universities. In addition, leading Chinese universities have established their AI labs (Table 5-1).

Table 5-1 AI Labs at leading Chinese universities

No.	University	Lab
1	Tsinghua University	State Key Laboratory of Intelligent Technology and Systems
2	Peking University	State Key Laboratory of Visual and Auditory Information Processing Laboratory, MOE Key Laboratory of Machine Perception
3	Chinese Academy of Sciences	State Key Laboratory of Pattern Recognition, Key Laboratory of Intelligent Information Processing
4	Zhejiang University	Institute of Artificial Intelligence, i-MD Research Center for Artificial Intelligence
5	Shanghai Jiao Tong University	Intelligent Computing and Intelligent Systems Laboratory (co-developed with Microsoft Research Asia)
6	Nanjing University	State Key Laboratory for Novel Software Technology
7	Fudan University	Institute of Science and Technology for Brain-Inspired Intelligence
8	Harbin Institute of Technology	MOE-MS Key Laboratory of Natural Language Processing and Speech
9	University of Science and Technology of China	National Engineering Laboratory for Brain-inspired Intelligence Technology and Application
10	Beijing University of Posts and Telecommunications	Lab of Mobile Robot and Intelligent Technology

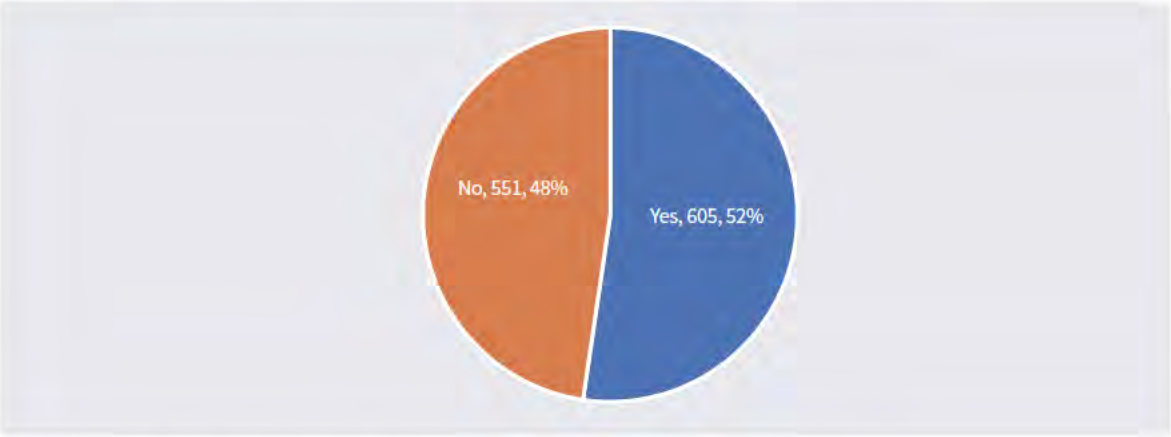
Source: *2017 Global Artificial Intelligence Talent White Paper*, Tencent Research Institute

In addition to degree programs at universities, there are various online learning platforms in China that offer AI courses and serve as a necessary supplement to the AI academic education. Currently, major active online education platforms include study.163.com, www.xuetangx.com, www.mooc.cn and www.icourse163.org.

5.3.2 Questionnaire on AI Education

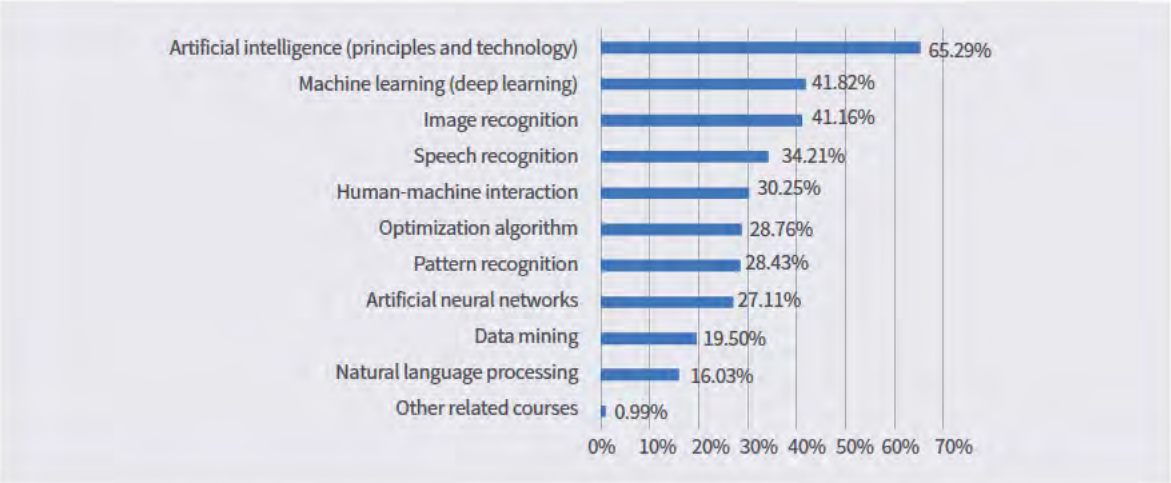
To get a further understanding of China's AI education development, this report collected first-hand data through an online questionnaire survey. The survey, conducted via the WJX platform, collected a total of 1,154 valid responses (as of May 15, 2018). The platform automatically recommends questionnaires to more than 500,000 visitors for completion every day. The valid responses had a fairly balanced age structure and university distribution, with most of the respondents (57.19%) falling within the 20-30 age group, which met the survey's expectation.

Question 1: Have you ever taken an AI course? [Single-select multiple choice question]



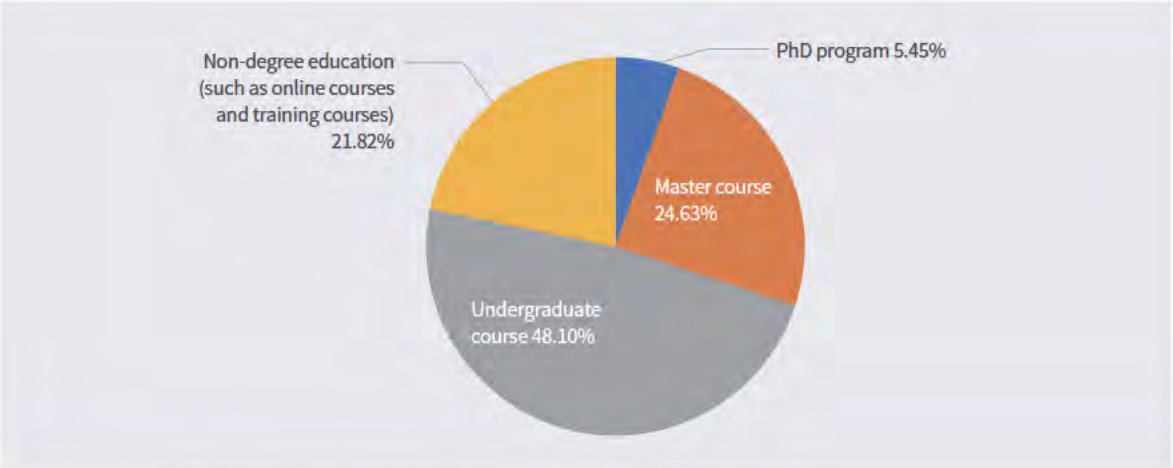
More than half of the 1,154 respondents have taken some sort of AI course (52.34%).

Question 2: Which of the following technologies did your courses cover? [Multi- select multiple choice question]



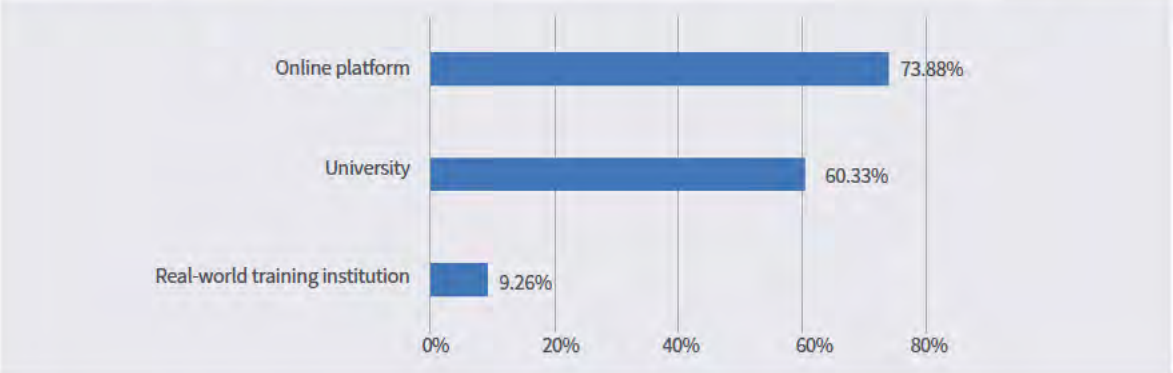
Among the AI courses, "artificial intelligence (principles and technology)", "machine learning (deep learning)" and "image recognition" are the top three most popular courses.

Question 3: At what stage of education did you take your AI course? [Single- select multiple choice question]



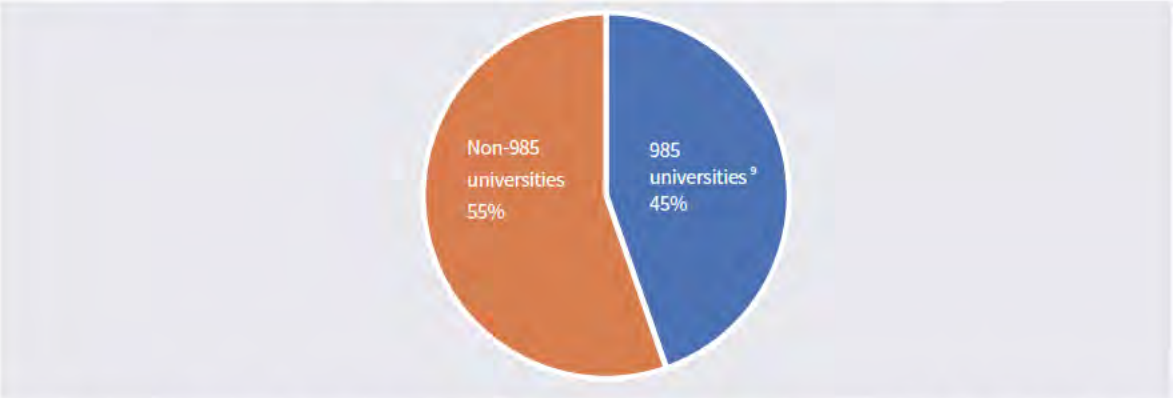
Most respondents took their AI course during their undergraduate studies.

Question 4: At what type of institutions did you take your AI course? [Multi- select multiple choice question]



University and online education are the top two platforms of AI course.

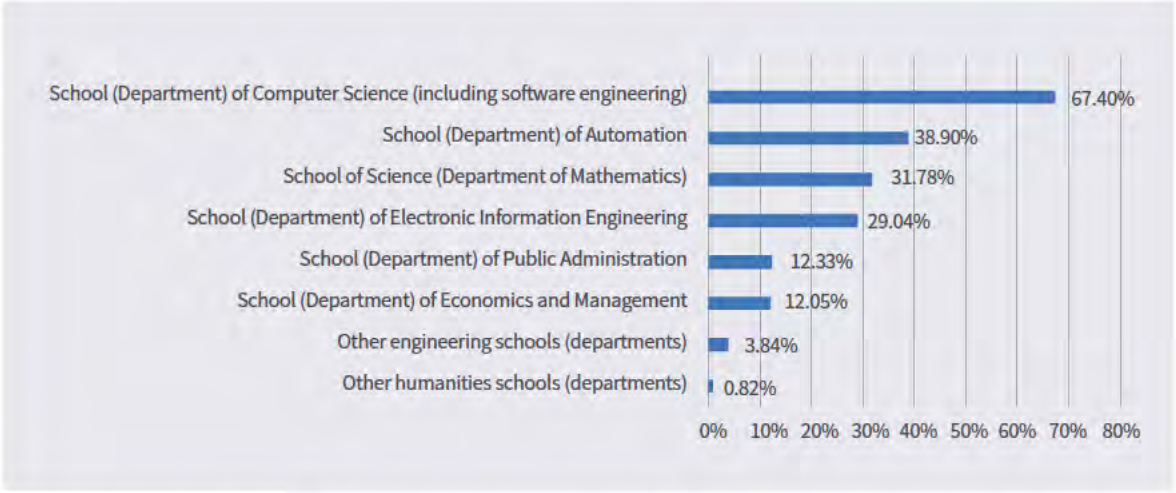
Question 5: At what university did you take your AI course? [Fill-in-the-blank question]



Note: Based on the number of respondents, the pie chart reflects the proportion of respondents who have studied artificial intelligence courses at a certain type of institution (985/non-985).

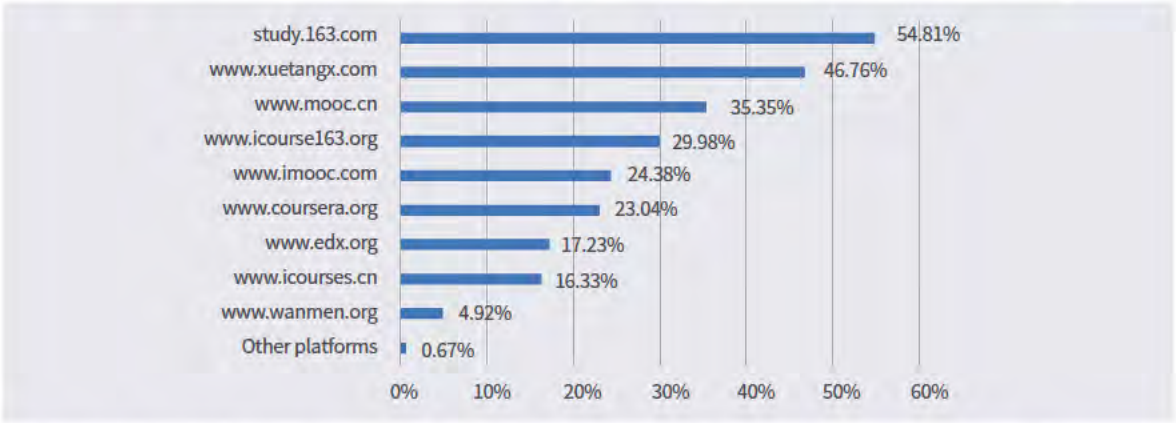
[9] a group of elite universities in China, as identified by the "985 Program"

Question 6: At what school/department did you take your AI course? [Multi- select multiple choice question]



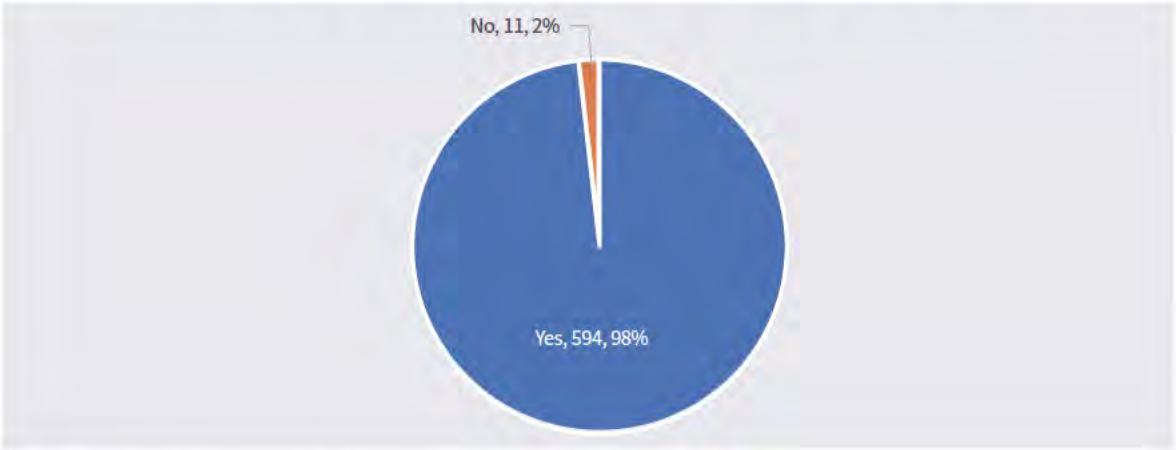
AI courses are mostly offered by computer and automation schools

Question 7: On what online platform did you take your AI course? [Multi-select multiple choice question]



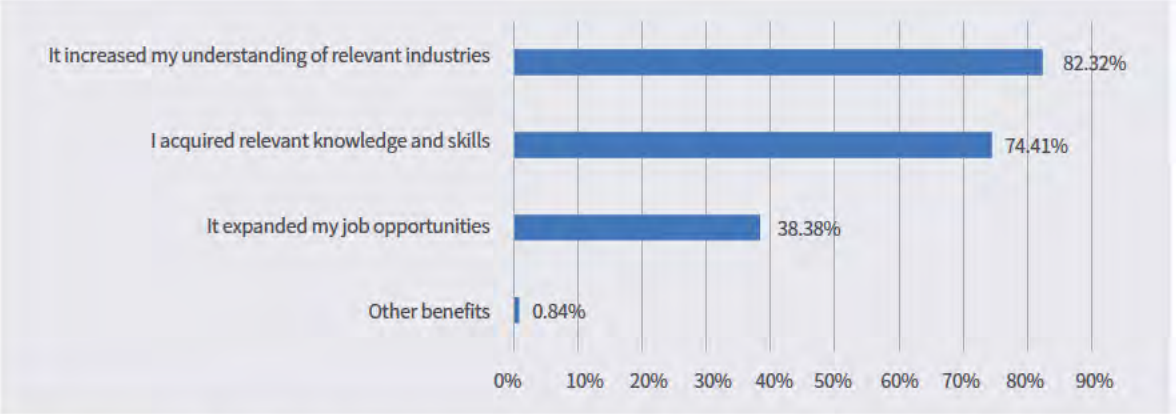
The main online platforms reported include study.163.com, www.xuetangx.com and www.mooc.cn.

Question 8: Do you think your AI course was helpful? [Single-select multiple choice question]



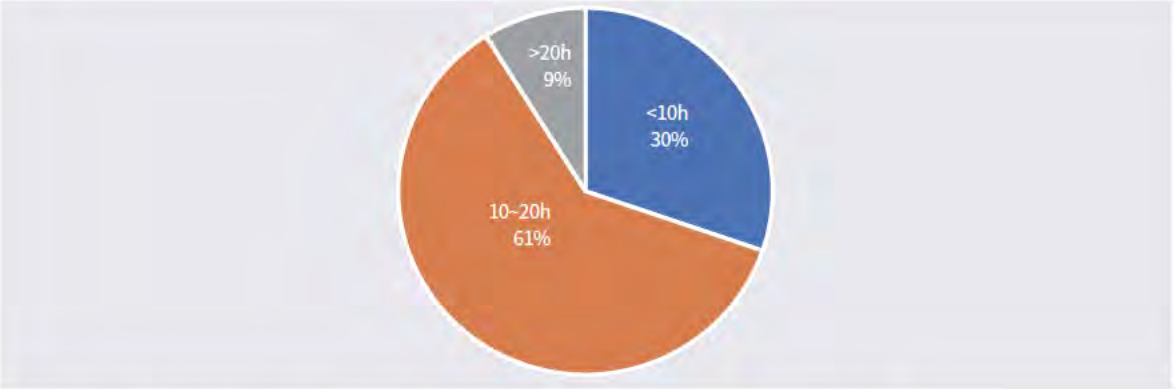
More than 98% of the respondents considered the courses to be helpful.

Question 9: In what ways do you think your AI course helped you? [Multi select multiple choice question]



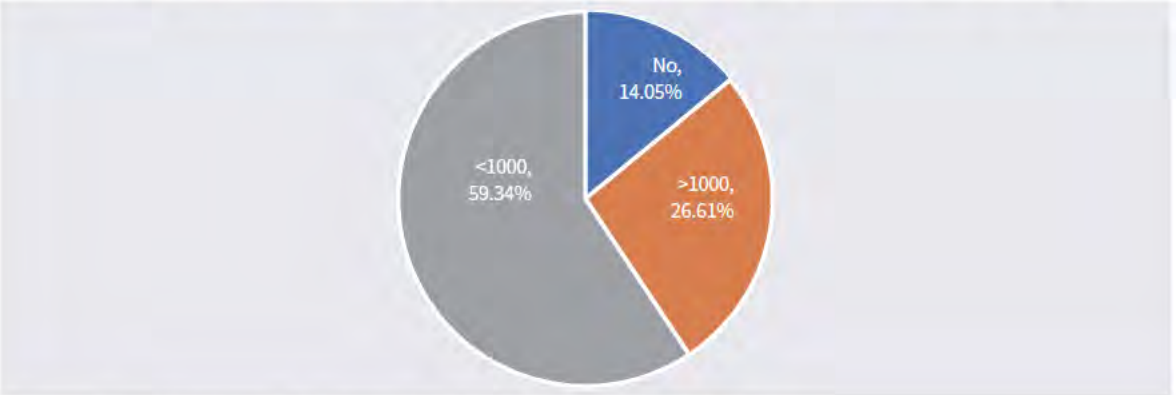
Only approximately 38% of the respondents stated that their AI courses expanded their job opportunities. The AI courses benefited the respondents mainly by way of acquisition of relevant knowledge and skills and strengthening their understanding of relevant industries.

Question 10: How much time did you devote to your AI course? (Weekly average) [Single-select multiple choice question]



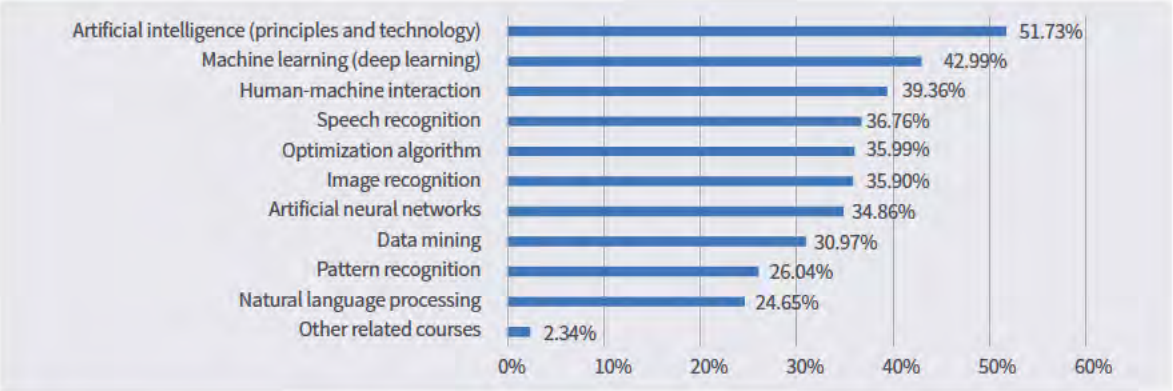
Approximately 61% of the respondents spent 10-20 hours on their AI courses per week.

Question 11: How much money did you spend on your AI course? [Single-select multiple choice question]

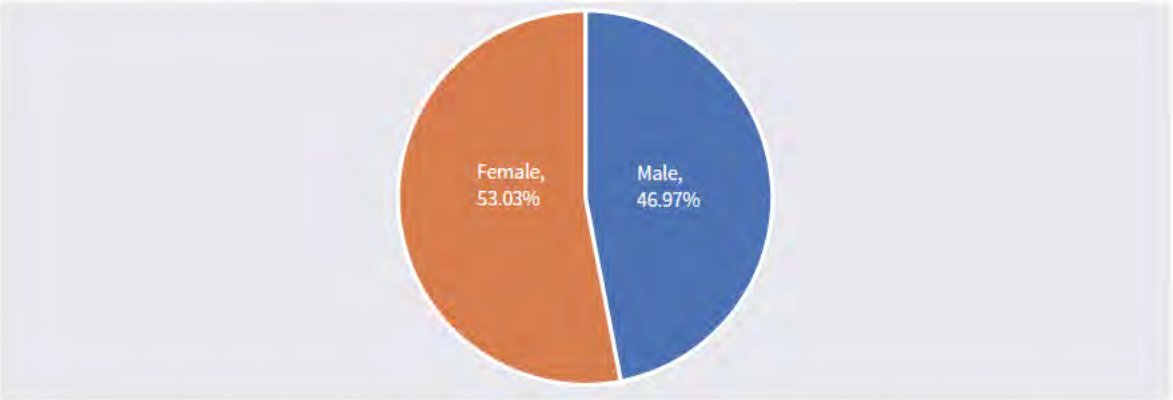


The majority of the respondents spent less than RMB 1,000 on their AI courses.

Question 12: What AI-related courses do you want to learn in the future? [Multi- select multiple choice question]

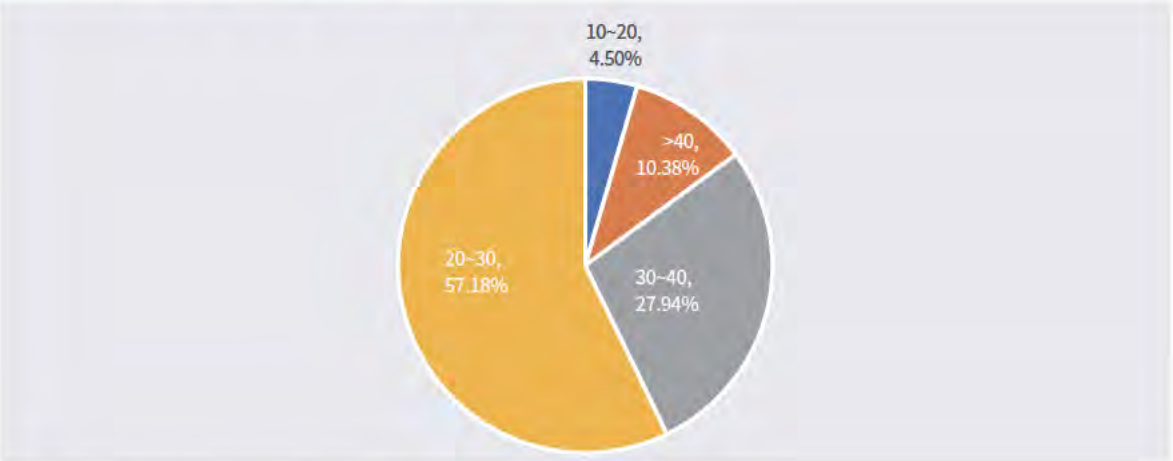


Question 13: Your gender? [Single select multiple choice question]



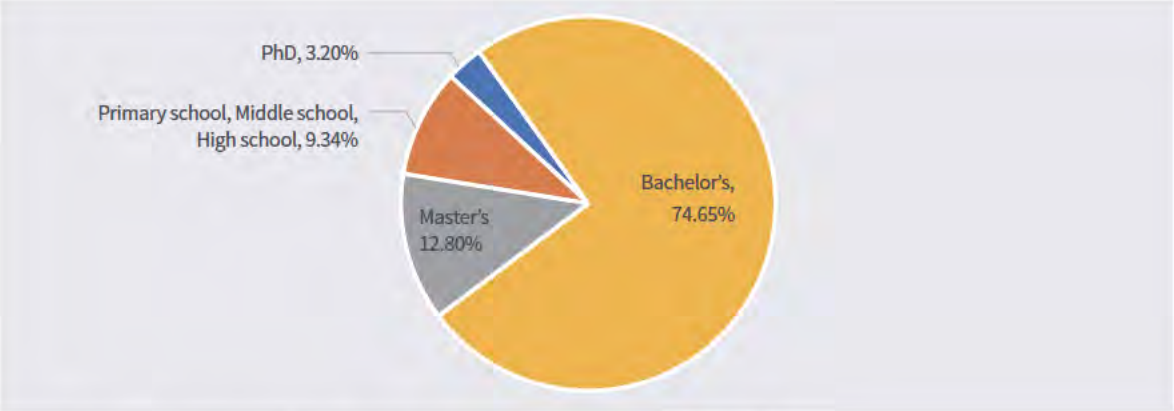
The respondents had a rather balanced gender ratio, with female respondents (approximately 53%) slightly outnumbering male respondents.

Question 14: Your age? [Single-select multiple choice question]



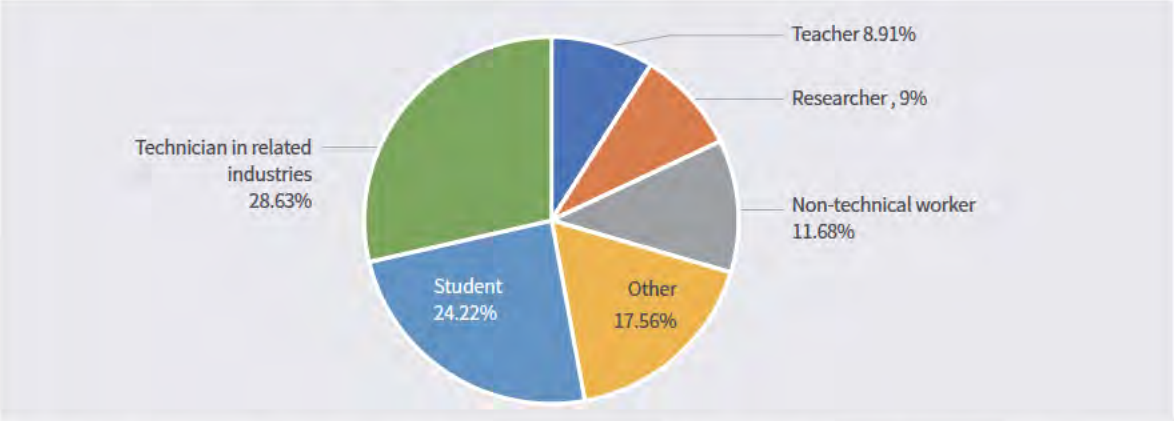
More than half of the respondents (57%) were in the 20-30 age group.

Question 15: Your education? [Single-select multiple choice question]



The majority of the respondents (approximately 75%) have a bachelor's degree.

Question 16: Your occupation? [Single-select multiple choice question]



The respondents were dominated by students (approximately 24%) and technicians (approximately 29%).

The survey found that the majority of the respondents had a strong enthusiasm for AI learning, with 61% spending 10-20 hours on AI learning per week and 85% expressing willingness to take paid courses. In terms of the channels of learning, online platforms have become an important channel of AI courses; among universities, AI courses are mainly offered by the school (department) of computer science, school (department) of automation, school (department) of science (mathematics) and school (department) of electronic information engineering. Technicians in related industries, researchers and students are the most enthusiastic groups for AI learning.


06
Reflection and Outlook

06 Reflection and Outlook

6.1 Summary and Reflection

Based on existing research reports and the above findings in this report, we can arrive at the following preliminary judgments and observations on China's AI development.

China has ranked among leading countries in AI technology development and market applications and is indeed in a race of "two giants" with the United States. In terms of technology output, industry development and applications, China is still significantly behind the United States overall but well ahead of other developed countries such as the United Kingdom, Germany, Japan and France. China is also behind the United States in the number of AI talents and enterprises but takes the lead in indicators such as AI papers and patents. In some specific fields like computer vision and intelligent speech recognition, China has been in an internationally leading position in both technology development and market applications. With respect to cities, Beijing has become the world's top AI city in terms of talent, enterprises, research institutions and venture capital. Overall, in the strategic field of AI, China has secured a head start and will maintain a growing momentum to achieve the goal of becoming a leading country in AI by 2030.

However, as far as the quality of development is concerned, China's AI development is far from being optimistic. China's strengths are mainly shown in AI applications and it is still weak on the front of core technologies of AI, such as hardware and algorithm, pointing to its not entirely solid foundation of AI development. Furthermore, although China's AI talents are next to the United States' in number, if only top-tier talents are considered, there is still a significant gap with the United States, the United Kingdom and Germany. As noted in Goldman Sachs' report, *China's Rise in Artificial Intelligence*[1], China's leading AI enterprises are mainly powered by returned overseas top talents. McKinsey's *Road to the Future of Artificial Intelligence*[2] report also attributed China's trailing far behind leading western countries in core algorithms to the lack of top-tier AI talents. University of Oxford's report, *Deciphering China's AI Dream*[3], which compared China and the United States on the four dimensions of hardware, data, algorithm and commercial system, found that China had a clear advantage on the data dimension only, and that its overall AI potential is only half of the United States'. *Therefore, China still faces a significant gap with the world-leading level in the core areas of AI development.*

In terms of the entities engaged in AI research, research institutes and universities are the main generators of AI knowledge in the world. According to the *Artificial Intelligence Index 2017* report[4], part of Stanford University's One Hundred Year Study

[1] Goldman Sachs. *China's Rise in Artificial Intelligence*, 2017
[2] McKinsey, *Road to the Future of Artificial Intelligence*, 2017
[3] Jeffrey Ding, University of Oxford, *Deciphering China's AI Dream—The context, components, capabilities, and consequences of China's strategy to lead the world in AI, 2018*
[4] Stanford One Hundred Year Study on AI,University, Artificial Intelligence Index 2017, 2017. http://aiindex.org/

on AI (AI100), academic activity is the main driving force of AI's stable development in its budding phase in the United States. The same thing is also true in China where research institutes and universities have generated the overwhelming majority of AI knowledge. Researchers from research institutes and universities represent 89% of all AI talents in China and are also leading forces in AI paper publication and patent application. Some research institutions and universities, such as the Chinese Academy of Sciences System and Tsinghua University, have become the powerhouses of China's AI technology development and held an important position in the world as well. However, it should also be realized that the substantial increase of scientific papers published by Chinese researchers in recent years has been on the one hand attributable to China's continuously increasing investment in R&D but on the other hand also had much to do with the over-emphasis on "papers" and "number-first" orientation in China's researcher evaluation system. In spite of the impressive growth of high-impact papers published by Chinese researchers in this field, research achievements that are original, ground-breaking or seminal, especially in basic research, are still very scarce.

China is already the world's largest patent applicant and the largest invention patent applicant and has more AI patent applications than the United States as well. However, it should be soberly realized that China's rapid patent growth—if not explosion—in recent years, while propelled by the country's economic transformation and transition from factor-driven to innovation-driven, has had much to do with all kinds of incentive policies, including performance evaluation indicators. Moreover, a large part of the patent applications in this field has been technological applications rather than underlying principles and key technologies. *Compared to their foreign counterparts, Chinese AI companies are technologically less inventive and far behind domestic universities and research institutions in AI patenting.* Even recognized domestic AI giants such as Baidu, Alibaba and Tencent (BAT) don't have an impressive performance in AI talent, papers and patents, while their U.S. competitors like IBM, Microsoft and Google lead AI companies worldwide in all indicators. Goldman Sachs' report, China's Rise in Artificial Intelligence, found that while Chinese internet giants have comparable R&D expenditure as a percentage of revenue, they are left far behind by their U.S. counterparts in terms of the absolute amount. China, though already the world's second largest AI ecosystem, still faces a significant gap with the United States.

In terms of leading enterprises, SGCC is the most prominent enterprise in both AI paper publication and AI patenting, which not only leads other Chinese enterprises by a big margin but also is high-ranked internationally. In China's AI patenting, electric power engineering is a prominent field. The fact that it has been either unmentioned or not highlighted in previous AI studies shows that the integration of AI with energy systems is likely an area that has been more or less neglected and represents a potential new direction of expansion of AI applications in China which will contribute to low-carbon transformation of the energy sector. *This example also demonstrates that it is ill-advisable to confine AI research to a number of emerging application areas and that the integration of AI with traditional sectors might represent a more promising direction.*

International collaboration and industry-university collaboration are important means of advancing AI development. As many as 42.64% of top papers on AI in the world were from international collaboration, versus 53% for China. As countries have different priorities and strength areas in AI development, international collaboration is significant by combining strengths and overcoming weaknesses and thereby promoting technological innovation

and should be encouraged and facilitated. At the same time, it should be noted that there is a lot of AI knowledge lying idle at Chinese universities and research institutions, and it is imperative to increase industry-university collaboration to promote AI knowledge application and transformation. According to the statistics, China's AI papers resulting from collaboration between research institutes and enterprises accounted for only 2.55% of its all AI papers, versus more than 6% for the United States, the United Kingdom, France and Germany. The researchers at big international technology firms represented by Microsoft, Google and IBM have not only filed for many patents, but also published a large number of papers, including high-impact papers. Some small and medium-sized technology firms, such as Deep-Mind and OpenAI, have even come to the forefront of AI research. AI is unlike traditional research areas in that the required resources such as data and computing power are controlled by large companies, meaning that they have better conditions than universities and research institutes to conduct research and tackle frontier issues. *Therefore, to advance research and applications in frontier areas of AI, China needs to not only encourage university-industry collaboration but also explicitly support enterprises to engage in basic AI research.*

With respect to the environment of AI development in China, both the central government and local governments have released policies in support of AI development; the capital market has shown a great enthusiasm for AI; most citizens have shown an optimistic attitude towards AI and a high interest in AI products; and there are all kinds of AI courses offered by universities and online education platforms which have been well received by young people. All these factors point to Chinese society's overall positive and optimistic attitude to AI, which has provided a very favorable environment in terms of policy, public opinion, market and talent for AI development. Policy keyword analysis found that local governments have shown a tendency of "following the steps of the central government" and "chasing after hot areas", raising the issue of how to avoid the problem of "redundant investment" which has frequently occurred in traditional industries and emerging strategic industries while promoting the sound development of AI, which policymakers need to come to grips with, especially in the new context of pursuing high-quality development. On the other hand, our survey has shown some worry and doubt of the public about AI development, a sentiment that has increased with media reports on relevant issues. Currently, China's AI policy has emphasized on promoting AI technological development and industrial applications and hasn't given due attention to such issues as ethics and security regulation. There are two extremes of view on AI, one considering AI as a "cure-all" and the other demonizing it. *How to properly guide the public opinion and attitude, strike a good balance between promoting AI development and putting AI development in an effective regulatory framework, and avoid the various negative issues that have previously occurred in other areas such as genetically modified food, will be a challenge and test of the government's governance ability and wisdom.*

6.2 Research Limitations and Prospect

At present, AI still lacks a clear universal definition, a tricky issue that is all too often encountered in the research of this emerging area. Although this report is based on a list of AI keywords strictly scrutinized and validated by experts, it cannot completely exclude activities which do not have much to do with core AI technologies. The use of keyword co-occurrence search as well as bibliometrics to identify AI academic output may lead to a broader, looser scope of data included. Given AI is an emerging phenomenon, a lot of industry statistics such as sales, corporate R&D, and gross product value are not up to date,

and therefore the industry development data in this report may not reflect the complete picture, which requires a set of more clear-cut criteria and more data investigation. Due to data availability, AI talent in this report is confined to researchers who have published AI papers or patents and thus AI specialists working in the industries may be less represented. Moreover, this report only examines the overall development of AI without scrutinizing its vertical areas such as infrastructure, hardware and data. All these are very important pillars of AI development and will be further examined in our future research.

China's AI development already enjoys very favorable conditions in the form of not only a vast application market and rich data but also strong policy support from the central government and local governments. But for China to become an AI superpower, the journey ahead is long and arduous. China must strengthen basic research, optimize the research environment, develop and attract top-tier talent, and make breakthroughs in core basic areas of AI to put the country's development on a solid foundation. Meanwhile, China needs to encourage university-industry collaboration to make enterprises a major force in AI innovation. China's AI policy research, which has so far tilted towards industry development and industry progress, should be more focused on the social impact and ethical implications of AI. AI technology development should be accompanied by social foresight with a view to supporting policymaking that steers AI development in anticipation of the technology roadmap and potential social impacts. Meanwhile, it is important to create mechanisms of public engagement in policy-making so that policies reflect and incorporate inputs from all sectors of society. Universities, research institutions and specialized research teams should also organize seminars and create relevant technical standards and norms and incorporate them in their educational or research activities. Finally, China should get actively involved in the global governance of AI and play a prominent role in relevant areas such as AI technology development, risk prevention and formulation of AI ethics norms to advance AI development for a beautiful future of human society.

Appendix 1: List of Main AI Conferences

Abbreviation	Full Name
AAAI	AAAI Conference on Artificial Intelligence
ICML	International Conference on Machine Learning
IJCAI	International Joint Conference on Artificial Intelligence
NIPS	Annual Conference on Neural Information Processing Systems
ACL	Annual Meeting of the Association-for-Computational-Linguistics
COLT	Annual Conference on Learning Theory
EMNLP	Conference on Empirical Methods in Natural Language Processing
ICPAS	International Conference on Automated Planning and Scheduling
ICCBR	International Conference on Case-Based Reasoning
KR	International Conference on Principles of Knowledge Representation and Reasoning
AAMAS	International Joint Conference on Autonomous Agents and Multiagent Systems
COLING	International Conference on Computational Linguistics
UAI	International Conference on Uncertainty in Artificial Intelligence
CVPR	Conference on Computer Vision and Pattern Recognition
ECAI	European Conference on Artificial Intelligence
ICRA	International Conference on Robotics and Automation
ICLR	International Conference on Learning Representations
IROS	International Conference on Intelligent Robots
NIPS	Neural Information Processing Systems

Appendix 2: Category Description

Computer Science, Artificial Intelligence

Computer Science, Artificial Intelligence covers resources that focus on research and techniques to create machines that attempt to efficiently reason, problem-solve, use knowledge representation, and perform analysis of contradictory or ambiguous information. This category includes resources on artificial intelligence technologies such as expert systems, fuzzy systems, natural language processing, speech recognition, pattern recognition, computer vision, decision-support systems, knowledge bases, and neural networks.

Appendix 3: Two Dimensions of AI Enterprise Identification

Technical Dimensions	
Speech	Speech recognition, speech synthesis, speech interaction, speech evaluation, human-machine dialogue, voiceprint recognition
Vision	Biometrics (face recognition, iris recognition, fingerprint recognition, vein recognition, etc.), affective computing, emotion recognition, expression recognition, behavior recognition, gesture recognition, body recognition, video content recognition, object and scene recognition, mobile vision, optical character recognition (OCR), handwriting recognition, text recognition, image processing, image recognition, pattern recognition, SLAM, spatial recognition, 3D scanning, 3D reconstruction, etc.
Natural language processing	Natural language interaction, natural language understanding, semantic understanding, machine translation, text mining (semantic analysis, semantic computing, classification, clustering), information extraction, human-machine interaction
Basic algorithm and platform	Machine learning, deep learning, open source framework, open platform
Basic hardware	Chips, lidars, sensors, etc.
Basic enabling technology	Cloud computing, big data
Product and Industry Dimensions	
Intelligent robotics (including solutions)	Industrial robotics (focusing on production processes such as handling, welding, assembly, palletizing and painting), service robotics (for banks, restaurants, hotels, shopping malls, exhibition halls, hospitals, logistics), personal/home robotics (virtual assistants, emotional support robot, child robot, educational robot, domestic robot (for floor and window cleaning, etc.), home security robot, in-vehicle robot)
Smart driving (including solutions)	Intelligent driving, driverless driving, autonomous driving, assisted driving, advanced driver assistance system (ADAS), laser radar, ultrasonic radar, millimeter wave radar, GPS positioning, high-precision map, vehicle chip, human-car interaction, etc.
Drone (including solutions)	Consumer drones (entertainment, aerial photography) Professional drones (agriculture, forestry, electric power, logistics, security, etc.)
AI+	Finance, insurance, judiciary administration, entertainment (social, games), tourism, healthcare, education, logistics and warehousing, smart home, smart city (traffic, electricity, environment), network security, video surveillance, commerce (marketing, retail, advertising) , human resources, corporate services

Appendix 4: AI Standards and Norms

	Organization	Main Research Areas	Main Standards
International	International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) Joint Technical Committee (JTC) 1	Key areas such as AI terminology, human-computer interaction, biometrics and computer image processing, as well as in AI enabling technologies such as cloud computing, big data and sensor networks	ISO/IEC2382-34:1999 Information technology – Vocabulary – Part 34: Artificial intelligence – Neural networks ISO/IEC 19794-2:2005 Information technology – Biometric data interchange formats – Part 2: Finger minutiae data ISO/IEC 29794-6:2015 Information technology – Biometric sample quality – Part 6: Iris image data ISO/IEC 8632-3 Information technology – Computer graphics – Metafile for the storage and transfer of picture description information – Part 3: Binary encoding
	International Organization for Standardization (ISO)	Industrial robots, smart finance, smart driving	ISO 11593:1996 Manipulating industrial robots – Automatic end effector exchange systems – Vocabulary and presentation of characteristics ISO 9946:1999 Manipulating industrial robots – Presentation of characteristics ISO 14539:2000 Manipulating industrial robots – Object handling with grasp-type grippers – Vocabulary and presentation of characteristics ISO 19092:2008 Financial services – Biometrics – Security framework ISO 14742:2010 Financial services – Recommendations on cryptographic algorithms and their use
	International Electrotechnical Commission (IEC)	Wearable devices	No specific standard released for the moment
	International Telecommunication Union (ITU)	At the AI for Good Global Summit held in June 2017, ITU-T put forward AI proposals on "Artificial Intelligence and Internet of Things" (ITU-T Y.AI4SC) and "Requirements of machine learning based QoS assurance for IMT-2020" (ITU-T Y.qos-ml).	No specific standard released for the moment
Overseas	Institute of Electrical and Electronics Engineers (IEEE)	Focused on research on AI ethical standards	IEEE P7000 Model Process for Addressing Ethical Concerns During System Design; IEEE P7001 Transparency of Autonomous Systems; IEEE P7002 Data Privacy Process; IEEEP7003 Algorithmic Bias Considerations; IEEE P7004 Standard for Child and Student Data Governance; IEEE P7005 Standard for Transparent Employer Data Governance IEEE P7006 Standard for Personal Data Artificial Intelligence (AI) Agent.
	National Institute of Standards and Technology (NIST)	NIST has conducted research in various AI areas including AI acquisition and analysis tools, future expert systems, AI-based collective production quality control, high-throughput material discovery and optimization, and optimized applications of machine learning	No specific standard released for the moment
China	Standardization Administration of China (SAC)	Focused on vocabulary, human-machine interaction, biometrics, big data, cloud computing, etc.	Information technology – Vocabulary – Part 31: Artificial intelligence – Machine learning Information technology – Vocabulary – Part 34: Artificial intelligence – Neural networks Specification of programming interface for Chinese speech recognition internet service Specification of programming interface for Chinese speech synthesis internet service

Appendix 5: AI Policy Data Sources

The U.S. AI policy documents are mainly from the Executive Office of the President and the National Science and Technology Council and Office of Management and Budget under it. Their websites are as follows:

Policy documents of the Executive Office of the President of the United States and its functions	https://www.whitehouse.gov
U.S. Networking and Information Technology Research and Development (NITRD) Program	https://www.nitrd.gov
U.S. Department of Homeland Security	https://www.dhs.gov
U.S. National Science and Technology Council (NSTC)	http://www.nstc.org.zm

The AI policy documents for other countries or regions are from their relevant government authorities, parliaments, national academies of sciences and related councils. Their websites are as follows:

European Union	https://www.eu-robotics.net/
German Federal Government	https://www.bundesregierung.de/Content/Infomaterial
German Federal Ministry for Economic Affairs and Energy	https://www.bmwi.de/Redaktion
German Academy of Science and Engineering	http://www.acatech.de/
German Federal Ministry of Education and Research	https://www.bmbf.de
French Parliament	https://www.aiforhumanity.fr
UK Engineering and Physical Sciences Research Council	http://hamlyn.doc.ic.ac.uk/ https://subtleengine.org/ https://assets.publishing.service.gov.uk/government
UK Parliament Science and Technology Committee	https://publications.parliament.uk
UK AI experts	https://assets.publishing.service.gov.uk/government
Prime Minister of Japan and His Cabinet	https://www.kantei.go.jp
Artificial Intelligence Technology Strategy Council	http://www.nedo.go.jp/

Data source of China's AI policy documents: China's AI policy documents are retrieved from the Government Documents Information System (GDIS) of Tsinghua University School of Public Policy and Management.

Working Group and Acknowledgement

Academic Advisers

Prof. Pan Yunhe, Member of Chinese Academy of Engineering
Prof. Wu hequan, Member of Chinese Academy of Engineering

Overall Planning

China Institute for Science and Technology Policy at Tsinghua University:	Xue Lan, Liang Zheng, Dai Yixin, Deng Xinghua, Li Daitian, Yu Zhen, Yang Fangjuan

Research & Writing

China Institute for Science and Technology Policy at Tsinghua University:	Xue Lan, Liang Zheng, Yu Zhen, Li Daitian, Yang Fangjuan, Zhang Yiming, Xu Bohong
Government Documents Center at Tsinghua University School of Public Policy and Management:	Huang Cui, Su Jun, Yang Chao, Huang Xinping, Wang Yidong, et al
Beijing Saishi Technology Co., Ltd.:	Zhi Qiang, Huo Dongyun, Li Yanxi, Xu Shiqian, Xie Songyan, Wang Jindi
Clarivate Analytics:	Wang Lin, Guo Yang
China Academy of Information and Communications Technology:	Zhu Jiajia, Wang Xuemei, Zhang Yankun, Lu Yapeng, Yun Mengyan
Beijing Bytedance Technology Co., Ltd.:	He Jia, Wang Ying

Acknowledgement

The preparation of this report received guidance and assistance from the following experts and scholars, to whom we express our heartfelt thanks for their support. Special thanks to Jack Clark from Open AI for polishing this report.

School of Public Policy and Management, Tsinghua University	Prof. Meng Qingguo, Prof. Yang Yongheng, Assoc. Prof. Zhang Nan, Assoc. Prof. Zhou Yuan
School of Social Sciences, Tsinghua University	Prof. Li Zhengfeng, Prof. Zhang Chenggang, Dr Chen Shouzhu
School of Law, Tsinghua University	Prof. Shen Weixing, Assoc. Prof. Cui Guobin, Dr He Yuan
Department of Automation, Tsinghua University	Prof. Zhang Tao, Prof. Zhang Zuo, Prof. Zhao Qianchuan

Department of Electrical Engineering, Tsinghua University	Prof. Shen Chen
School of Management, Zhejiang University	Prof. Huang Can
Institute for Strategic Studies, Shanghai University	Prof. Li Renhan
Institutes of Science and Development, Chinese Academy of Sciences	Mu Rongping (RF), Sui Jigang (ARF)
National Academy of Innovation Strategy, China Association for Science and Technology	Luo Hui (RF), Liu Xuan (ARF)
Chinese Academy of Labor and Social Security	Mo Rong (RF), Dr Li Zongze
Institute of Quantitative & Technical Economics, Chinese Academy of Social Sciences	Qi Jianguo (RF)
Development Research Center of the State Council	Lv Wei (RF), Zhao Changwen (RF), Wang Xiaoming (RF)
Bytedance Institute of Technology Strategy	Dr Zhang Hongjiang
China Academy of Information and Communications Technology	Dr Liu Yue
Beijing University of Technology School of Economics and Management	Li Xin (ARF), Dr Yuan Fei
Tus-Holdings Co., Ltd.	Mr. Wang Shugui, Mr. Yang Ming, Mr. Lin Zhuocun
JD.com, Inc.	Dr Zhou Bowen
Siemens UK	Dr Paul Beasley
Department of Computer Science, Cornell University	Prof. John Hopcroft
Artificial Intelligence Lab, Stanford University	Prof. Yoav Shoham
Harvard Law School	Prof. Urs Gasser
Technology and Management Centre for Development, University of Oxford	Prof. Xiaolan Fu
Science and Technology Policy Research, University of Sussex	Prof. Ed Steinmueller
Institute for Innovation Research, University of Manchester	Prof. Philip Shapira
Newcastle Business School at Northumbria University	Prof. Yu Xiong
Institute for Scientific Information at Clarivate Analytics	Dr Jonathan Adams
Joint Research Centre, European Commission	Dr Koen Jonkers
Institute of Electrical and Electronics Engineers	Mr. John Havens, Ms. Victoria Wang
Open AI	Mr. Jack Clark
World Economic Forum	Mr. Danil Kerimi

About the Sponsoring Organizations

Sponsoring Organizations:

清华大学中国科技政策研究中心
China Institute for Science and Technology Policy at Tsinghua University

The China Institute for Science and Technology Policy (CISTP) at Tsinghua University is a science and technology policy and development strategy research institute jointly founded by the Ministry of Science and Technology of China and Tsinghua University in 2003. Positioned as an international research institute with a high starting point, broad horizon and visionary foresight with the focus on the strategy of national invigoration through science and technology, sustainable development strategy and long-term national development goals, CISTP conducts theoretical and applied research on international S&T development trends, national S&T development strategy and related public policy and aims to become a leading institution in S&T policy and development strategy. Since its establishment, it has taken part in or undertaken a series of important research projects, including strategic research on national medium- and long-term S&T development plan, strategic research on national medium- and long-term education reform and development plan, evaluation of the Chinese Academy of Sciences' pilot project of knowledge innovation, research on the revision of the Law on Progress of Science and Technology, Chinese Academy of Engineering advisory research on China's 11th Five-year Plan, and "Research on China's National Innovation System and Innovation Policy" (collaboration with OECD). It has built remarkable expertise in research areas including national innovation system and S&T globalization and published academic articles in domestic and international high-level learned journals including Management World, China Soft Science, Studies in Science of Science and Nature, with some research reports and policy suggestions having been commented by national leaders with instructions and adopted and implemented by relevant policymaking bodies.

POLICY

The Government Documents Center at Tsinghua University School of Public Policy and Management (SPPM-GDC), established in 2005 as a research platform for disciplinary development, provides rich policy data and bibliometrics-based empirical research support for the development of the

public policy and management discipline in China and provides policymaking bodies with detailed comprehensive policy data and advisory and research support. The center has collected more than 1.6 million policy documents issued by China's central government and local governments since 1949 in a steadily expanding database with an addition of more than 150,000 policy documents annually. The center has a proprietary government documents information management system (IPolicy) which consists of data collection and input, full-text indexing and bibliometric analysis modules with extensive functions including new documents collection, formatted input, centralized management, online query, model analysis and thematic customization.

科学家在线
为知识寻找价值!

ScientistIn is an important platform serving innovation-driven regional development initiated by Yangtze Delta Region Institute of Tsinghua University, Zhejiang. Operated by Beijing Saishi Technology Co., Ltd. founded by a Tsinghua-Harvard team with investment from the Institute, ScientistIn is committed to integrating wisdom and expertise of Chinese scientists worldwide to provide process services for enterprises' technology-driven business transformation and provide policymakers with data support, on a mission to seek value for knowledge. ScientistIn currently has a Chinese expert database with 11 million entries and an international expert database with 6.5 million entries, including 4 million reachable; a patent database with more than 18 million entries; an S&T project database with 500,000 entries; a database of 800,000 Chinese technology companies; and S&T big data resources including local government industry plans nationwide.

Clarivate Analytics | 科睿唯安

Clarivate Analytics is the global leader in providing trusted insights and analytic. We enable trailblazers around the world to turn novel ideas into disruptive innovation and accelerate the pace of innovation and internationalization. We support the innovation and internationalization of global customers with comprehensive intellectual property and S&T information and decision support tools and services and help governments, academics, publishers and businesses discover new ideas, protect innovation, and achieve commercialization. We offer some of the most trusted brands across the innovation lifecycle, including Web of Science™ (including Science Citation Index, i.e. SCI), InCites™, Derwent Innovation™, Derwent World Patents Index™ (DWPI), Cortellis™, CompuMarkMark™, Monitor® and Techstreet™, among others.

CAICT 中国信通院

China Academy of Information and Communications Technology (CAICT), established in 1957, is a public research institution directly under the Ministry of Industry and Information Technology. Positioned as a national high-level specialized think tank and an industry innovation and development platform and steeped in the core values of "solid research for long-term industry development", CAICT has provided a strong support in many aspects including major strategies, plans, policies, standards, testing and certification of industry development and played an important role in driving the leap-frog development and take-off of China's ICT industry.

ByteDance 字节跳动

Beijing Bytedance Technology Co., Ltd., founded in March 2012, is the world's first company to apply AI to its main products. With the migration of reading behavior to mobile devices, Bytedance has achieved rapid development and established a superb reputation and influence in the industry. Bytedance allows content creators to distribute content more conveniently and helps all types of media better adapt to the mobile Internet era. While consolidating its position in the domestic market, Bytedance has proactively made deployments internationally and aims to become a world-leading mobile Internet company that provides advanced mobile Internet-based information distribution services globally.

Advisory Organization: Chinese Institute of Engineering Development Strategies (CIEDS)

中国工程院 Chinese Academy of Engineering

清華大學 Tsinghua University

About CIEDS: The Chinese Institute of Engineering Development Strategies (CIEDS) was jointly established by the Chinese Academy of Engineering and Tsinghua University in April 2011 to improve the level of research on engineering development strategies in China and create a first-rate engineering thinktank platform. Oriented to high-level, open-ended and forward-looking development with the focus on holistic, general and strategic research projects in engineering science and technology

development based on theoretical and applied research, policy advice, pre-planning research and personnel training, CIEDS strives to build a leading strategy research institute featuring "small entity, large alliance, network-based collaboration" and a top-level thinktank in engineering science and technology and an important member of China's high-level thinktank network. Its main functions include 1) undertaking engineering development strategies advisory research projects of the Chinese Academy of Engineering and providing advisory services for the strategic policymaking of the state and relevant ministries and commissions; 2) conducting research on important theoretical issues of engineering development and building a database of engineering development strategy and policy documents; 3) conducting research on theories, methods and processes of engineering development strategy formation and advancing relevant disciplines relating to engineering development; 4) developing research, teaching and management personnel in engineering development strategies; 5) providing engineering strategy advisory services for large enterprises, public institutions and social organizations; and 6) advancing international exchange and cooperation in engineering development strategy research.

China Institute for Science and Technology Policy at Tsinghua University

Add: School of Public Policy & Management, Tsinghua University, Haidian, Beijing, 100084, China
Tel: +861062797212
E-mail: cistp@mail.tsinghua.edu.cn
Website: http://cistp.sppm.tsinghua.edu.cn/

Defense Innovation Unit Experimental (DIUx)

China's Technology Transfer Strategy:

How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation

Updated with 2016 and 2017 Data

Michael Brown and Pavneet Singh

January 2018

UNCLASSIFIED

DEFENSE INNOVATION UNIT EXPERIMENTAL

Silicon Valley | Boston | Austin | Washington D.C.

Executive Summary

This report explores China's participation in venture deals[1] financing early-stage technology companies to assess: how large the overall investment is, whether it is growing, and what technologies are the focus of investment. **Chinese participation in venture-backed startups is at a record level of 10-16% of all venture deals (2015-2017)** and has grown quite rapidly in the past seven years. The technologies where China is investing are the same ones where U.S. firms are investing and that will be foundational to future innovation: artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics and blockchain technology. Moreover, these are some of the same technologies of interest to the U.S. Defense Department to build on the technological superiority of the U.S. military today. The rapidity at which dual-use technologies are developed in the commercial sector has significant impact on the nature of warfare; mastering them ahead of competitors will "ensure that we will be able win the wars of the future".[2]

Because the U.S. economy is open, foreign investors, including those from China, are able to invest in the newest and most relevant technologies gaining experience with those technologies at the same rate as the U.S. does. The U.S. government does not currently monitor or restrict venture investing nor the potential transfer of early-stage technology. The primary tool the government has to block or mitigate foreign investment is the Committee on Foreign Investment in the United States (CFIUS); however, since CFIUS reviews specific deals on a case-by-case basis (rather than systematic assessments of acquisitions or acquirers) and only deals that involve a controlling interest by foreign investors (usually mergers and acquisitions), CFIUS is only partially effective in protecting national security since its jurisdiction is limited. The other principal tool to inhibit technology transfer is the U.S. export control regime. Export controls are effective at deterring exports of products to undesirable countries and can be used to prevent the loss of advanced technologies but controls were not designed to govern early-stage technologies or investment activity. Importantly, to be effective, export controls require collaboration with international allies, a long process where cooperation is not assured.

Further, venture investing is only a small part of China's investment in the U.S.--which includes all forms of investment and investor types. Investing is itself only a piece of a larger story of massive technology transfer from the U.S. to China which has been ongoing for decades. This report places venture investing within the larger context of China's long-term, systematic effort to attain global leadership in many industries, partly by transferring leading edge technologies from around the world.

U.S. military superiority since World War II has relied on both U.S. economic scale and technological superiority. U.S. technological pre-eminence enabled the series of offset strategies which included being first with nuclear weapons (the First Offset) and the electronics-enabled weapons of night vision, laser-guided bombs, stealth and jamming technologies as well as spaced-based military communications and navigation enabling the U.S. to dominate the battlefield (the Second Offset). Much of this technology came from research sponsored by the U.S. government and

[1] A venture deal is a financing that provides startup or growth equity capital provided by private investors, usually venture capitalists.

[2] The 2018 National Defense Strategy recognizes the critical role of technology development in the commercial sector for national security purposes: "The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our nation has grown accustomed. Maintaining the department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base." p. 3

the Defense Department specifically. However, the technologies which will create the Third Offset are to a large extent being developed by early-stage technology companies with significant commercial markets. If we allow China access to these same technologies concurrently, then not only may we lose our technological superiority but we may even be facilitating China's technological superiority.

That China will grow to be an economy as large as ours may be inevitable; that we aid their mercantilist strategy through free trade and open investment in our technology sector is a choice. As a result, while strategic competition3 with China is a long-term threat rather than a short-term crisis, preserving our technological superiority and economic capacity are important issues for national focus today.

Key Points

- China is executing a multi-decade plan to transfer technology to increase the size and value-add of its economy, currently the world's 2nd largest. By 2050, China may be 150% the size of the U.S.[4] and decrease U.S. relevance globally[5].
- Technology transfer to China occurs in part through increasing levels of investment and acquisitions of U.S. companies. **China participated in ~16% of all venture deals in 2015 up from 6% average participation rate during 2010-2015.**
- **China is investing in the critical future technologies that will be foundational for future innovations both for commercial and military applications: artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, financial technology and gene editing.** The line demarcating products designed for commercial vs. military purposes is blurring with these new technologies.
- Investments are only one means of technology transfer, which also occurs through the following licit and illicit vehicles where the cost of stolen intellectual property has been estimated at $300 billion per year.[6]
  - Industrial espionage, where China is by far the most aggressive country operating in the U.S.
  - Cyber theft on a massive scale deploying hundreds of thousands of Chinese army professionals
  - Academia, since 25% of U.S. STEM graduate students are Chinese foreign nationals
  - China's use of open source information cataloguing foreign innovation on a large scale
  - Chinese-based technology transfer organizations
  - U.S.-based associations sponsored by the Chinese government to recruit talent
  - Technical expertise on how to do deals learned from U.S. firms.
- China's goals are to be #1 in global market share in key industries, to reduce reliance on foreign technology and to foster indigenous innovation. Through published documents such as Five-Year Plans and Made in China 2025, China's industrial policy is clear in its aims of import substitution and technology innovation.
- There are several examples of Chinese indigenous innovation where China is doing much more than copying technology.
- **The U.S. does not have a comprehensive policy or the tools to address this massive technology transfer to China.** CFIUS is one of the only tools in place today to govern foreign

investments but it was not designed to protect sensitive technologies. CFIUS is only partially effective in protecting national security given its limited jurisdiction.

- **The U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting.**
- DoD has several specific areas of risk resulting from the scale of China's investments and its technology transfer:
  - Supply chains for U.S. military equipment and services are increasingly owned by Chinese firms.
  - China's targeted investments to close the gap in capabilities between its military and the U.S. military.
  - Industrial espionage and cyber theft mean key defense designs and plans are in Chinese hands.
  - There is no agreed upon list of technologies to protect for the future though an effort exists today to delineate technologies critical to current acquisition programs (JAPEC[7]).

[3] As discussed in the summary of the 2018 National Defense Strategy, the central challenge to U.S. prosperity and security is the "reemergence of long-term strategic competition" by revisionist powers such as China and Russia.

[4] According to The Economist, U.S. GDP will be $70 trillion by 2050 and China's GDP will be $105 trillion. "Long Term Macroeconomic Forecasts--Key Trends to 2050," The Economist Intelligence Unit (2015).

[5] The U.S. has not competed with an economic rival that could be larger than its own economy in 150 years.

[6] "The IP Commission Report: The Report on the Theft of American Intellectual Property," National Bureau of Asian Research (May, 2013). Retrieved at http://www.ipcommission.org

[7] Joint Acquisition Protection & Exploitation Cell, described on p. 12 of this paper.

China's Growing Investment in the U.S. & in U.S. Technology

China's Global and U.S. Investment

China's global foreign direct investment (FDI) is growing rapidly and is at a record level in a range of $200-250 billion, with $213 billion in announced acquisitions in 2016.[8,9] China's FDI investment in the U.S. in 2016 was $45.6 billion and cumulative FDI in the U.S. since 2000 now exceeds $100 billion.[10] China's investment stems from a variety of motivations. As China's economy has grown to the world's second largest, there is a commercial interest in expanding to other markets as well as a motivation for companies and individuals to diversify their investments geographically and politically as well as hedge against currency fluctuations. With the recent concerns about devaluation of the currency relative to the U.S. dollar and concerns about the underlying economic fundamentals, Chinese investors have made more investments overseas and this has led to an increased level of capital controls.[11]

China's U.S. Technology Investment

China's total investment in U.S. technology (electronics, information and communications technology, biotech and energy) for the past decade, 2006-2016, totaled $35 billion and in 2016 was about $8.5B.[12] Since the U.S. is a global leader of technological innovation, it is logical that China would seek to make increasing investments in U.S. technology companies. While it is likely that China's investment in technology is driven in part by commercial interests, it is unlikely this is the sole reason given China's explicit technology goals. Investment is one of the means for China to accomplish its technology transfer goals.[13] Both these goals and China's multiple vehicles for technology transfer are described later.

China's U.S. Early-Stage Technology Investment

Chinese investment activity in *early stage technology* deals is also growing rapidly and peaked in 2015 with Chinese investors participating in 271 deals, with total deal value of $11.5 billion. **This represented almost 16% of the value of all technology deals in that year ($72 billion)**.[14] China invested on the order of $3-4 billion in early stage venture deals in 2015. The specific technology areas of these investments are covered in the next section.

These investments are consistent with China's goals made clear in President Xi Jinping's statements, successive Five Year Plans, Made in China 2025 and Project 863,[15] namely, to:

- Establish China as one of the most innovative countries by 2020 and a leading innovator by 2030;[16]
- Become a leading global science and technology power by 2049 -- the 100th anniversary of the PRC;
- Double down on R&D of core information and communications (ICT) technologies…to develop technologies on its own, *acquiring expertise from abroad when indigenous development is not possible.*

The growing investments in U.S. technology overall, and early-stage ventures in particular, comprise a part of China's plan to acquire expertise from abroad and to develop indigenous innovation.

[8] Lingling Wei, "China Issuing 'Strict Controls' on Overseas Investment," Wall Street Journal (November 26, 2016). Retrieved at http://www.wsj.com

[9] While China's global FDI has been growing at 33% annually since 2003, a leading China think tank expects global FDI to decline in 2017 to a level closer to 2015 and well below $200 billion. Lingling Wei, "China's Overseas Funding to Shrink," Wall Street Journal (January 14, 2017)

[10] Thilo Hanemann and Daniel Rosen, "Chinese Investment in the United States; Recent Trends and the Policy Agenda" Rhodium Group Report (December 9, 2016). Retrieved at http://www.rhg.com

[11] These capital controls and the slower growth rate of the Chinese economy are likely primary causes for the forecasted China global FDI to decline in 2017.

[12] China Investment Monitor, Rhodium Group, January 17, 2017; Retrieved at http://www.rhg.com

[13] "This strategy seems to be increasingly the norm in the tech industry, with Chinese companies making investments to soak up strategic technologies, capabilities, talent and brands that they can then take home." Ana Swanson, "Gold Rush: Chinese Tech Companies Invest Overseas," CKGSB Knowledge (April 20, 2015). Retrieved at http://knowledge.ckgsb.edu.cn/2015/04/20/finance-and-investment/gold-rush-chinese-tech-companies-invest-overseas/

[14] Data retrieved from CB Insights, October, 2017; data includes all rounds: Seed/Angel, Series A-E+, Convertible Notes, and "Other VC" investments.

[15] Project 863 is shorthand for the month (3/March) and year (1986) when it was introduced by China's leading strategic weapons pioneers to Deng Xiaoping. The proposal was approved and served as China's leading industrial R&D program, importantly reforming decision making to be less stove-piped and more collaborative; reorienting the procurement process; investing in training of technical experts; and developing technologies of strategic value.

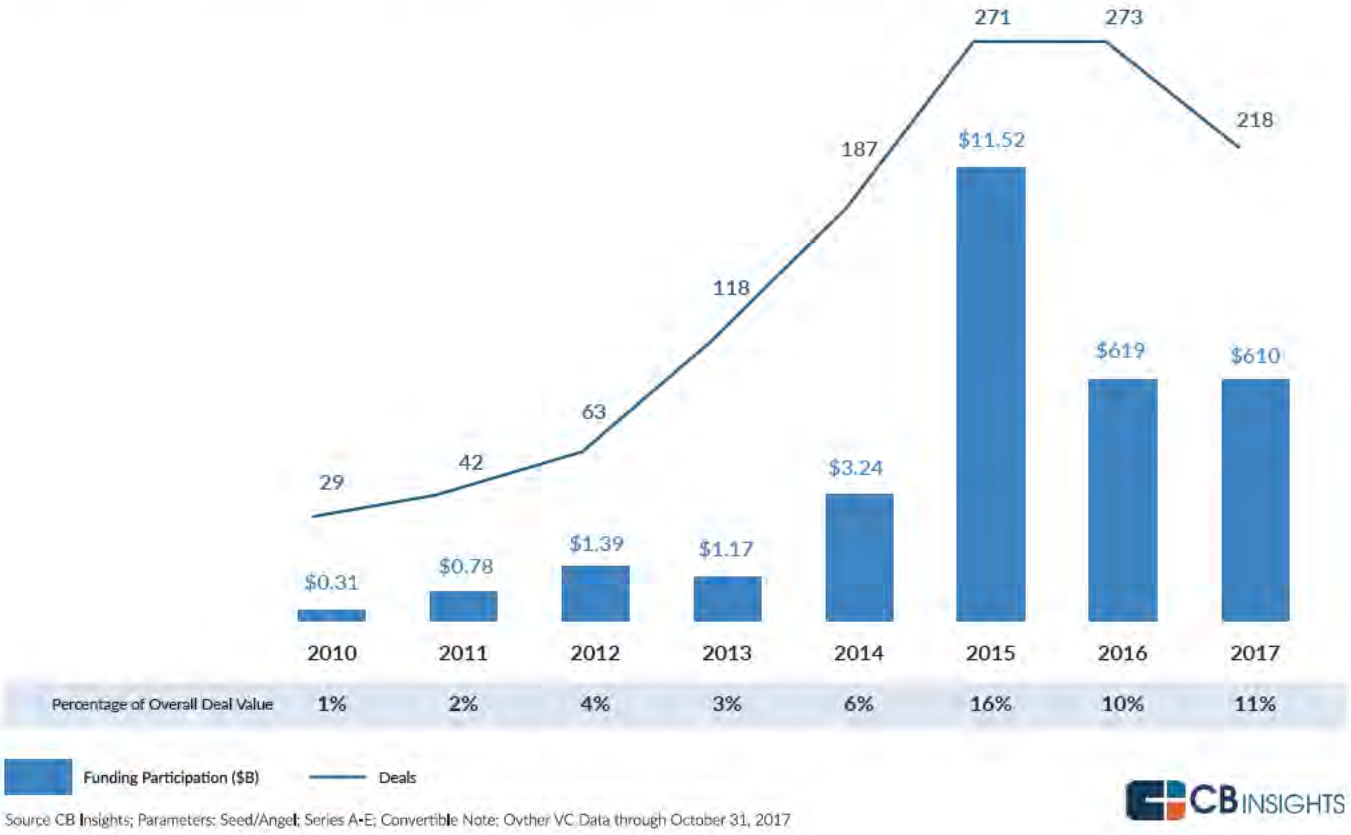
[16] "Xi Sets Targets for China's Science, Technology Progress" Xinhua (2016, May 30). Retrieved at http://www.xinhuanet.com

China's Investment in Critical Future Technologies

Investments from China-based[17] investors into early-stage U.S. technology companies continue to grow in all sectors and are dispersed across all the stages of the investment lifecycle.[18] Some notable investment data include:

- China-based investors participated in 1,201 financings in the U.S. from January, 2010 to October, 2017 contributing to roughly $31 billion in venture-backed funding. Over the same period, overall funding into early stage technology was roughly $372 billion, indicating that Chinese investors participated in 8% of overall deal value during this period (January, 2010 - October, 2017) hitting a peak of 16% in 2015 and remaining at roughly 10% in 2016 and 2017.
- Activity from Chinese investors peaked in 2015 participating in 271 deals valued at $11.52 billion. In 2016, Chinese investors participated in 10% of deals valued at $6.19 billion.[19]

Chart 1: Chinese Participation in U.S. Venture Capital Market, January 2010 - October 2017



Source CB Insights; Parameters: Seed/Angel; Series A-E; Convertible Note; Ovther VC Data through October 31, 2017

[17] For the purposes of this inquiry, China-based investors include investors from mainland China and Hong Kong.

[18] For the purposes of this study, we identified 537 unique investors from China that have invested in the United States from January 2010 to October 2017. These investors span from individual angel investors, Chinese entities serving as incubators or tech accelerators and traditional venture capital firms to corporations, banks, and hedge funds taking active stakes in early-stage companies. The full list of Chinese investment vehicle types included in the CB Insights database include: Incubator/Accelerator; Venture Capital; Corporation; Corporate Venture; Private Equity; Asset/Investment Management; Holding Company; Angel Investor; Investment Bank; Sovereign Wealth Fund; Angel Investor (Group); Hedge Fund; Advisory; Government; Diversified Financial Services; Merchant Bank; Family Office; Debt & Specialty Finance; Business Plan Competition

[19] Data retrieved from CB Insights, October, 2017; Data includes all rounds: Seed/Angel, Series A-E+, Convertible Note, and "Other VC" investments.

Table 1: Dispersion of Chinese Investment in U.S. Venture Capital Market, 2010 - 2016

Showing deals from Jan 01, 2010 - Oct 31, 2017

	Seed/Angel	Series A	Series B	Series C	Series D	Series E+
% of deals	32.73%	26.31%	17.12	12.31%	5.70%	5.79%
Avg. deal size	32.73%	$12.9M	$34M	$40.3M	$61.1M	$167.6M
Median deal size	$1.4M	$8M	$17.5M	$24M	$36.5M	$45M

- A majority of the investment occurred in the Seed/Angel stage (33% of all deals), followed by Series A (26% of all deals).[20] This corresponds with the recent increase in Chinese investment in early-stage technology deals and indicates that Chinese investors are interested in early looks at the most promising (even if yet unproven) technologies.
- By country, China invests far more in U.S. early stage technology companies than any other country outside the U.S. Details on this comparison by country are in Appendix 1.

Investment in Critical Technologies

China-based investors are particularly active in the emerging technology sectors of Artificial Intelligence, Augmented Reality/Virtual Reality, Robotics and Financial Technology. In 2015, Chinese investment in this portfolio of technologies represented approximately 20% of their overall investment, rising to 40% in 2016 and at 29% through the first three quarters of 2017.[21]

- **Artificial Intelligence (AI):** Between 2010-2017, Chinese investors participated in eighty-one AI financings, contributing to the roughly $1.3 billion raised. Participation accelerated in 2014 and has continued through the end of the third quarter of 2017, with Chinese investors active in sixty-nine deals and $1.2 billion in financing.
- **Robotics:** Chinese entities were active in nearly $237 million of financing for Robotics startups between 2010-2017. Deal activity peaked in 2015 with Chinese participation in twelve deals and $113 million in financing.
- **Augmented Reality/Virtual Reality (AR/VR):** Chinese investors participated in $2.1 billion worth of deals during the period 2010-2017. In 2016, China-based investors participated in seventeen deals, contributing to the $1.3 billion in total funding value.
- **Financial Technology (Fintech):** Investments in Fintech, including blockchain technology, continued their rapid pace in 2016 and 2017 with Chinese investors participating in forty-nine deals, valued approximately at $1.4 billion. Overall, Chinese investors have participated in 100 deals, representing $3.5 billion in funding for Fintech companies during 2010-2017.

[20] Seed/Angel stage is typically the first investment in an idea before the idea is proven and often attracts a different class of investors than those who might lead a later stage venture round (typically denoted by a letter such as "A", "B", etc.) leveraging a more proven idea or business model.

[21] Charts of the Chinese investment activity in these four critical technologies are in Appendix 1 and select deals for 2016 are provided in Appendix 2 which illustrates China's technology focus in venture investing.

Two important trends stand out with the new wave of technology being funded. **First, the line demarcating products designed and used for commercial versus military purposes is blurring with these emerging technologies.** For example, VR for gaming is at a similar level of sophistication as the VR used in simulators for our armed forces.[22] Facial recognition and image detection for social networking and online shopping has real application in tracking terrorists or other threats to national security; and much of today's commercial autonomous vehicle technology and drone technology solutions find their genesis in DARPA grants over the last two decades when the Department of Defense sought to develop autonomy for war-fighting purposes.

The current export control regime and the policy apparatus for vetting foreign investment in the U.S.–both of which are designed to keep sensitive technology, companies, and infrastructure out of the hands of our adversaries–are built on a framework of being able to clearly distinguish dual uses of a technology. This distinction becomes difficult when the technology itself is developed for commercial purposes and has widespread potential use as a fundamental technology building block such as artificial intelligence. With the blurring of the line between civilian and military use, faster development cycles and the increasing mobility of human capital globally, our current export control system becomes handicapped as a tool to manage how and where technology transfer occurs.

Second, these technologies – from artificial intelligence to robotics and virtual reality – will be foundational so that many applications or end-use technologies will be built upon them. These foundational technologies will be component technologies for future innovations much the same way that semiconductors have been components in all electronics, telecommunications and computing in the past several decades. This is especially true in the field of artificial intelligence, where the U.S. government is actively making investments to create the third wave of AI technology to achieve a future where machines can explain themselves to humans; where machines can create causal models, not just correlations; and where machines can take what they learn in one domain and apply the learnings to a completely different domain.[23] The breakthroughs that come with these new technologies will be the building blocks for innovations in the decades ahead. There is likely to be an interaction between the new capabilities that are available (through innovations in robotics, artificial intelligence and virtual reality) and new generations of uses, applications and products. The same phenomenon occurred when faster microprocessors, more storage or higher networking bandwidth became available and led to future innovations such as cloud computing, mobile phones and consumer applications for GPS. Consequently, it becomes even more critical that exports, foreign ownership, and technology partnerships with foreign entities do not become conduits for technology transfers that will directly enable key means of foreign military advantage. What is at risk for the U.S. is not only losing an edge in the foundational technology, but also in successive generations of applications and products that the foundational technology enables. According to Adam Segal, a specialist in emerging technologies and national security at the Council on Foreign Relations, "The Chinese leadership is increasingly thinking about how to ensure they are competitive in the next wave of technologies."[24]

[22] Major Loren Bymer, "Virtual Reality Used to Train Soldiers in New Training Simulator," U.S. Army News & Information (August 1, 2012). Retrieved at https://www.army.mil/article/84453

[23] Ed Felton and Terah Lyons, "The Administration's Report on the Future of Artificial Intelligence," White House Blog , October 12, 2016. Retrieved at: https://www.whitehouse.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence

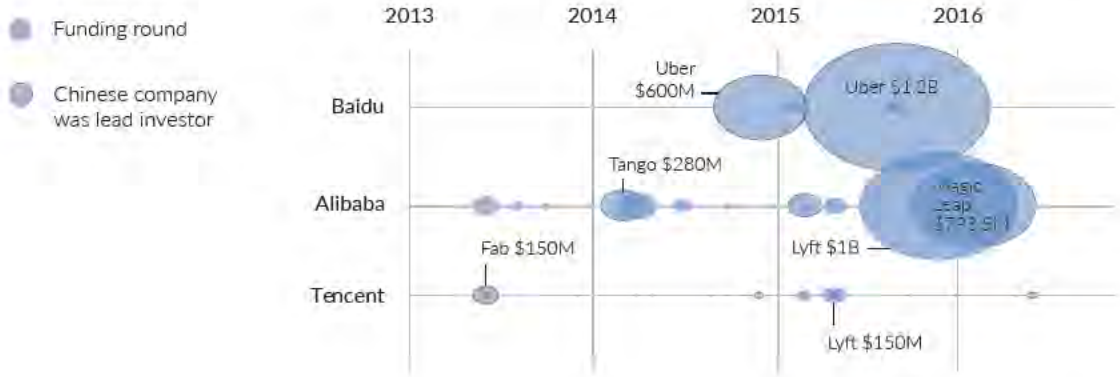
There are multiple ways Chinese invest in U.S. technology firms:

1. **Investments in U.S. venture-backed startups through venture firms.** In the past 10 years, China's investments in U.S. technology firms were limited to joint ventures or acquisitions, but now there are an increasing number of green field investments[25] in venture-backed startups (both as limited partners of U.S. venture firms and through Chinese venture firms) as well as investments through Chinese private equity firms. Examples of Chinese venture firms include West Summit Capital, Westlake Ventures (owned by the Hangzhou government), GGV Capital, GSR Ventures, ZGC Capital, Hax and Sinovation. Sinovation (formerly known as China's Innovation Works) provides a great example of an active Chinese venture firm investing in the U.S.: founded in 2009, it manages three funds of $1.2 billion in capital and has invested in almost 300 startups – including 25 in artificial intelligence. As evidence of its government sponsorship, Sinovation has received awards by China's Ministry of Science & Technology as well as the Municipal Science & Technology Committee of Beijing where the firm is headquartered. (An overview of Sinovation and Hax and their investments are profiled as case studies of Chinese venture capital firms in Appendix 3.) A sample listing of government-backed venture firms and their sources of capital are provided in Appendix 4.

2. **Investments by Chinese companies.** Increasingly, Chinese internet companies such as Baidu, Tencent, Alibaba and JD.com are aggressively investing in venture-backed technology deals. In 2015, these companies participated in 34 deals worth $3.4 billion, up from 7 deals in 2012 worth $355 million.[26] Tencent is by far the most active (with 2x the deals in 2015 than the others combined) having started earlier with its investing but Baidu and Alibaba are not far behind. Some Chinese internet companies are championing investments in specific technologies; Baidu, for example has a clear investment focus in artificial intelligence. The chart that follows shows the growth of investment from 2013 to 2016 from these Chinese internet companies.[27]

China is flooding Silicon Valley with cash

In recent years, Chinese companies have invested heavily in U.S. start-ups. Here are some high-profile deals involving Baidu, Alibaba and Tencent, often referred to as the Google, Amazon and Facebook of China



Source: Crunchbase

Darla Cameron/ The Washington Post

[24] John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race," The New York Times (February 3, 2017). Retrieved at http://www.nytimes.com.

[25] Green field investments typically refer to new investments and sometimes a parent company's operations in a foreign country built from the ground up.

[26] "The Rise of China's Investment in U.S. Tech Startups," CBInsights Blog

[27] Elizabeth Dwoskin, "China Is Flooding Silicon Valley with Cash," Washington Post (August 6, 2016).

3. **Private equity (PE).** Chinese private equity is expanding at an unprecedented pace with the number of globally active funds at 672 (2013-2015), the highest in five years. Total value of Chinese PE deals in 2016 (through June) is at a record $18 billion worldwide. In 2016, Chinese PE firms participated in the $3.6 billion takeover of Lexmark, the $2.75 billion purchase of Dutch chipmaker NXP Semiconductors and the $600 million acquisition of Oslo-based Operat Software's web browser business.[28] Examples of Chinese private equity firms include AGIC, Legend Capital and Golden Brick Capital and these often partner with U.S. private equity firms, such as TPG (involved in acquiring a stake in China International Capital in 2012) and Carlyle (involved in purchase of Focus Media Holding in 2013). One of the most globally active China PE investors is Yunfeng Capital started by Alibaba Group founder Jack Ma.

4. **Special purpose vehicles.** There are also examples of special purpose investment vehicles like Canyon Bridge (Chinese capital and U.S. management expertise combined) which are solely formed to purchase a company and obscure the source of capital for a foreign acquisition, in this case, Lattice Semiconductor. Presumably, a special purpose vehicle is formed to enhance the possibility that the transaction will be approved by CFIUS.

5. **Acquisitions.** Chinese acquisitions continue to increase dramatically with the largest globally being China National Chemical Corporation's proposed takeover of Syngenta (Swiss pesticides) for $43 billion. China's acquisitions of foreign companies are now equal to U.S. firms' acquisitions of foreign companies. In the U.S., the largest recent China-based acquisitions have been the electronics distributor, Ingram Micro ($6.1 billion) and the U.S. hotel owner, Strategic Hotels & Resorts – owners of the Waldorf-Astoria Hotel ($8.1 billion).

As long as U.S. policy supports open investment by all nations, we can expect increased investment from China through a broader number of vehicles, some cleverly designed to obfuscate Chinese capital and ownership. The investment activity *beyond acquisitions* is not tracked by the U.S. government and we have limited visibility into the investors, the technologies invested in, or the increase or decrease of investment flows, except through what is tracked by private data sources. However, even these private data sources are not comprehensively tracked by the U.S. government to assemble a holistic picture of what is happening.

[28] Cathy Chan, "Chinese Private Equity Funds Are Taking on the World's Giants", Bloomberg News (July 20, 2016)

China's Economic and Technology Goals

China has developed a leading global economy faster than any country in modern history. This transformation began with the reform and opening of China's economy under Deng Xiaoping in 1978. By 2015, China's GDP was $11.4 trillion compared to the U.S. at $18 trillion. However, in purchasing power parity (PPP), China is already slightly larger than the U.S. This represents the first time the U.S. has not been the largest economy since it overtook the U.K. in 1872.[29] Since the U.S. economy is growing at 1-3% and China's is growing at 5-7%, the trajectory is clear in narrowing the GDP gap (some projections show China's GDP exceeding U.S. GDP within the next decade)[30]. The time scale during which this growth occurred is stunning as China's economy has grown from 10% of the U.S. economy in the 1970s to the second largest global economy in just fifty years. Analogous growth in the U.S. economy to global leadership took a century to achieve.

China plans to further transform its economy through a national focus on technology and indigenous innovation with a goal of import substitution. To accomplish this, China aims to displace the U.S. in key industries using its large market size to promote domestic champions which can become global leaders through state subsidies, access to low-cost capital and limiting China's domestic market access to foreign companies. China already leads the world in many key industries including overall manufacturing (accounting for almost 25% of global manufacturing in 2012), autos, high-tech products, where China produced 2.5 times the value of goods that the U.S. produced in 2012[31, 32] , and e-commerce[33]. Beijing is home to the most Initial Public Offerings (IPOs) (2x the dollar value of the U.S.) and is the world's largest e-commerce retail market[34]. In fact, China has the potential to lead in all internet-based industries aided by discriminatory domestic policies such as data localization requirements, forced technology transfers and the Great Firewall which enables control over the content and flow of data on the internet. Chinese domestic champions such as Baidu, Tencent and Alibaba enjoy privileged market access in China and are market leaders domestically, while also becoming leading global technology companies.

China's leaders recognize that to achieve its economic goals, the economy must transform even faster in the future than in its recent past. The Chinese government wants to "revitalize the nation through science, technology and innovation."[35] President Xi's strategy is for China to develop its own industries to be leading globally, develop more cyber talent, double down on R&D especially of core ICT technologies and transform China to be a powerhouse of innovation. One area China has targeted for global leadership is the design and production of semiconductors. "China's strategy relies, in particular, on large-scale spending, including $150 billion in public and state-influenced private funds over a 10-year period aimed at subsidizing investment and acquisitions as well as purchasing technology." [36]Several official source documents clearly support these long-term economic and technology goals. (Summary descriptions of three documents are listed here with more documents and descriptions provided in Appendix 5.)

[29] Ben Carter, "Is China's Economy Really the Largest in the World?" BBC News (December 16, 2014)

[30] Malcolm Scott and Cedric Sam, "China and the U.S.: Tale of Two Giant Economies", Bloomberg News (May 12, 2016)

[31] High tech products are defined by the World Bank as products with high R&D intensity such as aerospace, computers, pharmaceuticals, scientific instruments and electrical machinery

[32] Jeff Desjardins, "China vs. United States: A Tale of Two Economies," Visual Capitalist (October 15, 2015)

[33] By 2010, China already led the world in several commodity industries where the US previously led such as steel (with 8x our output), cotton, tobacco, beer, and coal.

[34] E-Marketer.com: "China Eclipses the U.S. to Become the World's Largest e-Commerce Market." Retrieved at https://www.emarketer.com/Article/China-Eclipses-US-Become-Worlds-Largest-Retail-Market/1014364 (August 18, 2016)

- **Made in China 2025** is a plan designed to align State and private efforts to establish China as the world's pre-eminent manufacturing power by 2049 emphasizing the integration of information technology. Key prioritized sectors include advanced information technology, automated machine tools and robotics, aerospace and aeronautical equipment, maritime equipment and high tech shipping and biopharma and advanced medical products.[37]
- **13th Five Year Plan of 2016-2020 "Internet Plus"**[38] which deepens reforms and priorities called for in *Made in China 2025* and emphasizes stronger control by the government over national networks as China continues to control the internet domestically and gains access to global networks by controlling key component and telecommunications technologies. Key aspects include[39]:
  - Focus on catapulting China into a leading position in "advanced industries" including semiconductors, chip materials, robotics, aviation equipment and satellites;
  - Decreasing dependence on imports and innovation;
  - Increasing R&D spending to 2.5% of GDP (up from 2.1% from 2011-2015);
  - Creating a $4.4 billion fund to invest in startups and new technologies
- **China's Mega Project Priorities** are 16 Manhattan-style projects[40] to focus on specific innovations. These areanalogous to what is envisioned by Third Offset capabilities. In China these projects receive a national (not just a military) focus. Here are some selected examples (a complete list is in Appendix 6):
  - Core electronics, high-end general chips, basic software
  - Next generation broadband wireless mobile communications
  - Quantum communications
  - Classified defense-related projects (possibly satellite navigation and inertial confinement fusion)

Today, there are clear examples of Chinese indigenous innovation showing that China is doing more than copying technology – China is making progress on President Xi's goal to become one of the most innovative economies by 2020:

- **Micius Quantum Communications Satellite.** The 2016 launch of the Micius satellite suggests an aggressive push into quantum communications; expertise in quantum computing may someday enable the capability to break many existing encryption methods (based on factoring).
- **Sunway TaihuLight Supercomputer.** In June of 2016, China introduced the world's fastest supercomputer, the Sunway TaihuLight capable of theoretical peak performance of 124.5 petaflops. The TaihuLight is the first system in the world to exceed 100 petaflops (quadrillions of floating-point operations per second). More importantly, the previous version of this Chinese supercomputer used Intel microprocessors but the Sunway TaihuLight uses Chinese designed and manufactured microprocessors.[41]

[35] "Xi Sets Targets for China's Science, Technology Mastery" Xinhua (May 30, 2016).

[36]"Ensuring Long Term U.S. Leadership in Semiconductors," Executive Office of the President, President's Council of Advisors on Science & Technology, January, 2017. Retrieved at http://www.whitehouse.gov/ostp/pcast

[37]Scott Kennedy, "Critical Questions: Made in China 2025," Center for Strategic and International Studies" November 7, 2016. Retrieved at http://www.csis.org/analysis/made-china-2025.

[38]"China Unveils Internet Plus Action Plan to Fuel Growth," The State Council for the People's Republic of China. Xinhua (July 4, 2015) Retrieved at http://www.english.gov.cn/policies

[39]Lulu Chang, "China Outlines its Latest FYP Called Internet Plus," Digital Trends (March 6, 2016). Retrieved at http://www.digitaltrends.com.

[40]Michael Raska, "Scientific Innovation and China's Military Modernization," The Diplomat (September 3, 2013), Retrieved at http://www.thediplomat.com

[41] Patrick Thibodeau, "China Builds World's Fastest Supercomputer without U.S. Chips," Computerworld (June 20, 2016), Retreived at http://www.computerworld.com

- **Cruise Missile Incorporating Artificial Intelligence.** A cruise missile system with a high-level of artificial intelligence: a "semi-autonomous" weapon having the capability to avoid defenses and make final targeting decisions with a goal of destroying larger ships in a fleet like aircraft carriers.[42]
- **Consumer Drones.** DJI's (Da-Jiang Innovation) market leadership in low-cost, easy-to-fly drones and aerial photography systems which have made this company the standard in consumer drone technology accounting for 70% of the worldwide drone market.
- **Autos.** In the auto industry, China plans to take advantage of two paradigm shifts to further its lead in the world's largest manufacturing industry: autonomous vehicles and electric vehicles. China is investing in an electric vehicle supply chain including battery technology and aims to have 50% of the world's electric vehicle production and 90% of global battery production capacity.[43]

According to Tangent Link, a U.K.-based provider of defense reports, "one of the enduring myths in many Western CEO-suites is that the Chinese are great at copying and stealing, but will have difficulty 'out-inventing' the West. This arrogant and outdated hypothesis is crumbling fast."[44]

By some measures of innovation, China is already leading and without question China's capacity to innovate is rising:

- In patent applications, China already surpasses the U.S. with over 1 million patent applications received by the China State Intellectual Property Office in 2015 (up 19% year over year) compared to 589,410 patent applications received by the U.S. Patent and Trademark Office (up 2% year over year).[45]
- In academic research papers, Chinese authorship of articles in peer-reviewed international science journals increased such that China is now in 2nd place (2011) up from 13th place just a few years earlier.[46]
- China spent 1.6% of GDP in R&D in 2011 but has a stated goal of spending 2.5% of GDP R&D by 2020 – about $350 billion.[47] Combined U.S. business and federal government R&D spending is 3-4% of GDP.
- China awarded 1,288,999 Science, Technology, Engineering & Mathematics (STEM) degrees in 2014 – more than double the degrees the U.S. awarded at 525,374 degrees.[48]

To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed the industries where China has an innovation lead.[49] In traditional manufacturing industries where low costs provide a competitive advantage, China leads in innovation by leveraging a concentrated supply base and expertise in automation and modular design (examples: electronics, solar panels, construction equipment). In consumer markets, China leads given its market size (examples: smartphones, household appliances). In engineering markets, China has

42 John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race," The New York Times (February 3, 2017); and Lei Zhao, "Nation's next generation of missiles to be highly flexible," China Daily (August 19, 2016)

43 John Longhurst, "Car Wars: Beijing's Winning Plan" November, 2016.

44 "Quantum Leap: Who Said China Couldn't Invent?" Geo-political Standpoint (GPS) Report 85 (October 14, 2016), Tangent Link

45 "China vs. U.S. Patent Trends: How Do the Giants Stack Up?", Technology & Patent Research. Retrieved at http://www.tprinternational.com

46 Hannas, William C.; Mulvenon, James and Puglisi, Anna B. China Industrial Espionage. New York: Routledge, 2013. Chapter 3

47 Hannas, China Industrial Espionage, Chapter 3 and "The U.S. Leads the World in R&D Spending", The Capital Group Companies (May 9, 2016). Retrieved at http://www.thecapitalideas.com

48 Jackie Kraemer and Jennifer Craw, "Statistic of the Month: Engineering and Science Degree Attainment by Country", National Center on Education and the Economy (May 27, 2016). Retrieved at http://www.ncee.org

49 Erik Roth, Jeongmin Seong, Jonathan Woetzel, "Gauging the Strength of Chinese Innovation," McKinsey Quarterly (October, 2015).

mixed results leading in high-speed rail but not in aerospace, nuclear power or medical equipment. In science-based industries such as branded pharmaceuticals or satellites, China is behind the U.S. but China is investing billions of dollars to catch up. (The McKinsey analysis is provided in Appendix 7.)

Many of the critical future technologies attracting venture focus today such as artificial intelligence, augmented reality and autonomous vehicles are likely to have large consumer-based markets implying that China will apply its advantages both in efficiency-driven and customer-focused industries to these new technologies with the potential to *lead in innovation* and *be global market share leaders.* The success of DJI in the consumer drone market with 70% worldwide share is consistent with this McKinsey analysis. In artificial intelligence, the race between the U.S. and China is so close that whether the Chinese "will quickly catch the U.S...is a matter of intense discussion and disagreement in the U.S. Andrew Ng, chief scientist at Baidu, said the U.S. may be too myopic and self-confident to understand the speed of the Chinese competition."[50] And in the field of advanced industrial robotics, China is leveraging its market and investment capital to ultimately lead in the design and manufacture of robots.[51] Given there are many industries where China already leads the world in innovation and given China's massive scale and national focus on science and technology advancement, it would be foolhardy to bet against China's continued progress even in the areas where they do not lead today. A further concern is that China's long-term, national focus on innovation and expertise in advanced manufacturing might make China a more attractive destination market for new technologies--especially hardware technologies--since there is both less funding appetite in the U.S. for non-software technologies and less of an ecosystem for developing and manufacturing these technologies.

Implications for the Department of Defense (DoD)

U.S. military superiority since World War II has relied on both U.S. economic scale and technological superiority. The size of the U.S. economy allows DoD to spend $600 billion per year (while remaining only 3% of GDP in 2016) which equals the defense spending of the next eight largest nations combined. In 2016, China was the second largest spender at $215 billion, up 47% from the previous year while the U.S. spending remained flat.[52] U.S. technological preeminence enabled the series of offset strategies which included the First and Second Offsets and now DoD is currently working to maintain technology superiority in its Third Offset strategy.

China's goal to be the preeminent global economy combined with its emphasis on technology transfer and innovation constitutes a major strategic competition with the U.S. There are several areas of concern:

1. China's transformation to be the manufacturer for the world means more supply chains are owned by China, which creates risks to U.S. military technology and operations. For example, the Aviation Industry Corporation of China (AVIC) is a Chinese-state owned aerospace and defense company which has now procured key

[50] John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race." The New York Times (February 3, 2017).

[51] Farhad Manjoo, "Make Robots Great Again," The New York Times (January 26, 2017).

[52] 2016 Fact Sheet, Stockholm International Peace Research Institute (SIPR) and "The Military Balance", International Institute for Strategic Studies (IISS) 2016. Retrieved at http://www.en.m.wikipedia.org

components of the U.S. military aircraft supply chain.[53] Additionally, as the U.S.-based semiconductor industry focuses on high-end designs and moves older, low-end designs offshore, the Chinese semiconductor industry now controls a significant percentage of the supply of older chips used in maintaining U.S. military aircraft and equipment designed 40 years ago and still in service.

2. China has targeted several key technologies such as jet engine design which will reduce current U.S. military superiority and is actively working to acquire companies that will close this gap.
3. China's industrial espionage and cyber theft efforts continue without adequate U.S. investment in manpower and programs to thwart these efforts. This allows technology transfer at an alarming rate.[54]
4. China's investment strategy (through venture and private equity investments as well as acquisitions) includes the fundamental technologies which will likely be the sources of innovation for the next several decades: artificial intelligence, autonomous vehicles, robotics, augmented and virtual reality, gene editing, etc. As a result, China has access to U.S.-based innovation in the same areas and at the same time which could negate advantages for the U.S. Further, when the Chinese make an investment in an early stage company developing advanced technology, there is an opportunity cost to the U.S. since that company is potentially off-limits for purposes of working with DoD.
5. Beyond the threat from investments alone, China's national focus on mega projects (analogous to the U.S. space program in the 1960s to not only develop technology but create demand for technology) complements the increase in military spending as China gains experience in manufacturing and refining new technologies for practical use.
6. DoD does not currently have agreed-upon emerging technologies the U.S. must protect although there has been extensive work on export controls to protect technology products from being shipped to U.S. adversaries.

DoD began developing a list of critical technologies in 2016 in an effort known as the Joint Acquisition Protection & Exploitation Cell (JAPEC). The mission of JAPEC is to "integrate protection efforts across the Department to proactively mitigate losses and exploit opportunities to deter and disrupt adversaries which threaten U.S. military advantage." JAPEC is working to identify critical acquisition programs and technologies that require protection as well as assess vulnerabilities associated with known losses and implement advanced protection mechanisms.[55] However, there is much work left to do to consolidate the technologies across DoD requiring protection and determine which of those are the most critical. The JAPEC effort complements the government's robust system of export controls which are designed to comply with trade agreements, embargoes, sanctions and other political measures to meet U.S. national security and foreign policy objectives.

Finally, there is no technology landscape map to help DoD understand the fundamental component technologies required to protect applications or end-use technologies embedded in acquisition programs. For example, semiconductor technology is a fundamental component technology today that would be required to protect capabilities inherent in almost all acquisition programs. This is likely to be the case in the future with such fundamental technologies as artificial intelligence, robotics, autonomous vehicles, advanced materials science, etc. With agreed-upon emerging technologies to protect and a technology landscape to clarify the value-added map of technologies (from components to end-use applications), the U.S. government can be much clearer about what acquisitions to deny through a reformed CFIUS process and resource allocation to thwart industrial espionage or cyber theft.

[53] "How America's Giants Are Aiding China's Rise", Geo-political Standpoint (GPS) Report 84, October 13, 2016, Tangent Link.

[54] The IP Commission Report (2013)

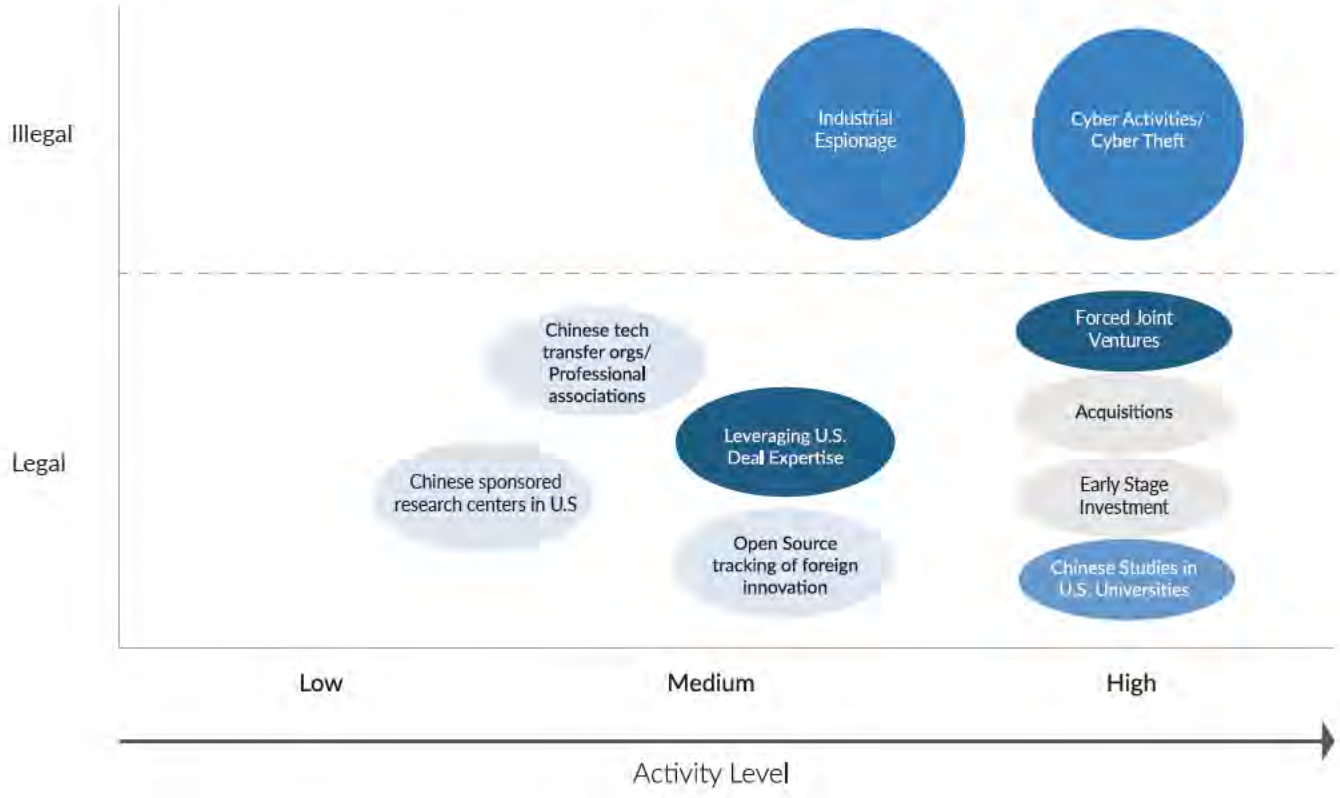
[55] Brian D. Hughes, "Protecting U.S. Military's Technical Advantage" presented at the 18th Annual NDIA Systems Engineering Conference in Springfield, VA, October 28, 2015. Retrieved at http://www.acq.osd.mil

China's Multiple Vehicles for Technology Transfer

Given the authoritarian nature of China's government, China can focus resources from a variety of different sources to enable a broad transfer of scientific knowledge and technology. Additionally, China coordinates these different sources to achieve a larger impact through a well-articulated industrial policy documented in its Five-Year and other plans. The principal vehicles discussed so far are investments in early-stage technologies as well as acquisitions. When viewed individually, some of these practices may seem commonplace and not unlike those employed by other countries. However, when viewed in combination, and with the resources China is applying, the **composite picture illustrates the intent, design and dedication of a regime focused on technology transfer at a massive scale.**

The following table compares these transfer vehicles on a relative scale of the level of activity for China in the U.S. compared to other countries. This illustrates that what differentiates China from other countries' activities in the U.S. is the scale of China's efforts. Naturally, the most troublesome of all the vehicles are the illegal ones – the outright theft of technology and intellectual property which is very cost-effective for China.

Vehicles for Chinese Technology Transfer from the U.S.



China's Activity in the U.S. Relative to Other Countries' Activities in the U.S.

The 8 principal sources and methods for technology transfer i*n addition to investments and acquisitions* are:

1. **Industrial espionage**

   For years, the Chinese have been engaged in a sophisticated industrial espionage program targeting key technologies and intellectual property to enhance commercial enterprises and support domestic champions.[56] This has recently been on the rise as Randall Coleman, Assistant Director of the FBI's Counterintelligence Division, observed in 2015 that espionage caseloads are up 53% in the past two years and that in an FBI survey of 165 companies, 95% of those companies cite China as the perpetrator. "China's intelligence services are as aggressive now as they've ever been" underscoring the pervasive nature of intellectual property and trade secret theft.[57] The FBI reports that China pays Chinese nationals to seek employment in targeted U.S. technology firms (where there is sensitive technology that China identifies it needs) where they become "insiders" and more readily exfiltrate valuable intellectual property. Fortunately, convictions of Chinese nationals and naturalized citizens for industrial espionage are also on the rise, up 10x since 1985[58].

   Despite the rise in convictions, there is no way to know how big this problem really is. The scale of the espionage (through some of the methods described below) continues to increase and it would be difficult to quantify this problem without more resources applied by both the FBI and the Defense Department's various counterintelligence agencies.

2. **Cyber theft**

   China's cyber capabilities are among the strongest in the world probably only exceeded by Russia and the U.S. although some have argued that China's cyber successes to date demonstrate more about U.S. system vulnerability than Chinese capabilities. Regardless, cyber theft is an ideal tool for China given the asymmetric vulnerability of the U.S. (given how much information is digitally accessible) and the plausible deniability given the difficulty of attribution in cyber-attacks. Several documented high profile cyber theft incidents are described in Appendix 8 and may be the tip of the iceberg in terms of the numbers of incidents and their scale. As former NSA Director General Keith Alexander famously told Congress in 2012, this represents the "greatest transfer of wealth in history". At that time, it was estimated that U.S. companies lose $250 billion per year through intellectual property theft and another $114 billion due to cybercrime, totaling $338 billion of impact each year. "That's our future disappearing in front of us," warned General Alexander.[59]

   As reported in the IP Commission Report of 2013, Verizon worked with 18 private institutions and government agencies to estimate that:

   - 96% of the world's cyber espionage originated in China;
   - $100 billion in lost sales and 2.1 million in lost jobs result from this theft;
   - $300 billion worth of intellectual property is stolen each year.[60]

[56] 2016 Report to Congress of the US-China Economic & Security Review Commission (November, 2016) and Hannas, China Industrial Espionage, Chapter 8

[57] Shanie Harris, "FBI Probes 'Hundreds' of China Spy Cases", The Daily Beast (July 23, 2015). Retrieved at http://www.thedailybeast.com

[58] Notes from briefing, "Economic and S&T Intelligence Collection" by Joseph P. O'Neill, Faculty Member, National Intelligence University, November 28, 2016.

[59] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' " Foreign Policy Magazine (July, 2012). Retrieved at http://www.foreignpolicy.com

[60] The IP Commission Report (2013)

What really distinguishes China from other nation-state actors in cyber attacks is the sheer scale of activity as China dedicates a massive amount of manpower to its global cyber activities. The FBI's former deputy director for counterintelligence reported in 2010 that the China deploys between 250,000 and 300,000 soldiers in the People's Liberation Army (3PLA) dedicated to cyber espionage. Within another part of the armed forces, 2PLA has between 30,000 and 50,000 human spies working on insider operations.[61] China's cyber activity is not solely focused on a national security agenda. In fact, much of this activity can be deployed to support China's economic goals in stealing valuable intellectual property to support China's technology transfer. Additionally, China recently passed two laws--the anti-terrorism law and the cybersecurity law--which are of concern since they could be used to gather sensitive commercial information from U.S. companies legally.[62]

3. Academia

For many years, China has sent an increasing number of students to the U.S. In 2016, there were 328,000 Chinese foreign nationals studying at U.S. colleges and universities (⅓ of all foreign students). Chinese foreign nationals represent ½ of all foreign applicants.[63] The U.S. educational system has come to rely on the financial contribution of these foreign students especially at the undergraduate level.

Statistics on U.S. STEM programs highlight the large proportion of foreign students:

- 84% of foreign students in PhD programs were studying in science and engineering (2001-2011);64
- For doctoral programs, 57% of engineering, 53% of computer science and 50% of math and statistics candidates were foreign; half of these were Chinese;[65]
- 54% of patents issued by universities include foreign student's work;[66]
- 45% of STEM undergraduates are foreign and ⅓ of these are from China.[67]

From this data, we can infer that 25% of the graduate students in STEM fields are Chinese foreign nationals. Since these graduates do not have visas to remain in the U.S., nearly all will take their knowledge and skills back to China. Academia is an opportune environment for learning about science and technology since the cultural values of U.S. educational institutions reflect an open and free exchange of ideas. As a result, Chinese science and engineering students frequently master technologies that later become critical to key military systems, amounting over time to unintentional violations of U.S. export control laws. The phenomena of graduate student

[61] Joshua Philipp, "Rash of China Spy Cases Shows a Silent National Emergency", The Epoch Times (April 25, 2016). Retrieved at http://www.theepochtimes.com

[62] **Anti-terrorism law** passed in December, 2015 which gives the Chinese government broad access to technical information and decryption codes when state security agents demand it for investigating or preventing terrorism. Telecommunication and internet service providers "shall provide technical interfaces, decryption and other technical support and assistance" when required. Chris Buckley, "China Passes Antiterrorism Law that Critics Fear May Overreach," The New York Times (January 6, 2016). Retrieved at http://www.nytimes.com.

Cybersecurity law passed in November, 2016 contains vague language aimed at preventing network intrusions that would require U.S. companies submit their technology, possibly including source code, to security reviews with Chinese officials. There are an expansive list of sectors defined as part of China's critical information infrastructure such as telecommunications, energy, transportation, information services and finance all of which would be subject to security reviews. The law does not specify what a security review will entail. Several U.S. companies are concerned about the increased costs of doing business in China as well as the need to provide company sensitive information to the Cybersecurity Administration of China to prove that their equipment, software and operations are safe. Josh Chin and Eva Dou, "China's New Cybersecurity Law Rattles Foreign Tech Firms," Wall Street Journal (November 7, 2016). Retrieved at http://www.wsj.com.

[63] Project Atlas, Institute of International Education, Fall 2015. Retrieved at http://www.iee.org.

[64] "Survey of Graduate Students and Postdoctorates in Science & Engineering", National Science Foundation, November, 2015.

[65] Drew Desilver, "Growth from Asia Drives Surge in US Foreign Students," Pew Research Center (June 18, 2015)

[66] National Science Foundation Survey, November, 2015

[67] Donisha Adams and Rachel Bernstein, Science (November 21, 2014); Retrieved at http://www.sciencemag.org

research increasingly having national security implications will inevitably increase as the distinction between military and civilian technology blurs. Further, since there are close ties between academia and U.S. government-sponsored research – including at our national laboratories – ensuring that foreign nationals are not working on sensitive research paid for by the U.S. government (including DoD) will become increasingly important.

Chinese companies are also approaching U.S. academic institutions to promote joint research and attract future talent. As an example, Huawei has partnered with UC-Berkeley to focus jointly on artificial intelligence research. Huawei made an initial commitment of $1 million in funding to cover areas such as deep learning, reinforcement learning, machine learning, natural language processing and computer vision[68] More recently, Huawei has approached MIT with an offer for a grant to build a joint research facility.

4. China's use of open sources tracking foreign innovation

China has made collecting and distributing science and technology information a national priority for decades. "By 1985, there were 412 major science & technology intelligence institutes nationwide [in China]…employing …60,000 workers…investigating, collecting, analyzing, synthesizing, repackaging, benchmarking and reverse engineering."69 In 1991, the book, Sources and Methods of Obtaining National Defense Science & Technology Intelligence, detailed a comprehensive account of China's foreign military open-source collection (known as "China's Spy Guide") collecting all types of media (including verbal information prized for its timeliness over written information) and making them available in database form. The National Internet-based Science & Technology Information Service Systems (NISS) makes 26 million holdings of foreign journals, patents and reports available to the public around the clock. Chinese exploitation of foreign open-source science and technology information is a systematic and scale operation making maximum use of diversified sources: scanning technical literature, analyzing patents, reverse engineering product samples and capturing conversations at scientific meetings. This circumvents the cost and risk of indigenous research.[70]

5. Chinese-based technology transfer organizations

At the national level, China has more than a dozen organizations that seek to access foreign technologies and the scientists who develop them (not counting the clandestine services, open-sources, and procurement offices). These organizations are led by the State Administration of Foreign Experts Affairs (SAFEA). SAFEA's success is evident in the 440,000 foreign experts working in China annually. Complementing SAFEA is the State Council's Overseas Chinese Affairs Office (OCAO) which provides overseas Chinese (whether they have lived in China or not) with the opportunity to support their ancestral country. The Ministry of Human Resources and Social Security[71] is involved heavily in foreign recruitment and foreign technology transfer including the Overseas Scholars and Experts Service Center to interact with Chinese students studying abroad. The Ministry of Science & Technology (MOST) also dedicates significant resources to acquiring foreign technology including 135 declared personnel in overseas embassies and consulates.

[68] Li Yuan, "Chinese Technology Companies, including Baidu, Invest Heavily in AI Efforts", Bloomberg News (August 24, 2016)

[69] Hannas, China Industrial Espionage, Chapter 2, p. 22.

[70] Hannas, China Industrial Espionage, Chapter 2

[71] Formerly known as the Ministry of Personnel.

The Overseas Scholars and Experts Service Center sponsors associations at many universities which serve as an organized means to transfer technology to China. Many of the national programs also have complementary provincial and municipal organizations specifically focused on the skills and talent than can benefit a local area. These organizations make available debriefing rooms, free translators, personnel to make travel arrangements, dedicated "transfer centers" and face-to-face meetings between technology experts and Chinese company representatives.

China also promotes "people to people" exchanges through a network of NGOs (e.g., the China Science and Technology Exchange Center and the China Association for the International Exchange of Personnel) that insulate overseas specialists from the potential risks of sharing technology directly with PRC government officials.[72]

6. **Chinese research centers in the U.S. to access talent and knowledge**

There are now increasing examples of Chinese firms setting up research centers to access U.S. talent and technology:

- In 2013, Baidu set up the Institute for Deep Learning in Silicon Valley to compete with Google, Apple, Facebook and others for talent in the artificial intelligence field.[73] Baidu recently hired former Microsoft executive Qi Lu as its group president and chief operating officer. Lu was the architect of Microsoft's strategy for artificial intelligence and bots.
- Another example is the Zhong Guan Cun (ZGC) Innovation Center opened in May, 2016 in Silicon Valley.
- A new type of research center is TechCode: an entrepreneurs' network "committed to breaking down geographic barriers and eliminating potential inequalities of international cooperation" according to its website. As a network of entrepreneurs, Tech Code is a system of incubators ("startups without borders") worldwide (Beijing, Shanghai, Shenzhen, Gu'an, Silicon Valley, Seoul, Tel Aviv and Berlin) that leverages an online development platform for projects focused on China's development and funded by the Chinese government.[74]
- In addition, there are several research centers promoting a sustainable environment and clean energy including the U.S.-China Clean Energy Research Center (CERC) recently expanded and promoted together by President Obama and President Xi.

7. **U.S.-based associations sponsored by the Chinese government**

There are many professional associations which bring Chinese engineers together such as the Silicon Valley Chinese Engineers (6000 members), the Hua Yuan Science & Technology Association (HYSTA) and the Chinese Association for Science and Technology (CAST). The largest concentration of China's science and technology advocacy groups in the U.S. are in California and Silicon Valley in particular. " 'The Valley' is ground [zero] for… legal, illegal and quasi-legal practices that fall just below the thresholds set by U.S. law."[75] With these professional associations being one of the primary targets, the Chinese have implemented a variety of programs such as the "Thousand Talents Program" to bring this technology home by recruiting Chinese engineers with offers of career

[72] Hannas, China Industrial Espionage, Chapter 4

[73] Li Yuan, "China Races to Tap Artificial Intelligence", Wall Street Journal (August 24, 2016)

[74] "Startups Nation" from the Tech Code website, http://www.techcode.com

[75] Hannas, China Industrial Espionage, Chapter 5, p. 122

advancement, increased compensation, the opportunity do basic research or to lead their own development labs in China. China set a goal of bringing back 500,000 Chinese overseas students and scholars from abroad by 2015.[76] Another example is "Spring Light" which pays overseas Chinese scientists and engineers to return home for short periods of lucrative service that may include teaching, academic exchanges, or working in government-sponsored labs. In addition, "Spring Light" includes a global database of Chinese scholars to match specific technology needs to pools of overseas talent.[77]

The Chinese diplomatic missions to the U.S. directly support technology transfer as embassy or consulate officials facilitate a wide variety of venues and forums supported by U.S. investors and local governments to promote Chinese investment. Seven examples of these are (descriptions of these forums are in Appendix 9):

- Silicon Valley Innovation and Entrepreneurship Forum (SVIEF)
- DEMO China
- Silicon Valley-China Future Forum
- China Silicon Valley
- The Global Chamber San Francisco (GCSF)
- U.S.-China VC Summit & Startup Expo
- Chinese American Semiconductor Professionals Association (CASPA)

The messaging for these associations and programs is often controlled by the "United Front" which is a propaganda arm for the Chinese government to promote a positive image of China and Chinese culture around the world.[78]

8. **Leveraging technical expertise of U.S. private equity, venture firms, investment banks and law firms**
As China has invested more in the U.S., its investment entities have enhanced their deal expertise by working with U.S. investment banks or law firms who benefit from increased business. As China works with U.S. private equity and venture firms to invest in deals, these firms benefit through the increased value of equity stakes in these investments. Many U.S. law firms have built a practice in advising Chinese companies on how to structure deals to increase the likelihood of CFIUS approval for transactions. Consulting organizations have also built a practice in structuring mitigation agreements that will be more likely to gain CFIUS approval. As China's investments have ramped up dramatically in the past three years, the level of deal expertise has increased considerably.

[76] Xu Liyan and Qiu Jing, "Beyond Factory Floor: China's Plan to Nurture Talent," Yale Global Online (September 10, 2012). Retrieved at http://yaleglobal.yale.edu/content/beyond-factory-floor-chinas-plan-nurture-talent

[77] Hannas, China Industrial Espionage, Chapter 5.

[78] The Confucius Institutes, launched in 2004, are a good example which offer Chinese language and cultural instruction often in partnership with local universities. However, their purpose is also to portray Chinese history and policy in the best possible light so that China can be seen as a "pacifistic, happy nation. In the past decade, these institutes have been welcomed on some 350 college campuses across the world including Stanford, Columbia and Penn." as quoted in Pillsbury's The Hundred-Year Marathon. Given a history of trying to influence the curriculum of Chinese history and Chinese studies at colleges, there are now a number of colleges which are disbanding these institutes.

How are these multiple vehicles used together for coordinated impact?

Because the Chinese Communist Party is much more involved in planning economic activity and supporting companies (not only through state-owned-enterprises but also in favoring national champions it supports globally like Huawei), there is a great deal more coordination of investment along with other vehicles of technology transfer to accomplish the larger economic goals specified in China's documented plans. The scale of the Chinese economy is so large that not everything is coordinated centrally; however, the importance and degree of political control by the Communist Party ensures that investments support national goals and are not purely guided by commercial interest. The goals of many of the government-funded Chinese venture capital firms are focused on experience with advanced technologies and recruiting talent – not simply making money.

There are not enough examples to definitively say there is a standard playbook of all the vehicles used in combination. However, there are a few examples where several of these technology transfer vehicles are used together. Documented examples show targeted cyber-attacks to understand the scope of technology and intellectual property of value and where that resides within a company followed by cyber theft or industrial espionage to steal that technology.[79] In another example, Chinese cyber attackers manipulated company sales figures to weaken that company's view of itself and make it more likely to accept a purchase offer from a Chinese company. In a variation on this theme, a Chinese customer placed large orders with a public company and then cancelled them to weaken a company's results as a market surprise. Finally, there is the example of Silicon Valley startup, Quixey, who relied on a large investor, Alibaba, as one of its most important customers promising access to the Chinese market. However, Alibaba refused to pay Quixey for a custom contract to provide specialized technology to search within apps in Alibaba's operating system. Alibaba subsequently took advantage of Quixey's cash squeeze to negotiate favorable financing terms which put Alibaba in a better position to later make an offer for the technology or the company.[80] Thus, through a combination of technology transfer vehicles, China can achieve more than with a single vehicle.

Before the U.S.-China Economic and Security Review Commission, a former forensic auditor and counterintelligence analyst testified that China is executing a series of campaigns targeting specific industries he studied including telecommunications and network equipment (to benefit global champions Huawei and ZTE), information security, semiconductors, media and entertainment and financial technology. He outlined a process that involves many of the vehicles described here as key technologies are targeted, studied, stolen and applied within Chinese companies. He characterized these as cyber-economic campaigns which "are persistent, intense, patiently executed and include the simultaneous execution of such a large and diverse set of legal and illegal methods, individuals and organizations, there's little chance the targeted U.S. competitors can effectively defend or compete in the future without significant support of the U.S. government." [81]

[79] "APT1: Exposing One of China's Cyber Espionage Units", Mandiant Report, 2013. Retrieved at http://www.fireeye.com/content/dam/fireeye-www.services/pdfs

[80] Elizabeth Dwoskin, "China Is Flooding Silicon Valley with Cash," Washington Post (August 6, 2016).

[81] Jeffrey Z. Johnson, President & CEO of SquirrelWerkz, in testimony before the US-China Economic and Security Review Commission, January 26, 2017.

U.S. Government Tools to Thwart Technology Transfer

1. **The Committee on Foreign Investment in the U.S. (CFIUS) is one of the only tools in place today to govern foreign investments that could be used to transfer sensitive technology to adversaries, but it was not designed for this purpose and is only partially effective.**[82] CFIUS was established by statute in the Foreign Investment and National Security Act of 2007 (FINSA) which formally gave an interagency working group the power to review national security implications of foreign investments in U.S. companies or operations. The Treasury Department is the lead agency among 14 participating agencies. The nine voting member agencies are Treasury, State, Commerce, the United States Trade Representative, Office of Science & Technology Policy, Defense, Homeland Security, Justice and Energy. While transaction reporting is voluntary, CFIUS can and does monitor transactions beyond those that are voluntarily submitted and can initiate a review of any of these. CFIUS is required to provide clearance for reviewed transactions on a short timeline: within 75 days unless a Presidential review is required and, in that case, there are 90 days for a review and a Presidential recommendation.

   As those involved in the CFIUS process readily acknowledge, CFIUS is a blunt tool not designed for the purpose of slowing technology transfer. CFIUS only reviews some of the relevant transactions because transactions that do not result in a foreign controlling interest are beyond its jurisdiction. There are many transaction types such as joint ventures, minority investments and purchased assets from bankruptcies that are effective for transferring technology but do not result in foreign control of a U.S. entity and are, therefore, outside of CFIUS' jurisdiction In 2017, Senators Cornyn (R-TX) and Feinstein (D-CA) introduced the Foreign Investment Risk Review Modernization Act (FIRRMA) which expands CFIUS' jurisdiction to cover the key transaction types beyond acquisition which might result in technology transfer. This legislation has broad support within the Administration including public statements by the White House, Secretaries of Defense, Treasury, Commerce and the Attorney General.

   The workload for CFIUS is increasing rapidly. CFIUS reviews about 150 transactions per year but this is rising. At the same time, the number of transactions which have national security implications is also rising as Chinese purchases of U.S.-based companies or assets now represent the largest number of CFIUS reviews. Congress has not provided dedicated funding for CFIUS reviews so this critical process must be handled within existing agency budgets. The proposed FIRRMA legislation recognizes the need for increased resources to handle a growing CFIUS caseload. A review of strengths and weaknesses of the current CFIUS process are included as Appendix 10.

[82] CFIUS was established by executive order in 1975 during the OPEC oil embargo of the 1970s to prevent oil-rich nations with greatly expanding wealth from gaining too much control of U.S. assets.

2. **Export controls** are designed to prevent sensitive technologies or products from being shipped to adversaries.[83] In practice, there are several problems that may result from using export controls to thwart technology transfer to an adversary. First, export controls are often backward-looking in terms of specifying the technologies that are critical since most controls focus on products rather than broad technologies. Second, there is diffused responsibility for export controls since some are controlled by the State Department and some by the Commerce Department with DoD in an advisory role.[84] Third, with the technologies that are the focus of venture investing (far in advance of any specific products produced or military weapons), export controls have not been traditionally effective. Failure in effectiveness has largely been a function of not having the foresight to place these technologies on an export control list nor the political will to do so. In other words, the authority is in place for effective export controls if there is agreement among DoD, State and Commerce about what technologies to protect. However, since complying with export controls is a company's responsibility, there is a question of whether early-stage technology companies understand the controls or have resources within a trade compliance function to handle this complexity.

   While the restricted export lists (EAR and CCL76) can accommodate the regulation of software-based technologies such as artificial intelligence, controlling a broad technology will be highly controversial within the venture and technology community where the largest markets are for benign, commercial purposes. In fact, there is great pressure to specify technologies as narrowly as possible when writing export controls to facilitate more U.S. exports especially if the technologies are available outside the U.S. As the venture investment data indicates, the regulations do not prevent (or even deter) foreign investment in seed or early-stage companies. Additionally, it is not the purview of the export control enforcement authorities to proactively seek out companies developing new technologies or to investigate the relationship between investors and employees of a startup. Lastly, export controls will be much more effective if there is an international effort to protect the technology; otherwise, there may be an unintended consequence of the technology developing faster outside the U.S. aided by foreign investment through an allied country. If and when a dual-use technology is deemed worthy of control, the U.S. government can impose unilateral controls while it undertakes an effort to have the technology controlled internationally through the multilateral export control regimes but this process can take up to three years and may not be successful.

3. **VISAs** for Chinese foreign national students studying in the U.S. are controlled by the State Department and not scrutinized for fields of study with the protection of critical technologies in mind.

[83] The current U.S. export control system is based on the requirements of the Export Administration Act, the International Economic Powers Enhancement Act (IEEPA), the Arms Export Control Act (AECA) and the resulting implementing regulations (most notably, Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR)). The EAR and ITAR each have a control list: the Commerce Control List (CCL) and the U.S. Munitions List (USML). Several other Federal Agencies have niche export control regulations such as the Department of Energy, the Food and Drug Administration and the National Nuclear Security Administration, among others. The CCL lists certain dual-use, fully commercial, and less sensitive military items while items that are considered defense articles and services are included in the USML. USML is a list of articles and/or services that are specifically designed, developed, configured, adapted or modified for a military application and do not have a predominant civil application or civil performance equivalent; have significant military or intelligence applicability; and are determined or may be determined as a defense article or defense service. Taking a closer look at the dual-use paradigm, the CCL enumerates dual-use, commercial, and less sensitive military goods, software, and technology in categories ranging from materials processing, electronics, sensors and lasers, to navigation and avionics. Each item has an Export Control Classification Number ("ECCN") that specifies characteristics and capabilities of the items controlled in each ECCN. The definition of an export is intentionally broad and includes the provision of technical information to a foreign national anywhere in the world.

[84] Previous attempts at consolidating the organizational responsibility for export controls to a single government department focused on controlling a single list have not been implemented.

Policy Framework

Given the multi-faceted nature of this problem which cuts across not only many parts of the executive branch of government but also private sector businesses and academia, there are multiple dimensions of a policy framework:

1. **Defensive policies: how to deter the technology transfer occurring.** The primary defensive levers are:
    a. CFIUS reforms
    b. Export controls
    c. Immigration policy for foreign students
    d. Level of counterintelligence resources

2. **Proactive policies: how to stimulate technology development and innovation in the economy.** Levers are:
    a. Level of basic research investment
    b. Incentives for encouraging U.S. students to study STEM fields
    c. Pro-growth and productivity enhancing economic policies

3. **Whole of Government scope:** actions or policies that require a coordinated strategy and multiple agencies/ departments working together. If there is agreement on what technologies to protect then multiple parts of the executive branch can enforce the defensive policies levers (CFIUS reforms, export controls, immigration policy, counterintelligence resources) to protect those technologies

The most comprehensive way to address the scale and long-term nature of Chinese technology transfer would be:

- both defensive and proactive policies as well as
- a "whole of government" approach coordinating a new China policy and the tools of the U.S. government.

Only with a "whole of government" approach would the U.S. government be able to effectively enlist the support of the private sector and academia.

There are three principal decisions to make regarding the *defensive* policies:

1. Breadth of technologies to protect
2. International cooperation to seek: how closely the U.S. government should act with allies formally to stem further technology transfer
3. Immigration policy for highly-educated foreign students in STEM fields

The principal decision to make regarding the proactive policies is the *level of investment* in basic research, talent and the processes to commercialize innovation. Federal funding of R&D in the U.S. is at 0.7% of GDP or far from its peak during the 1960s of 2% of GDP falling behind China, Japan, Korea, Finland, Sweden, Denmark and Germany as a percent of GDP. The U.S. economy today continues to benefit from the innovations arising from federal research which created entirely new industries at the forefront of technology today including those based on semiconductors, GPS, the internet, hydraulic fracturing, genomics, and many others. To benefit from a thriving future economy, we must increase the investment we are making today in federally-funded research and the talent to drive a growing pipeline of innovations and technology breakthroughs. Additionally, to preserve our technological advantage we must take steps to ensure "a healthy and secure national security innovation base that includes both traditional and non-traditional defense partners"[85] including early-stage companies.

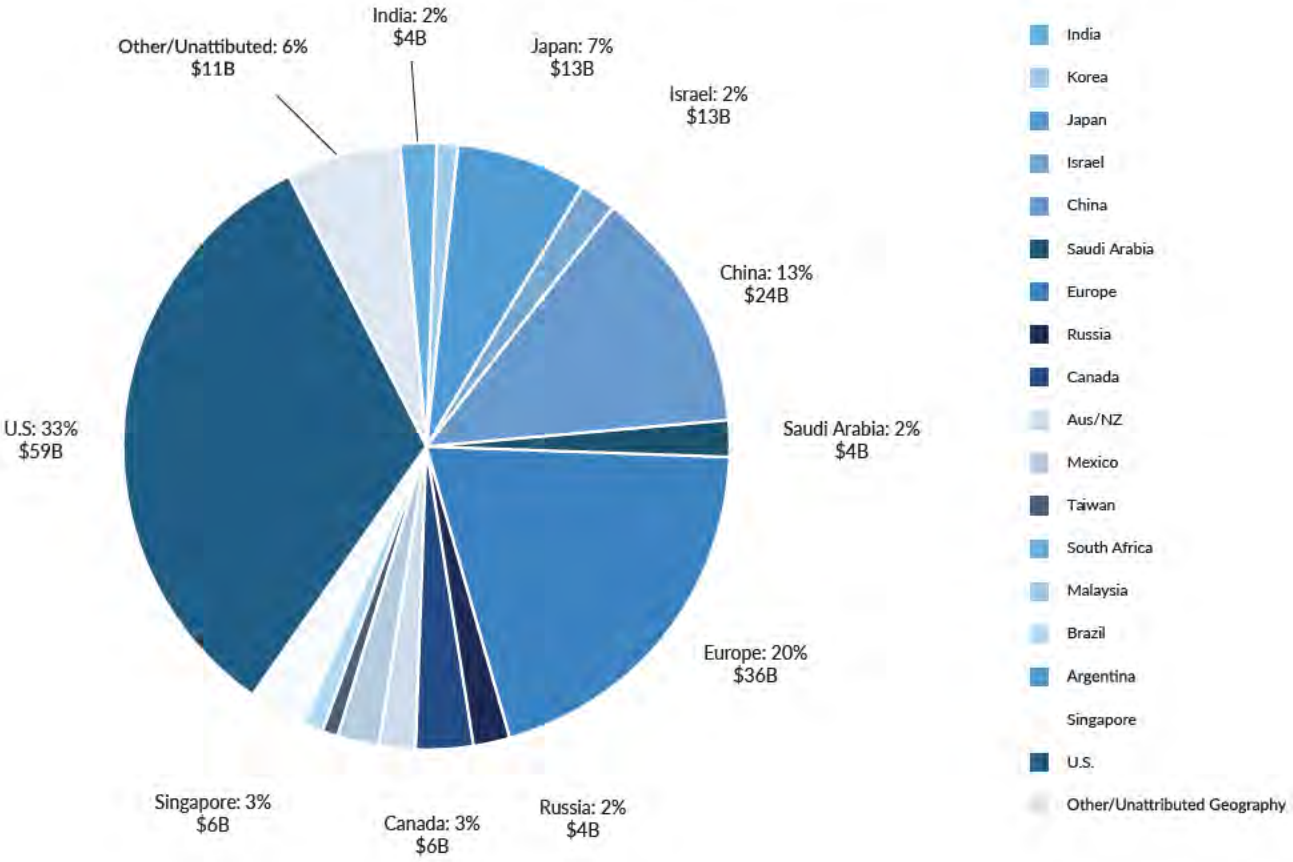
[85] Summary of the National Defense Strategy, January 2018, "Sharpening the American Military's Competitive Edge", p. 11

List of Appendices

APPENDIX 1: Chinese Investment in Critical Technologies

Compared to other sources of investment, Chinese entities ranked only behind domestic U.S. sources ($59 billion) and Europe ($36 billion), but well ahead of Japan ($13 billion), Russia ($4 billion), Israel ($4 billion), India ($4 billion), and Korea ($1 billion).

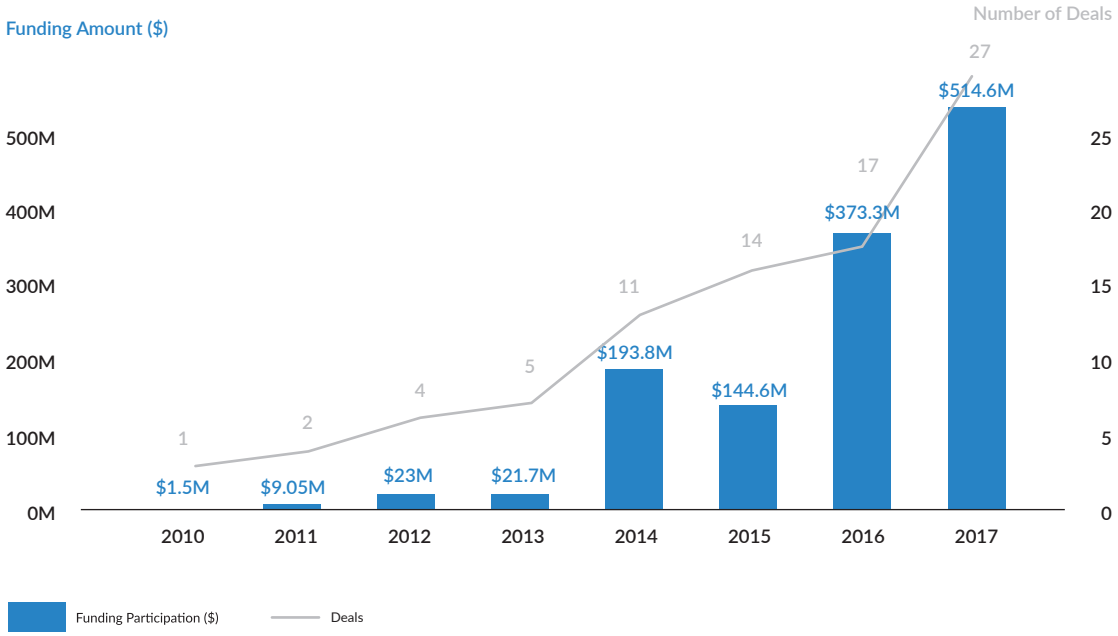
Chart 2: Worldwide Investment in U.S. Venture-backed Companies 2015 - 2017



Source: CB Insights; Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

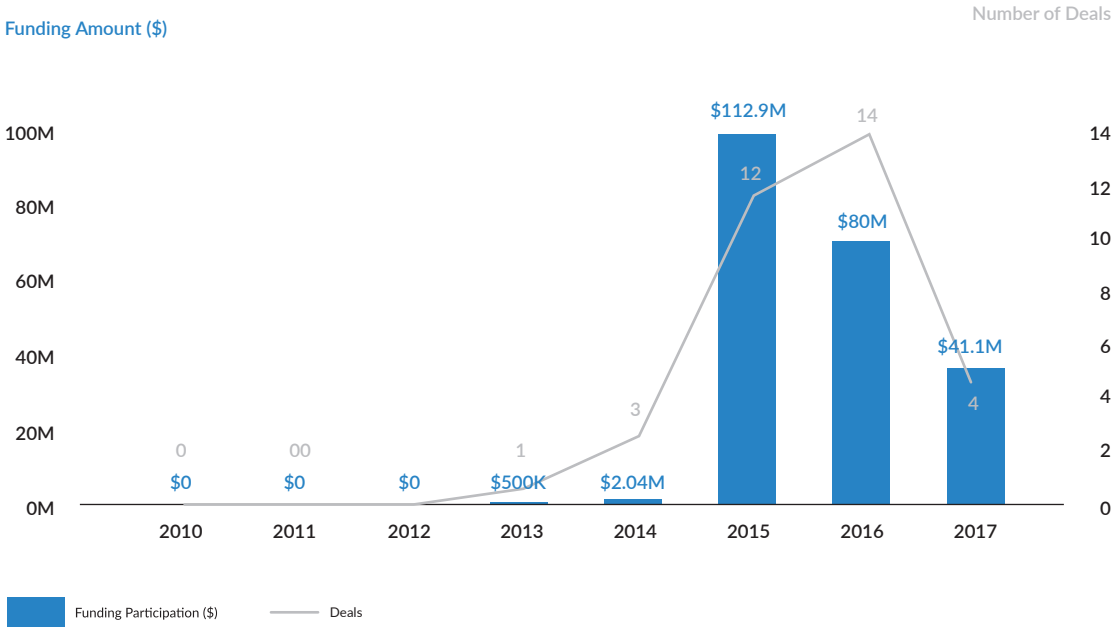
Source: CB Insights; Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

Chart 3: Chinese Investment in U.S. Artificial Intelligence Companies, 2010 - 2017
$1.3 Billion in Deal Value; 81 deals



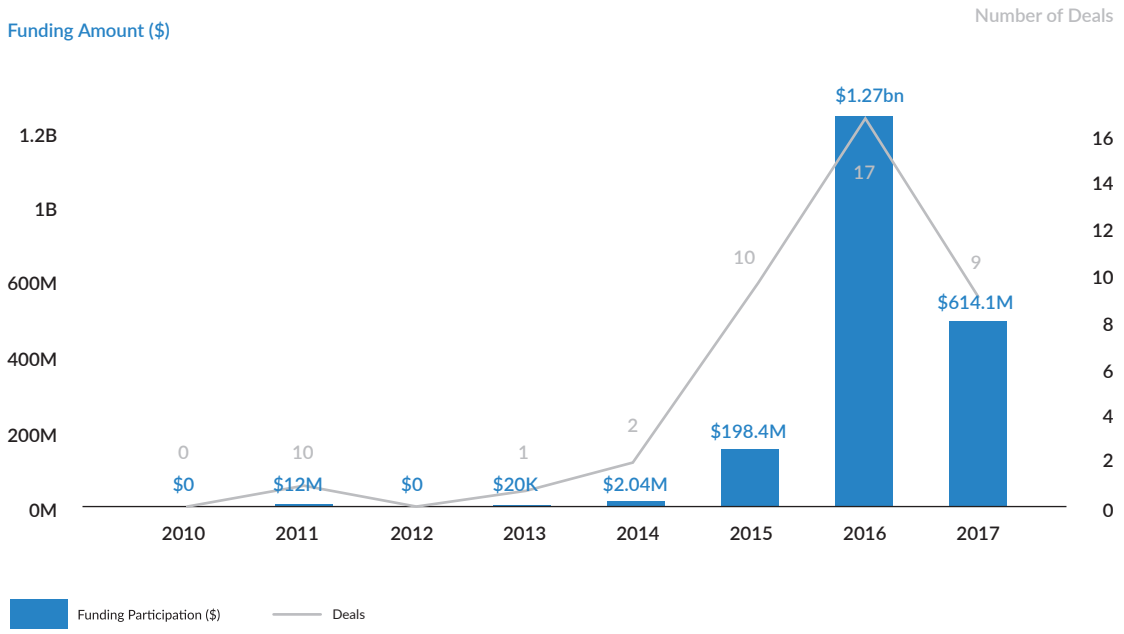
*CB Insights Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

Chart 4: Chinese Investment in U.S. Robotics Companies, 2010 - 2017
$237 Million in Deal Value; 34 Deals



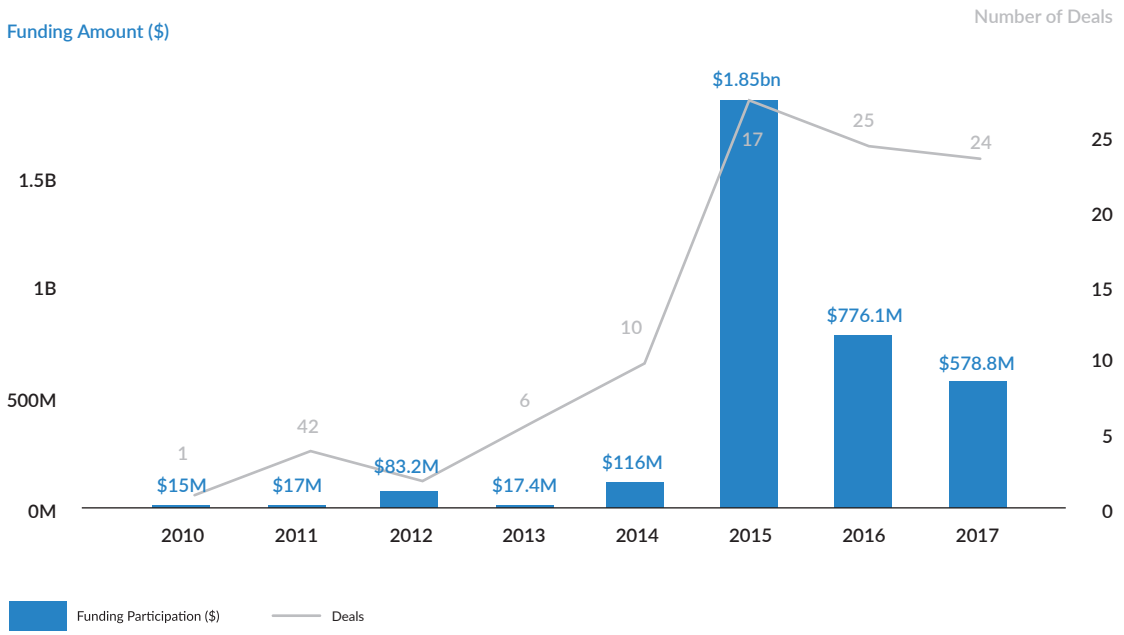
*CB Insights Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

Chart 5: Chinese Investment in U.S. AR/VR Companies, 2010 - 2017
$2.1 Billion in Deal Value; 40 deals



*CB Insights Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

Chart 6: Chinese Investment in U.S. FinTech Companies, 2010 - 2017
$3.5 Billion in Deal Value; 100 Deals



*CB Insights Search parameters include: Seed/Angel; Series A-E+; Convertible Note; Other VC

APPENDIX 2: Select Chinese Venture Deals in 2016 Illustrating Technology Focus[86]

Company	Focus Area	Round Amount ($M)	China Investors	Date	Location
Magic Leap	Augmented Reality	$798.5	Alibabe Group, Enjoyor Group	Feb-16	Florida
Zoox	Autonomous Vehicles	$200	AID Partners	May-16	California
Unity Technologies	Game Development Platform	$181	China Investment Corporation, Frees Fund	Aug-16	California
Velodyne	LiDAR Sensor Technology	$150	Baidu	Aug-16	California
NextVR	VR Content	$80	CITIC Guoan, NetEase, Capital, China Assets Holdings, CMC Holdings	Jul-16	California
Razer	Gaming Hardware and Products	$75	Hangzhou Liaison Interactive	Jun-16	Massachusetts
Circle Internet Financial	Consumer Payments	$60	Baidu	Jun-16	Massachusetts
Meta	Augmented Reality	$50	Tencent, Lenovo Group, Ningbo GQY, Horizons Ventures, Banyan Capital	Jun-16	California

[86] CBInsights data

Appendix 3: Case Studies of Chinese Venture Firms: SINOVATION and HAX

Sinovation Ventures

Sinovation Ventures is a venture capital firm domiciled in China with an office in Silicon Valley. The firm was founded by Dr. Kai-Fu Lee in September 2009 and invests in early stage companies (Series A and Series B) in the United States and China. The company focuses on the following investment areas: Internet of Things connected devices, developer tools; and online education. Sinovation's portfolio includes companies developing artificial intelligence, robotics, financial technology and AR/VR technologies.[87]

Some sample portfolio companies include[88]:

- **Swivl:** Swivl, owned and operated by Satarii, is the maker of a personal cameraman robotic video device. Swivl turns an iOS device into a personal cameraman with wireless microphone.
- **Robby:** Robby manufactures self-driving delivery robots that can autonomously navigate sidewalks to the consumer's door. This can reduce the costs for the on-demand meal, grocery, and package delivery industry by eliminating the high costs of human deliverers, which can ultimately lead to lower costs for the consumer.
- **Deep Vision:** Deep Vision is a deep learning company that is developing computer vision for cars, robots, drones and machines of all type. Deep Learning-powered breakthroughs are ushering in a revolution in computer vision which combine big data sets and powerful data centers.
- **SPACES:** SPACES is an independent virtual-and mixed-reality company based in Los Angeles, CA. SPACES is working with such companies as Microsoft, NBCUniversal, Big Blue Bubble and The Hettema Group, among others, to develop and produce a wide range of projects across all VR and MxR platforms and technologies, including Oculus Rift, HTC Vive, Microsoft HoloLens, Samsung Gear VR, PlayStation VR and Google Cardboard.

Sinovation Ventures has invested in almost 300 start-ups so far, including many well-known internet companies such as Zhihu, Dianxin, Umeng, Tongbu Network, Wandoujia, Anquanbao, Kuaiya, Qingting FM, Yaochufa, Weiche, Moji Weather, Elex, Kakao, Baozou Comics, Face++, VIPKID, Boxfish, U17, SNH48, ImbaTV, Molbase, Ebest, Maihaoche, EALL, The ONE Piano, Zaijia, Joy Run, Horizon Robotics, Niu, Planetary Resources, etc. and Meitu which is expected to go public on the Hong Kong Stock Exchange soon.[89]

[87] http://www.sinovationventures.com/

[88] Data retrieved from CB Insights Database

[89] https://www.crunchbase.com/organization/sinovation-ventures#/entity

[90] Ibid.

The firm combines incubation and investment offerings to facilitate the growth of companies that suit the Chinese marketplace. It has been awarded as a cutting-edge "National-Level Technology Company Incubator" by China's Ministry of Science and Technology (MOST). It has also been recognized as an "Incubation Base for Strategic Emerging Industries in Beijing" and a "Zhongguancun National-Level Innovative Model of Incubator for Indigenous Entrepreneurship" by Municipal Science and Technology Committee of Beijing, where the Firm's headquarters is based. Sinovation Ventures has established itself as a top-tier venture capital firm in China and has been backed by leading investors around the world. It currently manages three U.S. dollar funds and two RMB funds, with a total asset under management of $1.2 billion (or about RMB 8 billion).[90]

Hax

HAX is a hardware accelerator that has helped over 30 companies launch in the past 2 years. Based in Shenzhen and with an office in San Francisco, HAX provides end-to-end technical and financial support to early-stage hardware companies through its "Interactive Manufacturing Process", which enables rapid development of manufacturable products.

Between 2014 and 2016, Hax participated in nearly half of all deals involving Chinese investors (14 of 29 deals). HAX companies receive up to $25,000 to $100,000 each and access to the SOS Ventures Hardware scaling fund.[91]

Some examples of Hax investments include:

- **Petronics:** Petronics is the creator of "Mousr", a robotic mouse that has sensors, actuators, and intelligence that actually sees a cat and responds to its hunting movements like a real animal would.
- **Dispatch:** Dispatch is creating a platform for local delivery powered by a fleet of autonomous vehicles designed for sidewalks and pedestrian spaces.
- **Clean Robotics:** Clean Robotics provides trash sorting robots for offices.

HAX is backed by SOS Ventures, a venture firm with headquarters in Shenzen and an office in San Francisco. It funds a handful of accelerators similar to Hax – Indie Bio in the biosynthetic space; Chinaccelerator for pure software; and Food-X for food-related startups. SOS Ventures provides funding at the seed, venture, and growth stage, providing expertise and technical assistance to entrepreneurs in areas such as engineering, mass manufacturing, product/market fit, messaging, and presentation. The company's website claims funding for over 500 startups.[92]

[91] Retrieved at https://www.crunchbase.com/organization/haxlr8r#/entity

[92] Retrieved at https://www.sosv.com/

Appendix 4: Chinese Government-Backed Funds in Silicon Valley[93]

Company	Tie to Local Government	Total Money Raised	Select Investments
Westlake Ventures	Owned by Hangzhou government	$66 million ($16 million already available and $50 million pending approval for transfer out of the country)	WI Harper Group, SVC Angel Fund, Amino Capital, FreeS Fund, Spider Capital, Benhamou Global Ventures
ZGC Capital Corporation	Indirectly owned by 17 state-owned enterprises, including China State Construction and Beijing Industrial Development Investment Management Company.	$60 million so far, plans to raise $500 million by 2020	KiloAngel, Danhua Capital, Plug & Play (in the process), Santa Clara office building
HEDA Investment Co.Ltd	HEDA is a fund set up by Hangzhou Economic and Development, an economic development zone under municipal government of Hangzhou	$500 million	None yet: Focusing on information technology and bio tech.
Shanghai Lingang Economic Development Group	Supervised by the state-owned Assets Supervision and Administration Commission of the State Council (SASAC) of Shanghai.	None yet; plans to raise an overseas fund this year	A San Francisco office building for $42 million.
Research Institute of Tsinghua University in Shenzhen	Half-owned by the municipal government of Shenzhen, and the other half is owned by Tsinghua University.	Tens of millions of dollars	TEEC (Tsinghua Entrepreneurs & Executives Club) Angel Fund, Early-stage startups

Appendix 5: China's Economic and Technology Goals

Made in China 2025 is a plan aligning State and private efforts to establish China as the world's pre-eminent manufacturing power by 2049. "Its guiding principles are to have manufacturing be innovation-driven, emphasize quality over quantity, achieve green development, optimize the structure of Chinese industry and nurture human talent."[94] *Made in China 2025* highlights 10 priority sectors emphasizing the criticality of integrating information technology with industry.

[94] Scott Kennedy, "Critical Questions Made in China 2025," Center for Strategic and International Studies; Retrieved at https://www.csis.org/analysis/made-china-2025

Key sectors prioritized include:

- Advanced information technology
- Automated machine tools and robotics
- Aerospace and aeronautical equipment
- Maritime equipment and high tech shipping
- Biopharma and advanced medical products
- New energy vehicles & equipment

12th Five Year Plan of 2011-2015 lists a "new generation information technology industry" as one of the seven strategic and emerging industries to develop. Policies and practices were put in place to (1) prioritize indigenous innovation, especially in high-performance integrated circuit products, (2) promote domestic champions and (3) encourage technology acquisitions

- CT priorities include
  - Mobile communications,
  - Next generation internet
  - Internet of things
  - Cloud computing
  - Integrated circuits
  - New display technologies
  - High-end software & servers
- Policies and practices:
  - Prioritize indigenous innovation, especially in high-performance integrated circuit products
  - Promote domestic champions: pursue M&A, reorganizations and alliances between upstream and downstream enterprises
  - Encourage technology acquisitions, participation in standards setting & moving up the value chain

13th Five Year Plan of 2016-2020 "Internet Plus"[95] deepens reforms and priorities called for in *Made in China 2025* and emphasizes stronger control by the government over network-related issues as China continues to control the internet within China and gains access to global networks by controlling key component and telecommunications technologies

- Plan goal to "Encourage hundreds of thousands of people's passion for innovation, building the new engine for economic development"
- Leverages large internet base of 649 million users, 557 million of whom access the internet with a mobile phone
- Deliver to large cities 100 MBps internet bandwidth and provide broadband access to 98% of the population living in incorporated villages

[95] Lulu Chang, "China Outlines its Latest FYP Called Internet Plus."

- ICT priorities include:
  - Expansion of network economic space
  - New generation information infrastructure,
  - Advancements in Big Data
  - Enhanced information security and cyberspace governance
  - Fostering of domestic capabilities in:
    - Artificial intelligence
    - Smart hardware
    - New displays and intelligent mobile terminals,
    - 5th generation mobile communications
    - Advanced sensors and wearable devices

Medium and Long-Term Plan for Science & Technology Development is the most far- reaching of government plans to "shift China's current growth model to a more sustainable one, to make innovation the driver of future economic growth and emphasize the building of an indigenous innovation capability."[96] There are 3 strategic objectives:

- Building innovation-based economy through indigenous innovation
- Fostering an enterprise-centered technology system and enhancing Chinese firms' innovation
- Achieving major breakthroughs in targeted strategic areas of development and basic research and boosting domestically owned intellectual property

Project 863: China's National High Technology Program is designed to overcome the shortcomings in national security through the use of science & technology

- Encompasses development of dual-use technology (civilian and military applications)
- Lays a foundation for indigenous innovation

China's Mega Project Priorities are 16 Manhattan-style projects[97] to bring together the focus on specific innovations and the resources to ensure progress. These are outlined in Appendix 6.

[96] Hannas, Chinese Industrial Espionage, Chapter 3

[97] Michael Raska, "Scientific Innovation and China's Military Modernization", The Diplomat (September 3, 2013), Retrieved at http://www.thediplomat.com

Appendix 6: Chinese National Science and Technology Major Special Projects Mega-Projects as of October, 2016

Original Announced National Science and Technology Major Special Projects Contained in the '2006-2020 Medium and Long-Term S&T Development Plan'	Agencies in Charge
Core Electronics, high-end general chips, basic software	Ministry of Industry and Information Technology (MIIT)
Ultra large scale integration manufacturing technology	Beijing, Shanghai governments
High-end computer numerical controlled machine tools and basic manufacturing technology	National Development and Reform Commission, MIIT
Water pollution control and treatment	Ministry of Environmental Protection
Large-scale oil and gas fields and coal-bed methane development	China Petroleum, China United Coal-bed Methane Co.
Next generation broadband wireless mobile communications	Ministry of Science & Technology (MOST), National Energy Bureau, Tsinghua University
Genetic transformation and breeding of new plants	MIIT, Datang Electronics, CAS, Shanghai Institute of Microsystems, China Putian
Major new drug development	Ministry of Agriculture
High-resolution Earth observation system	MOST, Ministry of Health, People's Liberation Army (PLA) General Logistics Department
Prevention and control of major infectious diseases	State Administration for Science, Technology and Industry for National Defense (SASTIND), China National Space Administration
Large passenger aircraft	MOST, Ministry of Health, PLA General Logistics Department
Manned spaceflight and lunar exploration project	MIIT, Commercial Aircraft Corp. of China
3 Unidentified Classified Defense-Related Mega-Projects (candidates include Beidou Satellite Navigation System and Inertial Confinement fusion)	
New Additional National Science and Technology Major Special Projects Contained in the 'Science, Technology and Innovation 2030 Plan'	
Aero-engines and gas turbines	SASTIND, China Aircraft Engine Corp.
Quantum communications	
Information networks and cyber security	
Smart manufacturing and robotics	
Deep-space and deep-sea exploration	
Key materials	
Neuroscience	
Health care	

Source: Dr. Tai Ming Cheung, Associate Professor and Director of the Institute on Global Conflict and Cooperation (IIGC) at University of California, San Diego

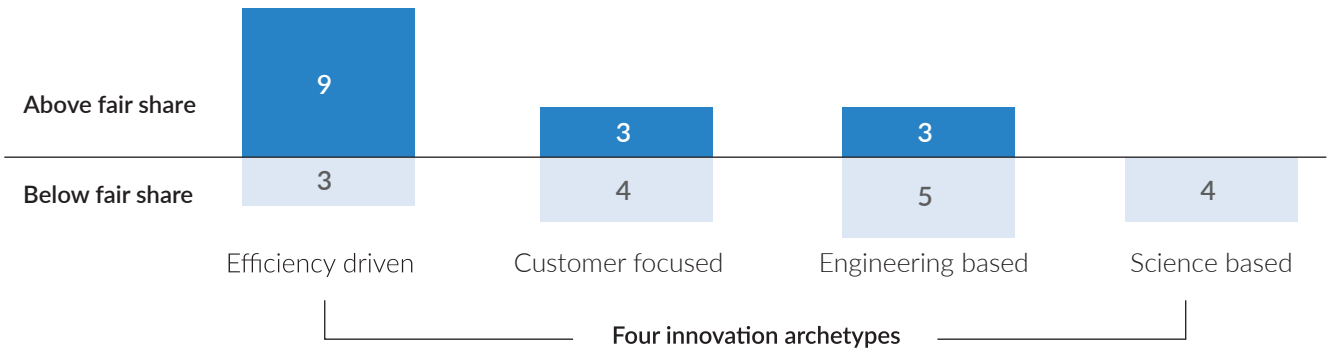
Appendix 7: McKinsey Study -- Industries Where China Leads in Innovation

To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed in what industries China was developing an innovation lead and in what industries China is lagging.[98]

- In traditional manufacturing-based industries where low costs provide a competitive advantage, it is not surprising that China is leading the world. These industries would include electronics, solar panels and construction equipment where a combination of a large and concentrated supply base, agile manufacturing, modular design and flexible automation all provide benefits.
- In its consumer markets (which are customer-focused), China has a natural advantage given the sheer size of the market of 1.3 billion people (4x that of the U.S.) and this advantage is compounded when markets are protected. Industries where China again leads the world would include household appliances, smartphones (functionality delivered at low cost) and internet software companies (Alibaba, Baidu and Tencent).
- In engineering-based industries, the results are mixed. The best example is high-speed rail where innovation has been matched with local demand and government sponsorship. China accounts for 86% of the global growth in railroads since 2008. Other examples would be wind power and telecommunications equipment (Huawei and ZTE). China is not yet leading in automobile engines, aerospace, nuclear power or medical equipment.
- In science-based industries, such as branded pharmaceuticals, the results are poor. Here, the massive growth and national focus on R&D spending have not yet paid dividends. These investments naturally take a long time to pay off and the Chinese government is actively working to remove obstacles to enable Chinese firms to lead. This is an area where focus on national mega projects can be fruitful since they concentrate government sponsorship with focused resources and local demand. For example, China is rapidly improving its drug discovery and medical trials process to favor its domestic companies. Gene editing is a technology where the government sees tremendous promise and is actively supporting.

The following chart summarizes this industry-grouping analysis:

Chinese Industries: actual vs expected performance performance in innovation
(based on China's share of global GDP[1]), number of industries = 31



[1]China's share was 12% in 2013.

Source: IHS Global Insight; International Data Corporation; annual reports; McKinsey Global Institute analysis

[98] Erik Roth, Jeongmin Seong, Jonathan Woetzel, "Gauging the Strength of Chinese Innovation," McKinsey Quarterly (October, 2015).

Appendix 8: Largest Chinese Cyber Attacks

- **Breach of more than two dozen major weapons system designs** in February, 2012 from the military and defense contractors including those for the advanced Patriot missile system (PAC-3), an Army system for shooting down ballistic missiles (Terminal High Altitude Area Defense, THAAD) and the Navy's Aegis ballistic-missile defense system, the F-35 Joint Strike Fighter, the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship[99]

- **"Titan Rain"** a series of coordinated attacks for multiple years since at least 2003 which compromised hundreds of government computers stealing sensitive information[100] " In 2004, an analyst named Shawn Carpenter at Sandia National Laboratories traced the origins of a massive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province in China. The hackers, code named by the FBI "Titan Rain," stole massive amounts of information from military labs, NASA, the World Bank, and others."[101]

- **PLA Unit 61398** (a cyberforce within the Chinese military) which penetrated the networks of >141 blue chip companies across 20 strategically targeted industries identified in China's 12th Five Year Plan for 2011-2015 such as aerospace, satellite and telecommunications and IT. Among other areas of theft, source code was stolen from some of the most prominent U.S. technology companies such as Google, Adobe and others; Google announced this in January, 2010. This resulted in the U.S. indictment of 5 members of this organization. According to Mandiant, PLA Unit 61398 is just one of more than 20 cyber attack groups within China.[102]

- **"Hidden Lynx"** which according to Symantec has a long history of attacking the defense industrial sector of Western countries with some of the most sophisticated techniques has successfully attacked the tech sector, financial services, defense contractors and government agencies since at least 2009[103]

- "DHS says that between December 2011 and June 2012, cyber criminals targeted **23 gas pipeline companies** and stole information that could be used **for sabotage purposes**. Forensic data suggests the probes originated in China."[104]

- "Canadian researchers say in March, 2105 that Chinese hackers attacked U.S. hosting site **GitHub**. GitHub said the attack involved "a wide combination of attack vectors" and used new techniques to involve unsuspecting web users in the flood of traffic to the site. According to the researchers, the attack targeted pages for two GitHub users—Great Fire and the *New York Times'* Chinese mirror site—both of which circumvent China's firewall."[105]

[99] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies", Washington Post (May 27, 2013). Retrieved at http://www.washingtonpost.com

[100] Nathan Thornburgh, "Inside the Chinese Hack Attack", Time (August 25, 2005). Retrieved at http://www.content.time.com

[101] Josh Rogin, "The Top 10 Chinese Cyber Attacks (that We Know of)," Foreign Policy (January 22, 2010) Retrieved at http://www.http://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/

[102] "APT1: Exposing One of China's Cyber Espionage Units", Mandiant Report, 2013.

[103] "Hidden Lynx--Professional Hackers for Hire", Symantec Official Blog (September 17, 2013). Retrieved at http://www.symantec.com

[104] Robert Knake, "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack," Defense One (June 15, 2015). Retrieved at http://www.defenseone.com.

[105] Knake, "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack"

- **"The Commerce Department's Bureau of Industry and Security** had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued."[106]

- **Breach of the U.S. Office of Personnel Management (OPM)** in 2014 where the personnel files of 4.2 million former and current government employee as well as the security clearance background information for 21.5 million individuals was stolen. Former NSA Director Michael Hayden said that this would compromise our national security for an entire generation.[107]

[106] Rogin, "The Top 10 Chinese Cyber Attacks (that We Know of)

[107] "The OPM Breach: How the Government Jeopardized our National Security for More than a Generation," Committee on Oversight & Government Reform, U.S. House of Representatives, 114th Congress (September 7, 2016).

Appendix 9: U.S. Events with Chinese Sponsorship

1. **Silicon Valley Innovation and Entrepreneurship Forum (SVIEF),** according to its website "is an international conference designed to foster innovation and promote business partnerships connecting U.S. and Asia-Pacific region." SVIEF has expanded to hold two conferences per year, the main conference held in the fall of 2016 and Silicon Valley Smart Future Summit held in winter and focused on interconnected devices. Both events are held at the Santa Clara Convention Center in Silicon Valley. A U.S. Congresswoman (Judy Chu) is the honorary Chairwoman of SVIEF and a keynote speaker at the principal fall conference was former U.S. Secretary of Energy Steven Chu. This gathering of startup CEOs, venture capitalists, Chinese companies and Chinese venture capitalists makes this an ideal location to collect information on the state of U.S. technology. Chinese officials attend who are assigned to collect intelligence.

2. **DEMO China,** an annual event held in Santa Clara, California (the heart of Silicon Valley) showcasing promising startups to Chinese investors. The event includes a keynote by the Chinese Consulate General, and has panels throughout the day covering topics such as navigating obstacles to investment in the U.S. and China; tips on how to evaluate startups; advantages of technology accelerators; and discussion of other investment trends.

3. **Silicon Valley-China Future Forum** (August, 2016) to link Silicon Valley with Chinese capital specifically in the fields of augmented reality, virtual reality and artificial intelligence.

4. **China Silicon Valley** is working with Silicon Valley city governments to drive increased investment and job growth by facilitating talent, technology and business exchange and investment between cities and businesses in China and their Silicon Valley counterparts. The intent is to help provide a one-stop service for government relations, legal, tax, consulting, networking and talent acquisition to facilitate Chinese government, businesses and individuals to invest, establish a factory, R&D center or other business activities in Silicon Valley. China Silicon Valley has an extensive network of business partners from diversified industries in Silicon Valley to carry out these activities.

5. **The Global Chamber San Francisco (GCSF)** hosts a seminar for entrepreneurs, investors and service providers with an interest in U.S.-China markets on strategies and best practices to enter and capitalize on business opportunities in U.S. & China.

6. **U.S.-China VC Summit & Startup Expo** (October, 2016) hosts a conference in Boston for investors and entrepreneurs who want to collaborate on opportunities between the U.S. and China.

7. **Chinese American Semiconductor Professional Association (CASPA)** holds many dozens of events per year in Silicon Valley and China. For 2017, the published schedule includes 4 conferences, 4 tradeshows, 4 workshops, 3 career development events, 3 international trips to China, hosted delegations from China and 6 members networking events. These events are all gathering Chinese and American semiconductor talent with the purpose of recruiting American talent.

Appendix 10: Strengths and Weaknesses of CFIUS Process Today

Strengths

- An understood process defined by FINSA statute (2007)
- No clear view on what constitutes a controlling interest that triggers an assessment by CFIUS which allows CFIUS to review more transactions than if a quantitative metric were always applied such as a 51% equity stake
- Many problematic potential acquisitions by Chinese companies have been stopped

---

Weaknesses

- CFIUS reporting is voluntary--transactions do not have to be reported
- There are many types of technology transfer not currently covered by CFIUS
  - Joint ventures where the U.S. company contributes IP/technology rather than an entire business
  - Technology licenses
  - Private company transactions that are "below the radar"
  - Minority investments that do not rise to the level of a "controlling interest"
  - Reverse mergers
  - Greenfield investments
  - Assets purchased from bankruptcies
- There's an inherent bias to develop mitigation agreements[108] to allow transactions to proceed but mitigation agreements are difficult to construct and enforce. Mitigation agreements lock companies into uncompetitive cost structures; these are too often designed under time pressure resulting in one-of-a-kind agreements or agreements which are far too comprehensive. There are no government resources assigned to monitor these agreements which undoubtedly means they are unenforced. The likelihood of a costly mitigation agreement also reduces the incentive for friendly foreign companies to acquire U.S. companies.
- There is no formal risk-scoring (by country and by sector) to create a transparent, scalable process to manage large numbers of transactions; expecting consensus among the 14 CFIUS agencies is unrealistic

[108] Mitigation agreements incorporate conditions that satisfy the national security risks such as governance measures, security requirements, separating a sensitive operation from the transaction or monitoring/verification mechanisms. From 2009-2011, roughly 8% of all cases reviewed resulted in mitigation agreements. "Understanding the CFIUS Process," Organization for International Investment.

- Security agencies (Department of Defense, Department of Justice, Department of Homeland Security) are not tasked to collaborate in articulating the national security risks of foreign investment in sensitive technology and facilities
- No comprehensive view of the technology landscape exists, and since CFIUS is only designed to review a single deal at a time, there is increased risk of damaging a complete sector critical to national security such as is happening in semiconductors[109]
- Allied governments' view of threats are not incorporated
- Required certification to Congress of "no unmitigated security threats" is unrealistic; with an increasing number of complex transactions there will be unmitigated security threats that evolve
- 90-day timeline defined by statute does not allow for dealing with more complex transactions
- CFIUS transactions are expanding to >150/year and there is no dedicated funding by Congress to support this effort; resources are stretched in every participating agency

[109] "Ensuring Long-Term U.S. Leadership in Semiconductors," President's Council of Advisors on Science and Technology, January 2017

About the Authors

Michael Brown is a White House Presidential Innovation Fellow working with DIUx.

Through August of 2016, Michael was the CEO of Symantec Corporation, the global leader in cybersecurity. During his tenure as CEO (2014-16), he led a turnaround as the company developed a new strategy focused on its security business, sold its Veritas business, hired a new executive team, formed business units, improved operating margins and articulated a new culture fostering innovation. Michael served on the Symantec Board from 2005 until 2016.

Michael is the former Chairman and CEO of Quantum Corporation (1995-2003), a leader in the computer storage industry specializing in backup and archiving products. As CEO of Quantum, the company achieved record revenues as the world's leader in disk drives for PCs and the world's largest tape drive business. Michael joined Quantum in 1984 and served in various management roles before being named as CEO in 1995. Michael served on the Quantum Board from 1995 until 2014.

Michael has also served as the Chairman of EqualLogic and Line 6 and has served on the public boards of Nektar Therapeutics, Maxtor Corporation, and Digital Impact. He serves on the Board of Trustees of the Berklee College of Music in Boston. He has a BA degree in economics from Harvard and an MBA from Stanford University.

Pavneet Singh has served in several roles on the National Security Council and National Economic Council at the White House and is a consultant with DIUx.

Most recently, he served as director of international affairs and managed the U.S.-China and U.S.-India economic relationships including serving as the NSC's lead director for the Asia Pacific Economic Cooperation (APEC) Leaders' Summit in Beijing and developing the President's economic deliverables for the bilateral summit with Chinese President Xi Jinping.

From 2011 to 2013, Pavneet was the senior advisor to the Deputy National Security Advisor Mike Froman and provided strategic and policy guidance across a portfolio that included trade, energy, climate, exports and managing the U.S. economic relationships with emerging economies. Prior to the White House, Pavneet worked as an analyst at the World Bank and at the Brookings Institute. Pavneet earned his master's with distinction in international relations at Georgetown University and his undergraduate degrees in business administration and political economy from UC-Berkeley.

List of Sources

Venture Data sourced from CBInsights and Rhodium Group

"China vs. U.S. Patent Trends: How Do the Giants Stack Up?" Technology & Patent Research.

"The Rise of Chinese Investments in U.S. Tech Startups." CBInsights Blog and Webinar, December 2, 2016.

Hanemann, Thilo and Rosen, Daniel. "Chinese Investment in the United States; Recent Trends and the Policy Agenda." Rhodium Group Report, December 9, 2016.

Hanemann, Thilo; Rosen, Daniel; Gao, Cassie. "Two-Way Street: 25 Years of U.S.-China Direct Investment." Rhodium Group and the National Committee on US-China Relations. November, 2016.

Reports

2016 Fact Sheet, Stockholm International Peace Research Institute (SIPRI)

2016 Report to Congress of the U.S.-China Economic & Security Review Commission. November, 2016. "2016 Special 301 Report." Office of the United States Trade Representative. April, 2016.

"APT1: Exposing One of China's Cyber Espionage Units." Mandiant Report. 2013.

"A 21st Century Science, Technology & Innovation Strategy for America's National Security." Committee on Homeland National Security of the National Science & Technology Council. May, 2016.

Adams, Donisha and Bernstein, Rachel. *Science.* November 21, 2014.

Cheung, Tai Ming; Mahnken, Thomas; Seligsohn, Deborah; Pollpeter, Kevin; Anderson, Eric; Yang, Fan. "Planning for Innovation: Understanding Chain's Plan for Technological, Energy, Industrial and Defense Development." Prepared for the US-China Economic and Security Review Commission by the University of California Institute on Global Conflict and Cooperation (IGCC). 2016.

"China Unveils Internet Plus Action Plan to Fuel Growth." The State Council for the People's Republic of China. Xinhua. July 4, 2015.

Cornell University, INSEAD and WIPO. "The Global Innovation Index 2016: Winning With Global Innovation." 2016. Desilver, Drew. "Growth from Asia Drives Surge in U.S. Foreign Students." Pew Research Center. June 18, 2015.

"Ensuring Long-Term U.S. Leadership in Semiconductors." President's Council of Advisors on Science and Technology (PCAST). January, 2017.

Felton, Ed and Lyons, Terah. "The Administration's Report on the Future of Artificial Intelligence." *White House Blog*. October 12, 2016

"Hidden Lynx--Professional Hackers for Hire." *Symantec Official Blog.* September 17, 2013.

"Historical Trends in Federal R&D." American Association for the Advancement of Science. October 13, 2016.

"How America's Giants Are Aiding China's Rise." *Geo-political Standpoint Report 84*. Tangent Link. October 13, 2016.

Hughes, Brian D. "Protecting U.S. Military's Technical Advantage" presented at the 18th Annual NDIA Systems Engineering Conference in Springfield, VA. October 28, 2015.

"The IP Commission Report: The Report on the Theft of American Intellectual Property." National Bureau of Asian Research. May, 2013.

Kraemer, Jackie and Craw, Jennifer. "Statistic of the Month: Engineering and Science Degree Attainment by Country." National Center on Education and the Economy. May 27, 2016.

"M&A in the U.S." Institute for Mergers, Acquisitions & Alliances.

"Military & Security Developments Involving the People's Republic of China 2017." Annual Report to Congress by the Office of the Secretary of Defense.

"The Military Balance." International Institute for Strategic Studies (IISS). 2016.

"National Outline for Medium and Long-Term Talent Development (2010-2020)." Xinhua Domestic Service. June 6, 2010.

Nichols, Gregory. "National Security Risks of Emerging Technologies." Homeland Defense and Security, Information Analysis Center. November 15, 2016.

O'Neill, Joseph P. "Economic and S&T Intelligence Collection." November 28, 2016.

"The OPM Breach: How the Government Jeopardized our National Security for More than a Generation." Committee on Oversight & Government Reform, US House of Representatives, 114th Congress. September 7, 2016.

"Project Atlas." Institute of International Education. Fall, 2015.

"Quantum Leap: Who Said China Couldn't Invent?" *Geo-political Standpoint, Report 85*. Tangent Link. October 14, 2016. "Special Reports: Economic Impact of International Students." Institute of International Education. 2016.

"Startups Nation" from the Tech Code website.

"Survey of Graduate Students and Postdoctorates in Science & Engineering." National Science Foundation. November, 2015. "Understanding the CFIUS Process." Organization for International Investment

"Understanding the U.S.-China Trade Relationship." Prepared for the US-China Business Council by Oxford Economics. January, 2017. "The U.S. Leads the World in R&D Spending," The Capital Group Companies. May 9, 2016.

"U.S. China Trade Facts." Office of the United States Trade Representative. 2016.

"U.S. Treasury Issuance--Gross and Net." Securities Industry and Financial Markets Association. 2016.

Book and Articles

Allison, Graham. *Destined for War: Can America and China Escape Thucydides's Trap?* New York: Houghton Mifflin Harcourt, 2017.

Areddy, James T. "U.S.-China Investment Flows Bigger than Thought." *Wall Street Journal.* November 17, 2016.

Auslin, Michael R. *The End of the Asian Century.* New Haven: Yale University Press, 2017.

Autor, David H.; Dorn, David; Hanson, Gordon H. "The China Shock: Learning from Labor Market Adjustments to Large Changes in Trade." *National Bureau of Economic Research (NBER) Working Paper 21906. January,* 2016.

Bader, Jeffrey. *Obama and China's Rise: An Insider's Account of America's Asia Strategy.* Washington: Brookings Institution Press, 2011.

Baker, Stewart. Skating on Stilts. Stanford, California: Hoover Institution Press, 2013.

Barton, Dominic; Woetzel, Jonathan; Seong, Jeongmin; Tian, Qinzheng, "Artificial Intelligence: Implications for China." *McKinsey Global Institute.* April, 2017.

Buckley, Chris. "China Passes Anti-terrorism Law that Critics Fear May Overreach." *The New York Times*. January 6, 2016.

Bymer, Maj. Loren. "Virtual Reality Used to Train Soldiers in New Training Simulator." *US Army News & Information.* August 1, 2012

Carter, Ben. "Is China's Economy Really the Largest in the World?" *BBC News*. December 16, 2014.

Cendrowski, Scott. "Is the World Big Enough for Huawei?" *Fortune*. February 1, 2017.

Chan, Cathy. "Chinese Private Equity Funds are Taking on the World's Giants." *Bloomberg News.* July 20, 2016.

Chang, Lulu. "China Outlines its Latest FYP Called Internet Plus." *Digital Trends.* March 6, 2016.

Chin, Josh and Dou, Eva. "China's New Cybersecurity Law Rattles Foreign Tech Firms." *Wall Street Journa*l. November 7, 2016.

Dwoskin, Elizabeth. "China Is Flooding Silicon Valley with Cash." *Washington Post*. August 6, 2016.

Fallows, James. "China's Great Leap Backward." *The Atlantic*. December, 2016.

French, Howard W. *Everything Under the Heavens: How the Past Helps Shape China's Push for Global Power*. New York: Alfred A. Knopf, 2017.

Hannas, William C.; Mulvenon, James and Puglisi, Anna B. *Chinese Industrial Espionage.* New York: Routledge, 2013.

Harris, Shane. "FBI Probes 'Hundreds' of China Spy Cases." *The Daily Beast*, July 23, 2015.

Jesjardins, Jeff. "China vs. United States: A Tale of Two Economies." *Visual Capitalist*. October 15, 2015.

Johnson, Jeffrey Z. "Chinese Investment in the U.S.: Impacts and Issues for Policy Makers." Testimony before the US-China Economic and Security Review Commission. January 26, 2017.

Kennedy, Scott. "Critical Questions Made in China 2025." Center for Strategic and International Studies (CSIS). November 7, 2016.

Knake, Robert. "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack." *Defense One*. June 15, 2015.

Lanman, Scott. "China's Holdings of U.S. Treasuries Fall to Lowest Since '13." *Bloomberg News.* September 15, 2016.

Li, Cheng. *Chinese Politics in the Xi Jinping Era.* Washington: Brookings Institution, 2016.

Lieberthal, Kenneth. *Managing the China Challenge: How to Achieve Corporate Success in the People's Republic*. Washington: Brookings Institution Press, 2011.

Liyan, Xu and Jing, Qiu. "Beyond Factory Floor: China's Plan to Nurture Talent." *Yale Global Online.* September 10, 2012.

Longhurst, John. "Car Wars: Beijing's Winning Plan." November, 2016.

Manjoo, Farhad. "Make Robots Great Again." *The New York Times*. January 26, 2017.

Markoff, John and Rosenberg, Matthew. "China Gains on the U.S. in the Artificial Intelligence Arms Race." *The New York Times*. February 3, 2017.

McGregor, Richard. The Party: *The Secret World of China's Communist Rulers*. New York: Harper Collins, 2010.

Miller, Tom. *China's Asian Dream: Empire Building Along the New Silk Road*. London: Zed Books, Ltd., 2017.

Mingfu, Liu. *The China Dream: Great Power Thinking and Strategic Posture in the Post-American Era.* New York: CN Times Books, 2015.

Nakashima, Ellen. "Confidential Report Lists U.S. Weapons Systems Designs Compromised by Chinese Cyberspies." *Washington Post*. May 27, 2013.

Navarro, Peter W. *Death by China*. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2011.

Philipp, Joshua. "Rash of China Spy Cases Shows a Silent National Emergency." *The Epoch Times*. April 25, 2016.

Pillsbury, Michael. *The Hundred-Year Marathon.* New York: St. Martin's Griffin, 2016.

Rachman, Gideon. *Easternization: Asia's Rise and America's Decline from Obama to Trump and Beyond.* New York: Other Press, 2016.

Raska, Michael. "Scientific Innovation and China's Military Modernization." *The Diplomat*. September 3, 2013.

Rauhala, Emily. "America Wants to Believe China Can't Innovate. Tech Tells a Different Story." Washington Post. July 19, 2016.

Rogin, Josh. "NSA Chief: Cybercime Constitutes the 'Greatest Transfer of Wealth in History'. " *Foreign Policy Magazine.* July 2012.

Rogin, Josh. "The Top 10 Chinese Cyber Attacks (that We Know of)". *Foreign Policy Magazine.* January, 2010.

Roth, Erik; Seong, Jeongmin; Woetzel, Jonathan. "Gauging the Strength of Chinese Innovation." *McKinsey Quarterly*. October, 2015.

Schell, Orville and Delury, John. *Wealth and Power: China's Long March to the Twenty-First Century*. New York: Random House, 2014.

Scott, Malcolm and Sam, Cedric. "China and the U.S.: Tale of Two Giant Economies." *Bloomberg News.* May 12, 2016.

Sirkin, Hal; Rose, Justin; Choraria, Rahul. "An Innovation-Led Boost for U.S. Manufacturing." Boston Consulting Group

Publications. April 17, 2017. .https://www.bcg.com/publications/2017

Stowsky, Jay. "The Dual-Use Dilemma" *Issues in Science and Technology*, Volume XIII, Issue 2, Winter, 1997. Swanson, Ana. "Gold Rush: Chinese Tech Companies Invest Overseas." CKGSB Knowledge. April 20, 2105.

Thibodeau, Patrick. "China Builds the World's Fastest Supercomputer without U.S. Chips." *Computerworld*. June 20, 2016.

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time*. August 25, 2005.

"Top 7 Worst Cyber Attacks in History." *Future Technology News*. September 23, 2010.

Trivedi, Anjani. "Subsidies Figure Big in China's New World." *Wall Street Journal*. November 17, 2016.

Tromblay, Darren E. and Spelbrink, Robert G. *Securing U.S. Innovation: The Challenge of Preserving a Competitive Advantage in the Creation of Knowledge.* Lanham, Maryland: Rowman & Littlefield, 2016.

Wei, Lingling. "China Issuing 'Strict Controls' on Overseas Investment." *Wall Street Journal.* November 26, 2016.

Wei, Lingling. "China's Overseas Funding to Shrink." *Wall Street Journal*. January 14, 2017.

"Xi Sets Targets for China's Science, Technology Progress." *Xinhua*, May 30, 2016.

Yang, Steven. "China Said to Mull Scrutiny of U.S. Firms If Trump Starts Feud." *Bloomberg News.* January 6, 2017.

Yuan, Li. "Chinese Technology Companies, including Baidu, Invest Heavily in AI Efforts." *Bloomberg News.* August 24, 2016.

Yuan, Li. "China Races to Tap Artificial Intelligence." *Wall Street Journal.* August 24, 2016.

Zhang, Yunan. "Chinese Government's Path to Silicon Valley." *The Information*. January 25, 2017.

TESTIMONY BEFORE THE SENATE ARMED SERVICES COMMITTEE

HEARING ON IMPLEMENTATION OF THE NATIONAL DEFENSE STRATEGY

BY

ELBRIDGE A. COLBY

DIRECTOR OF THE DEFENSE PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

JANUARY 29, 2019

Thank you, Mr. Chairman, Ranking Member Reed, and distinguished members of this Committee, for the invitation to appear before you. It is a great honor to testify before this body on a topic of the highest importance to our nation – the implementation of the 2018 National Defense Strategy (NDS), a Strategy which entails a fundamental shift in the orientation of our nation's armed forces toward great power competition.

I. Personal Involvement

During 2017 and 2018, I served as Deputy Assistant Secretary of Defense for Strategy and Force Development. In this capacity, I led a superb team of civilian and military officials from key parts of the Department tasked with developing the National Defense Strategy, reporting to Secretary Mattis and Deputy Secretary Work and Deputy Secretary (now Acting Secretary) Shanahan. In light of this experience, there are a number of distinctive attributes of this Strategy that I believe it is useful for the Committee to know.

- This Strategy is a result of the leadership and deep personal engagement of Secretary Mattis as well as Deputy Secretaries Work and Acting Secretary Shanahan. The Department's top leadership engaged regularly and in depth with the Strategy team and reviewed the document numerous times. Secretary Mattis met repeatedly with the team for long sessions; he considered the hardest issues in the Strategy and made clear choices about them in close consultation with then-Deputy Secretary Shanahan, who made the Strategy his priority in his first months in office and played a crucial, personal role in bringing the Strategy to fruition. The Strategy therefore reflects the considered judgment of those charged with leading the nation's defense.
- At the same time, this Strategy was not a purely top-down document. As Secretary of the Air Force Heather Wilson has related, the last version of the Strategy she recalls reviewing was on the order of the sixty-sixth version of the draft. From the earliest stages of its development, the Strategy received input from across the Department, and the range of Department leaders had the opportunity to review and comment on the Strategy as it evolved. Essentially everyone had their say. While the Strategy is – by design – a reflection of leadership judgments rather than a consensus or lowest-common denominator document, it benefited from the collective wisdom of the U.S. defense enterprise as well as from input from the Intelligence Community and other relevant organs of the U.S. Government.
- The Strategy team and Department leadership received input from Congress and outside experts from the beginning of the document's development, and it was red-teamed several times by leading defense experts.
- The Strategy was also informed by both strategic and operational-level wargaming.

II. A Recap of the National Defense Strategy

This hearing has been called to ascertain how the implementation of the Strategy is faring. I believe there is no more important issue on which the Committee can focus oversight, as the Strategy requires "urgent change at significant scale" for our national interests to be effectively

protected.[1] This is especially pressing because the National Defense Strategy Commission, a body chartered by Congress and composed of leading defense experts who had unparalleled access to the Department, reported that its members are "skeptical that DOD has the attendant plans, concepts and resources needed to meet the defense objectives identified in the NDS, and [they] are concerned that there is not a coherent approach for implementing the NDS across the entire DOD enterprise…[The Commissioners] came away troubled by the lack of unity among senior civilian and military leaders in their descriptions of how the objectives described in the NDS are supported by the Department's readiness, force structure, and modernization priorities..."[2] This is cause for significant concern.

Before discussing the Department's progress in implementing the NDS and how Congress can facilitate it, however, I believe it is valuable first to recap concisely what the Strategy, in concert with the 2017 National Security Strategy (NSS) with which it is so closely tied, assesses and directs.

The National Defense Strategy can be summarized as follows:

U.S. Defense Strategy in our Broader Grand Strategy

The United States has a lasting interest in maintaining favorable regional balances of power in the key regions of the world, especially East Asia, Europe, and the Persian Gulf. These favorable balances preserve our ability to trade with and access the world's wealthiest and most important regions on fair grounds, and prevent their power from being turned against us in ways that would undermine our freedoms and way of life.

Alliances are the critical mechanism for maintaining these favorable balances, and it is in the U.S. interest to continue to be able to effectively and credibly defend our allies and established partners such as Taiwan, in concert with their own efforts at self-defense.

The Particular Threat Posed by China and Russia

China in particular and to a lesser extent Russia present by far the most severe threats to our alliance architecture. *The once overwhelming U.S. conventional military advantage vis a vis these major powers has eroded and will continue to erode absent overriding focus and effort by the United States and its allies and partners.*

China and Russia pose a particular kind of threat to U.S. allies and established partners like Taiwan. Beijing and Moscow have plausible *theories of victory* that could involve employing a combination of "gray zone" activities (such as through the use of subversion by "little green men,"), robust anti-access/area denial (A2/AD) networks, lethal and fast maneuver forces, and strategic capabilities, especially nuclear arsenals. The adept integration of these assets could enable Beijing or Moscow first to overpower U.S. allies and seize their territory while holding off U.S. and other allied combat power. China or Russia could then, by extending their A2/AD

[1] Summary of the 2018 National Defense Strategy of the United States of America: Sustaining the American Military's Competitive Edge," Washington, D.C.: U.S. Department of Defense, 2018, 11.
[2] Eric Edelman, Gary Roughead, et al, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*. Washington, D.C.: U.S. Institute of Peace, 2018, 18.

and defensive umbrella over these new gains, render the prospect of ejecting their occupying forces too difficult, dangerous, and politically demanding for Washington and its allies to undertake, or undertake successfully.

The fait accompli is not the only but it is the most severely challenging of the theories of victory the Chinese or Russians could employ – especially against Taiwan in the Pacific or the Baltics and Eastern Poland in Europe.

Particularly in the case of China, these threats will worsen and expand as the power of the People's Liberation Army grows. Taiwan is the focal point today; before long, unless the ongoing erosion of our and our allies' military edge is reversed, the threat will be to Japan and the Philippines and thus to our whole position in maritime Asia, the world's most economically dynamic region.

The Need to Focus on Great Power Competition and its Implications

Accordingly, as Secretary Mattis put it in January 2018, "Great power competition – not terrorism – is now the primary focus of U.S. national security."[3] The United States' defense establishment must therefore focus on and adapt to this top priority – at scale and urgently, as the Strategy emphasizes.

What does this new prioritization mean and what does it entail?

At its deepest level, it requires a fundamental shift in the way the Department of Defense conceives of what is required for effective deterrence and defense. This is because the United States and its allies will be facing great powers – especially in the case of China. This is a dramatically different world than that which characterized the post-Cold War period, in which our armed forces could focus on "rogue states" and terrorist groups due to the lack of a near-peer competitor. Today and going forward, however, China in particular will present us with a comparably-sized economy and a top-tier military operating in its own front yard.

Above all, this requires a change in the mindset of our defense establishment. We have left a period of overwhelming American dominance and have entered one in which our armed forces will have to prepare to square off against the forces of major economies fielding the most sophisticated conventional and survivable nuclear forces. *Our armed forces will therefore need to shift from an expectation that they could dominate the opponent to one in which they must expect to be contested throughout the fight – and yet still achieve the political objectives set for them in ways that are politically tenable.*

Fortunately, our political-strategic goals, as indicated in the NSS and NDS, are defensive. We hope only to prevent our allies and partners like Taiwan from being suborned or conquered by our opponents. We therefore must defeat Chinese or Russian invasions or attempts at suborning our allies, and force Beijing or Moscow to have to choose between unfavorably escalating – and demonstrating to all their aggressiveness and malign intent by doing so – or settling on terms we

[3] Speech by Secretary of Defense James Mattis at Johns Hopkins University, School of Advanced International Studies, January 19, 2018.

can accept. This, to emphasize, is a different goal than regime change or changing borders. Rather, it is about *preserving the status quo by favorably managing escalation to win limited wars*.

How our forces achieve this objective in the event of conflict will be of the essence. Our forces must be exceptionally lethal and capable, optimized to defeat China or Russia. At the same time, however, wars with China or Russia must remain limited because the alternative is apocalypse, which neither side wants – thus we must plan and prepare for them as limited wars. Above all, this requires focusing on *defeating the other side's theory of victory, and particularly the fait accompli strategy.*

The NDS is specifically designed to deal with this challenge. Its military and force implications proceed from the political-strategic demands the NSS and NDS set out. As a core concept, the NDS calls on the Department to expand the competitive space – meaning above all to adopt a competitive mentality in everything that Department personnel do, one that refuses to take American superiority for granted, that searches for new or untapped sources of advantage, and that ensures that it is China and Russia that fear more what we might what do – rather than the other way around.[4]

The NDS therefore directs substantial changes in the following elements of our armed forces:

- Warfighting approach;
- Force structure: size, shape, and composition;
- Force employment;
- Posture; and
- Relationships with allies and partners.

Warfighting Approach

The Strategy calls for a different approach to warfighting from the post-Cold War era. This call stems from the political-strategic requirement to defeat the adversary's theory of victory by, at a minimum, rapidly delaying and degrading or ideally denying China or Russia's ability to impose the fait accompli on, for instance, Taiwan or the Baltics.

This necessitates a change from what might be called "the Desert Storm model" of warfighting. This model involved the time-consuming construction of an "iron mountain" of U.S. military capability in the region of conflict before the United States launched a withering assault to establish all-domain dominance and then ejected the enemy from our ally's territory. The Desert Storm model was enormously successful against "rogue state" adversaries – but it is also exactly the model on which China and Russia have ably and assiduously gone to school. By the time the United States constructs this iron mountain in response to a Chinese attack on Taiwan or Russian invasion of the Baltics, the war may already be lost because the costs and risks of ejecting an enemy now fortified in its new gains may be too prohibitive or because allies will not support the massive and terrifying counteroffensive needed for victory.

[4] "Summary of the 2018 National Defense Strategy of the United States of America", 4.

The United States consequently needs a new warfighting approach adapted to this threat. *This new warfighting approach involves U.S. forces resisting Chinese or Russian attacks from the very beginning of hostilities, fighting in and through enduringly contested operational environments to first blunt Beijing or Moscow's assault and then defeat it – without ever gaining the kind of all-domain dominance that the United States could establish against Iraq or Serbia.* With its invasion blunted or readily reversed, neither China nor Russia would have a way to end the war favorably; rather, Beijing or Moscow would face the awful choice of expanding the war in ways that play to U.S. advantages or swallowing the bitter but tolerable pill of settling on terms the United States can accept. Such a posture should deter a minimally rational adversary from choosing to pursue such a course.

The National Defense Strategy's Global Operating Model represents a new conceptual paradigm designed to help frame the Department's efforts to realize this new warfighting approach. This Global Operating Model is designed to defeat Chinese or Russian theories of victory, and especially the fait accompli.

- Its *"Contact" Layer* is designed to orient activities in the "gray zone," especially in concert with allies, to prevent Russia or China from dominating the crucial perceptual landscape or surprising the United States and its allies by augmenting allied defenses, collecting intelligence, and challenging salami-slicing activities.
- Its crucial *"Blunt" Layer* is designed to focus U.S. and allied force development, employment, and posture on the crucial role of "blunting": delaying, degrading, and ideally denying the enemy's attempt to lock in its gains before the United States can effectively respond. Crucially, *blunting is a function – not an attribute – of the force*. *The central idea is to prevent China or Russia from achieving a fait accompli* – it does not require a fixed force. Indeed, blunting is likely to be done best by a combination of munitions launched from afar as well as forces deployed and fighting forward.
- The *"Surge" Layer* is designed to provide the decisive force that can arrive later, exploiting the operational and political leverage created by the "Blunt" Layer to defeat China or Russia's invasion and induce them to end the conflict on terms we prefer.
- The *"Homeland" Layer* is designed to deter and defeat attacks on the homeland in ways that are consistent with the Joint Force's ability to win the forward fight and favorably manage escalation.

Likewise, the Strategy's core attributes of the future Joint Force also point to this new warfighting approach. The Strategy directs U.S. armed forces to become more *lethal, resilient, agile, and ready*. These terms have specific meanings, all designed to shift to a force able to fight through contested operational environments to deny the opponent's theory of victory:

- *Lethality* refers to the Joint Force's ability to strike at enemy maneuver forces without the kind of all-domain dominance the U.S. military has enjoyed over the last generation. Going forward, the Joint Force must be increasingly lethal in its ability to strike at key Chinese or Russian forces from the beginning of hostilities, even through dense air defense and other A2/AD networks.

- *Resilience* refers to the ability of the Joint Force and its enabling infrastructure to operate and achieve its objectives even in the face of determined and sophisticated multi-domain attack.
- *Agility* refers to the Joint Force's ability to become more operationally unpredictable while remaining strategically predictable, forcing the opponent to fear when, where, and how U.S. forces might appear and act rather than being able to anticipate when, where, and how they will perform.
- *Readiness* refers to the preparedness of the Joint Force on short notice to contest Chinese or Russian attempts to implement their theories of victory. This is a more narrow definition of readiness than that often used in defense discussions, one focused more on readying the Joint Force more for specific missions rather pursuing full-spectrum preparedness. Under the NDS approach, some units may not need to be highly ready; those crucial to blunting Chinese or Russian attacks against vulnerable allies, on the other hand, will need to be at a high pitch of preparedness.

To be realized and translated from concept into prepared forces, however, the Global Operating Model and these attributes *require new operational concepts* focused on these objectives and derived through rigorous gaming, experimentation, and training. These new concepts should be designed to overcome the operational problems laid out in the classified version of the Strategy.

Force Structure: Size, Shape, and Composition

The Strategy has marked implications for the size, shape, and composition of the Joint Force. Most significantly, the Strategy places a clear prioritization on being able to deter and, if necessary, to prevail over a major power adversary like China or Russia in a strategically significant, plausible scenario. Consequently, it prioritizes ensuring that the U.S. armed forces are able to win a fight over Taiwan or the Baltics before investing in the capacity to fight two wars simultaneously. This is only logical; losing the war in the primary theater would render success in any secondary theaters either fleeting or futile. Being able to fight two or more wars simultaneously is a good, but it is a good subordinate to that of winning in the primary, decisive fight.

Accordingly, the Strategy, as Secretary Mattis put it, prioritizes "capability over capacity" – or, put another way, "*capable capacity*." That is, the Joint Force must focus on what it takes to beat China *or* Russia in a key, plausible scenario – and this means enough forces of high caliber combined with attritable lower-end assets. This in turn requires budgets that prioritize manned and unmanned forces optimized to fight China or Russia over increases in personnel, force structure, and legacy systems best suited for taking on Saddam Hussein's Iraq or Slobodan Milosevic's Serbia. At the same time, it puts high emphasis on developing and fielding lower-cost and more sustainable ways of conducting secondary missions, such as operations against non-state actors in places like the Middle East.

Force Employment

The Strategy focuses on readying the Joint Force for plausible conflicts with China or Russia – precisely in order to deter them. The problem is that the Joint Force is not as ready for such

conflicts as it should be. Instead, U.S. forces have been focused on operations in the Greater Middle East and a wide variety of "shaping" missions, especially since 2001.

This must change. *The Joint Force needs to prioritize readying for major war against China or Russia* – through realistic exercises (including with allies) and training at places like Red Flag, Top Gun, and the National Training Center, as well as through needed rest and recuperation amidst a demanding readiness improvement schedule.

By necessity, this requires that *the Joint Force also do less* of these "shaping" and other secondary activities, and especially that the primary forces needed for major war be largely spared such duties. Continuing the current pace of operations and patterns of employment, such as using F-22s and B-1s over Syria and Afghanistan, will expend the readiness of the Joint Force on these peripheral missions rather than augmenting it against China and Russia.

In summary, *U.S. armed forces should become, as in most of the Cold War, primarily a training and readiness-oriented force prepared for war against a near-peer opponent, and not, as in the post-Cold War period, a military largely focused on operations in the Middle East and on "shaping" activities.*

Posture

The Strategy represents a reemphasis on forward presence – but a forward presence of a particular kind. *It is not about presence for its own sake or for symbolic or reassurance purposes.* Rather, it is about *combat-credible forward forces* – that is, forces that are or can rapidly get forward, survive a withering Chinese or Russian assault, and blunt the adversary's aggression. And it about is bases, operating locations, and logistic networks that can perform their missions in support of these goals even under heavy and sustained enemy attacks.

In the Pacific, this means investing in base defenses – including not only missile defenses but also camouflage, hardening, deception techniques, and other passive measures – that can make our relatively small number of bases more resilient, while also investing in a wider range of primary bases as well as secondary and tertiary operating locations throughout maritime Asia.

In Europe, posture is crucial. Much of the threat posed by the Russian theory of victory is due to the anachronistic placement of U.S. and allied forces, which reflects a pale fraction of the pre-1989 force laydown trapped in amber. Accordingly, the Strategy calls for a substantial near-term investment in rectifying the deficiencies in our deterrent and defense for Eastern Europe. This includes posturing more heavy equipment and advanced munitions in key places in Europe and readying allied infrastructure in Eastern Europe for rapid reinforcement.

Relationships with Allies and Partners

Another category of crucial changes initiated by the NDS is in our defense relationships with our allies and partners. The Strategy is clear: the era of untrammeled U.S. military superiority is over, yet we face not only high-end threats from China and Russia but also serious threats from North Korea, Iran, and terrorists with extra-regional reach. *We simply cannot do this all by ourselves.* This means that rebalancing our alliances and empowering new partners is not only a

matter of equity – as important as these are – but of strategic necessity. *We need our allies and partners to contribute real military capability* both to deterring China and Russia directly as well as to handling secondary threats.

This entails significant changes in how we deal with our allies and partners. We need to empower our allies as well as partners like India, Vietnam, Indonesia, and the United Arab Emirates to be able to defend themselves better from Chinese or Russian coercion, to handle secondary but still important shared threats with less U.S. involvement, or both.

Accordingly, we should see much more streamlined and liberalized procedures for arms and technology sales and transfers as well as for more intelligence sharing. States that share our broad interests, including ones, like Vietnam, with which we do not always agree, should be able to purchase military equipment more rapidly and with greater confidence in the sustainability and reliability of purchasing from the United States.

III. What Should Successful Implementation of the NDS Look Like in the Near Term?

What, then, should successful implementation of the NDS look like in the near term? The measures laid out below, while by no means exhaustive, would represent meaningful progress toward the fulfillment of the Strategy.

Warfighting Approach

The Department must make progress on developing innovative operational concepts. These must be oriented on overcoming the operational problems identified in the Strategy in ways that favorably manage escalation and achieve our national political-strategic ends.

Unfortunately, as the NDS Commission noted, there is little evidence that the Department has yet made meaningful progress on developing these new operational concepts.[5] Congress cannot make informed judgments about the Department's budget request and other authorization issues without understanding the Department's approach to developing such concepts, however, since they are vital to determining what capabilities the Department needs and what the Joint Force's composition and size should be.

- In this context, Congress might request a formal report from the Department on the state of its progress on developing novel operational concepts designed to deal with the operational problems identified in the Strategy.

Force Structure/Budget

The Department's Fiscal Year 2020 budget proposal is the first designed from its inception under NDS guidance. As Acting Secretary Shanahan has indicated, this should be the "masterpiece" budget in terms of implementing the NDS. The budget should therefore reflect measurable progress in realizing the NDS vision. *This in particular means budgets and programs should be demonstrably linked to improving the Joint Force's performance in the most stressing, strategically significant potential warfights against China or Russia. In practice, in the near*

[5] *Providing for the Common Defense*, vii.

term this should mean significant investments in augmenting capability rather than growing the size of the Joint Force, including in the FY20 budget.[6]

Key indicators of progress in the budget request toward implementing the NDS would include, but are not limited to:

- Rectifying clear, major shortfalls for key scenarios (especially Taiwan and the Baltics) through:
    - Procurement of substantial numbers of munitions designed to increase the existing Joint Force's lethality against Chinese invasion or Russian maneuver forces, such as longer-range anti-ship missiles (e.g., the Long-Range Anti-Ship Missile), longer-range air-launched cruise missiles (e.g., the Joint Air-to-Surface Standoff Missile-Extended Range), and guided anti-armor weapons for attacks on ground maneuver forces. These types of munitions are must-buys to increase the defensibility of Taiwan and the Baltics.
    - Sustained and substantial investment in augmenting threatened base and logistic network defense and resilience. This includes adequate active defenses for key bases and nodes (e.g., the Army's Indirect Fire Protection Capability, Increment 2) but also especially passive defenses to increase their resilience (e.g., funds for hardening, decoys, camouflage, deception techniques, et al).
- More robust space-based, airborne, and terrestrial assets for conducting surveillance and reconnaissance to support situational awareness, battle management, and targeting in heavily contested environments.
- Funding for a "high-low" mix of highly capable, lethal, and survivable platforms (e.g., penetrating aircraft and munitions, space systems, and attack submarines) and more attritable systems designed to complement and enable these more expensive platforms (e.g., lower cost unmanned aerial and underwater systems and smaller satellites).
- Investment in lower-cost systems and formations for secondary and tertiary missions. These include but are not limited to:
    - Light-attack aircraft, including potentially unmanned such platforms.
    - Smaller, tailored Army formations on the model of the Security Force Assistance Brigade (SFAB) optimized for training and assisting partner militaries.
- Reduction and, wherever possible, elimination of forces that are not survivable and useful in a high-end scenario and are too expensive for economical employment in low-end operations.
    - The Department's cancellation in FY2019 of JSTARS – a platform of dubious utility in a potential conflict with China or Russia – was an important step forward in this vein.
- The Congress should consider providing authorization and resourcing to enable the Secretary of Defense to reserve a substantial fund of money to be awarded to Services

[6] I highly commend to the Committee's attention an excellent short list of key top priority investment areas designed to address the National Defense Strategy's requirements in David A. Ochmanek, "Restoring U.S. Power Projection Capabilities: Responding to the 2018 National Defense Strategy," Arlington, VA: The RAND Corporation, 2018, 10-11.

and other entities based on proposals they submit that hold promise in addressing the key operational problems laid out in the Strategy.[7] This would encourage the development of innovative programs to deal with the challenges prioritized in the NDS.

Force Employment

The Joint Force is not ready enough for major war with China and Russia. As this is the most important and dangerous security threat affecting our national interests, rectifying this shortfall must be the primary goal of the Joint Force's activities. Such activities should include:

- Focus Joint Force activities on high-end training and invest in improving training facilities and techniques to prepare the Joint Force for high-end combat against China and Russia.
- Conduct exercises, including with allies in Europe and Asia, designed to actually test the Joint Force and allies' readiness to fight and prevail against Russia or China.
    - Such exercises should be designed in light of the Global Operating Model's framework to demonstrate the ability of U.S. and allied forces to blunt Chinese or Russian fait accompli strategies, including through falling in on prepositioned stocks and engaging the adversary quickly.
        - For example, in EUCOM, focus NATO alliance exercises much more on high-end fighting.

Given how demanding improving the Joint Force's readiness for major war with China or Russia will be, U.S. forces must consequently do less of everything else not connected to that goal. Accordingly, the Congress should expect the Department to propose to:

- Reduce activities not connected to this priority goal, including a wide range of exercises; shaping, assurance and presence missions and operations.

Posture

In both Europe and Asia, U.S. posture is not optimized to deal with our potential adversary's theories of victory. Accordingly, *the NDS calls for a substantial increase in investment for European posture designed to quickly and materially address the imbalance in military power on NATO's Eastern flank and improve the Alliance's ability to defeat a Russian fait accompli strategy, followed by a plateauing of this investment in the medium term to focus on the more substantial long-term Chinese threat.* In Asia, in addition to resources for making bases and operating locations more defensible and resilient, investment should focus on increasing options for operating locations throughout maritime Asia and the Western and Central Pacific.

- Congress should expect and require investments in the European Deterrence Initiative and within Service budgets to continue to go toward enhancing the combat-credibility of U.S. forces in Europe and the ability of Surge Layer forces to fall in on prepositioned stocks in the event of crisis or conflict.

[7] David A. Ochmanek, "Improving Force Development Within the U.S. Department of Defense: Diagnosis and Potential Prescriptions." Arlington, VA: The RAND Corporation, 2018.

    - This should include prepositioning heavy equipment and advanced munitions.
- Congress should expect near-term growth in investments in our European deterrent and defense posture but a plateauing of this investment over the coming years as U.S. and NATO posture, capability, and readiness against the Russian threat improves.

Ensuring Clear and Consistent Guidance for the Department

There is a significant problem within the Department of Defense with the proliferation of strategic guidance. Candidly, there is too much guidance and it is not as rigorously aligned as it should be. Too much guidance is redundant at best and at worst confusing, conflicting, and detrimental to effectively aligning the Department behind leadership intent.

The National Defense Strategy, the document established by Congress and embraced by Secretary Mattis and Acting Secretary Shanahan as the Secretary of Defense's preeminent strategic guidance, provides clear guidance not only at the high political level but also in terms of force structure and composition, development, employment, and posture. It establishes clear priorities and identifies areas for reducing emphasis. In addition, the Secretary's Defense Planning Guidance (for budget and force development) and Guidance for the Employment of the Force/Contingency Planning Guidance (for force employment) provide clear follow-on specialized guidance.

Every other document issued by subordinate officials – civilian and uniformed – in the Department should closely and clearly reflect these priorities. Yet this is not always the case, resulting in confusion, stasis, or misaligned activities.

Congress can help rectify this problem by:

- Expressing its view that the Defense Planning Guidance and Guidance for the Employment of the Force/Contingency Planning Guidance clearly and effectively ensure the implementation of the National Defense Strategy in their respective domains.
- Providing for clearer lanes in the road for the documents issued by the Chairman of the Joint Chief of Staff. In particular:
    - Providing a clearer, more narrowly scoped purpose for the National Military Strategy, and specifically providing that it focus on realizing the military dimensions of the National Defense Strategy. This should include a clear focus on operational concept development, a core military responsibility.
    - Clarifying that the Chairman's Program Recommendations and Global Campaign Plans should be derived from the Defense Planning Guidance and Guidance for the Employment of the Force/Contingency Planning Guidance, respectively.

Allies and Partners

Allies and partners are key to the success of the Strategy. They must understand and buy in to the Strategy for it to succeed. And they must be able to obtain the arms, technologies, and intelligence necessary to integrate with our Strategy.

Congress can help encourage this crucial element of the Strategy by:

- Advocating for a releasable version of the classified Strategy to be shared not only with close allies but also the broader set of allies and partners crucial to the Strategy's success.
- Reduce barriers to selling or providing financing for purchases of arms consistent with the Strategy (such as systems useful for developing indigenous A2/AD networks) to the wider range of allies and partners identified in the Strategy, such as India, Vietnam, and Indonesia. To realize this goal, Congress could:
    - Ensure that strategic considerations predominate in interagency and congressional decisions and authorizations about whether to sell arms and transfer technologies (consistent with security concerns).
    - Remove CAATSA penalties and barriers for partners such as India, Vietnam, and Indonesia. China is the most significant strategic challenge the United States faces. Penalizing partners crucial to helping us check Chinese assertiveness not only inhibits their ability to do so, but actively alienates them. It also undermines our long-term ability to shift these states away from their historical reliance on Russian arms sales toward our own and friendly states' defense industries.
        - Moreover, the best way to deal with the military threat posed by Russia is to augment our posture and forces in Europe, not to penalize partners that have historically relied on Soviet/Russian arms.

There are several allies and partners on which the Committee could most productively focus in light of their unique importance. Taiwan is especially significant because it is the most vulnerable member of the U.S. alliance and partnership architecture, especially over time, and because its own behavior is crucial to its defensibility. Japan and Germany, meanwhile, are the largest economies among U.S. allies. Greater and more focused defense effort from Tokyo is essential to the allied defense posture in the Indo-Pacific in light of the continuing military build-up by China. A cognate increase in effort by Berlin, meanwhile, is crucial to developing a more equitable and thus more politically sustainable NATO defense posture.

- The United States is committed to the defense of Taiwan against unprovoked aggression, but Taiwan itself must demonstrate much greater commitment and seriousness in providing for its own defense. Congress can help by ensuring the Administration provides and implements substantial defense sales to Taiwan that are in conformity with an asymmetric strategy along the lines of Taiwan's new Defense Concept.
    - While Taiwan's defense spending has inexcusably lagged, President Tsai Ing-wen's administration has committed to increased defense spending. Congress should encourage this and urge Taipei to fulfill its pledge.
    - Taiwan needs help from the United States to help defend itself. The Congress should therefore ensure defense sales and transfers to Taiwan are regular and actually useful for Taiwan's defense.
    - In particular, Taiwan needs to shift from a legacy force toward an asymmetric one capable of blunting and degrading a Chinese invasion or blockade. In particular, this means a shift from a focus on procuring vulnerable, big-ticket items like short-range aircraft and surface ships to an emphasis on A2/AD systems that can degrade a Chinese invasion or blockade and buy time for U.S. intervention. This

entails Taiwan focusing on procuring short-range UAVs, coastal defense cruise missiles, sea mines, mobile air defense systems, and rocket artillery.
    - Taiwan's Tsai administration has endorsed this approach but faces internal resistance, often political or bureaucratic in nature. To help, Congress should applaud Taiwan's shift to this new Defense Concept and ensure U.S. defense sales and transfers to Taiwan are consistent with the asymmetric strategy.
- Congress can applaud and support allies and partners that are working to align with the National Defense Strategy, and encourage others to do so. It can do so through direct engagements both here and on Congressional Delegations (CODELs). In particular:
    - Japan's level of defense spending is far too low for the threat environment it faces, and inconsistent with a mature, equitable alliance relationship with the United States. The administration of Prime Minister Shinzo Abe has, however, been working hard to change this, and deserves support.
        - Moreover, Japan's new National Defense Planning Guidelines are a cardinal example of an allied strategy that is very much in line with the National Defense Strategy.
        - Thus, while Congress should continue to press Japan to increase its defense spending, it should applaud Japan for its new Guidelines and its efforts to bring Japan's defense efforts into conformity with the security conditions it faces and an appropriate and sustainable alliance relationship with the United States.
    - Germany has lagged behind its obligations to NATO collective security for several decades. During the Cold War, the Bundeswehr was the most capable NATO military, save that of the United States. Yet Germany effectively almost demilitarized after the Cold War, and today is incapable of meaningfully contributing directly to the collective defense of NATO's newer entrants – a collective defense from which the Federal Republic benefited so greatly during the Cold War.
        - But Germany appears to have turned a corner, and Berlin has recommitted its military to the NATO collective defense mission and to increasing its defense spending from 1.2% to 1.5% of GDP by 2031. This is not enough, but it is a start that deserves support.
        - Congress could, while encouraging Germany to continue to increase defense spending, applaud the Federal Republic for its commitments and renewed seriousness in the service of NATO defense.

Defense Spending

Adequate funding is crucial for successful implementation of this Strategy, and thus for defending America's interests abroad. *Hard choices in the Department's programs and operations are necessary simply to keep up with the Chinese and Russian military challenge; they are not a basis for a smaller defense budget.*

As Secretary Mattis regularly put it, "the United States can afford survival."[8] The Congress should therefore insist that the Department follow through on the hard choices laid out in the Strategy but also provide the substantial and consistent funding needed to realize it.

An Active Congress and Senate Armed Services Committee

Congress – and especially this Committee – played a crucial role in setting the conditions for success for the NDS, including by sending a clear signal of the importance of prioritization and providing for a classified version of the Strategy. *The NDS is as much Congress' Strategy as the Department's.*

Because of Congress' tremendous importance in the nation's defense, realizing the strategic shift initiated by the NDS will require Congress to play a central role.

Most importantly, Congress and especially this Committee can continue to make clear, as Chairman Inhofe has already indicated, its strong and continued support for the National Defense Strategy. This is especially important and timely in light of the leadership transition in the Department.

- *In this vein, the Committee should ensure that the next nominee for Secretary of Defense commits to advancing and implementing the National Defense Strategy.*

Congress can also support and enable the implementation of the Strategy by both supporting the Strategy's hard choices and providing adequate and consistent levels of funding to the Department.

This is central because what differentiates the NDS from run of the mill strategic documents is not only its clear, overriding focus on the major contemporary security challenge the nation faces – great power competition – but also the hard choices reflected in the Strategy that Congress demanded and that the Department's leadership made. The Strategy reflects the understanding that the demands of preparing for great power competition require conducting secondary missions in a more economical way.

Saying that great power competition is important but failing to delineate clearly what not to do effectively undermines the ability to genuinely prioritize on this most pressing challenge. *If the political leadership of the Department is unwilling to say with some precision not only what the Department's priority is but also where risk can be taken and cuts can be made, no one below them will do so – nor should they be expected to do so. It is the job of the political leadership of the Department to assume responsibility for those hard calls and credibly communicate those decisions to subordinate echelons.* Secretary Mattis and Acting Secretary Shanahan – in what is probably an unprecedented act (at least in the post-Cold War era) of leadership – did exactly this.

Congress' support for these hard choices – and thus for actually prioritizing great power competition – is crucial and equally commendable.

[8] Speech by Secretary of Defense James Mattis at The Reagan National Defense Forum, December 1, 2018.

- Congress should therefore work with the Department to support and authorize, as appropriate, the Department's implementation of the hard choices reflected in the Strategy.

There is no better forum than this Committee for ensuring that serious deliberation over the nation's crucial defense matters receives the official and national attention it deserves. This Committee does not need to attempt to dictate the right answers to the Department, but it can ensure the right issues are being soberly and expertly discussed and highlighted, as it did during the 1970s and 1980s.

- In this vein, the Committee could hold both closed and open hearings on key issues that require attention, featuring both Department officials and outside experts, such as:
    - The results of the most recent and authoritative assessments of key conflict scenarios;
    - New operational concepts;
    - New ways of performing missions in secondary theaters, such as the Middle East, more economically; and
    - Improving interoperability with allies and partners to defeat Chinese and Russian theories of victory.
- In addition, the Committee could help communicate more effectively to and with the American public concerning the serious and growing threat posed by great power military competition – and, given its size and sophistication, China in particular – and why this challenge demands priority even as our national security infrastructure continues to manage threats from terrorists and "rogue states."
- At the same time, it is crucial that the National Security Strategy and National Defense Strategy priorities be reflected across government. The Committee could therefore work with the Senate Foreign Relations Committee and Senate Select Committee on Intelligence to ensure strategies and efforts are aligned, a crucial part of ensuring the United States effectively expands the competitive space.

Conclusion

The 2018 National Defense Strategy represents a fundamental shift in our country's defenses. Its core purpose was to identify and anticipate the most consequential and dangerous threats to our nation's interests, provide clear and actionable guidance to the Department of Defense as to how to maintain effective deterrence and defense against those threats, and by implementing these decisions stand the best chance of preserving a favorable peace in the coming years. It is a Strategy that directs hard choices and rigorous prioritization now, so that we may balance the power of a rising China and check a revanchist Russia. Failing to make those hard choices and investments now will not relieve us of the obligation to make them – it will only make them harder and costlier in the future.

THE 5G ECOSYSTEM:

RISKS & OPPORTUNITIES FOR DoD

DEFENSE INNOVATION BOARD

April 2019

The 5G Ecosystem: Risks & Opportunities for DoD

Defense Innovation Board, 3 April 2019

Coauthors: Milo Medin and Gilman Louie

TABLE OF CONTENTS

Executive Summary

The term “5G” refers to the oncoming fifth generation of wireless networks and technology that will produce a step-change improvement in data speed, volume, and latency (delay in data transfer) over fourth generation (4G and 4G LTE) networks. 5G will enable a host of new technologies that will change the standard of public and private sector operations, from autonomous vehicles to smart cities, virtual reality, and battle networks. Historical shifts between wireless generations suggest that the first-mover country stands to gain billions in revenue accompanied by substantial job creation and leadership in technology innovation. First movers also set standards and practices that were then adopted by subsequent entrants. Conversely, countries that fell behind in previous wireless generation shifts were obligated to adopt the standards, technologies, and architectures of the leading country and missed out on a generation of wireless capabilities and market potential.

In the early 2010’s, AT&T and Verizon rapidly deployed LTE across the United States on the 700 Megahertz (MHz) spectrum they won at auction in 2008. Building on this deployment, the United States became the first country (after Finland) to see a comprehensive LTE network that delivered approximate 10x the consumer network performance of then-existing 3G networks. This step-change in performance drove rapid adoption of new handsets with new semiconductors that not only could move much more data, but were also computationally much faster. U.S. companies like Apple, Google, Facebook, Amazon, Netflix, and countless others built new applications and services that took advantage of that bandwidth. As LTE was deployed in other countries, those same handsets and applications spread across the world. This initiative helped drive global U.S. dominance in wireless and internet services, and created a U.S.-led wireless ecosystem on which the Department of Defense (DoD) and the rest of the world has operated for nearly a decade.

Since the rollout of LTE, these wireless competitive landscape has undergone many changes. Chinese telecommunications equipment giant Huawei grew global revenues from approximately $28B in 2009 to $107B in 2018, while other traditional market leaders like Ericsson and Nokia have declined in revenue over that same period. Chinese handset vendors like Huawei, ZTE, Xiaomi, Vivo, and Oppo have rapidly grown in global market share, and are still growing rapidly in adoption and influence despite minimal sales in the U.S. market. In 2009, all of the top 10 Internet companies by revenue were American. Today, four of the top 10 are Chinese. These trends are already in effect, and 5G has the potential to skew future networks even further in the direction of China if it continues to lead.

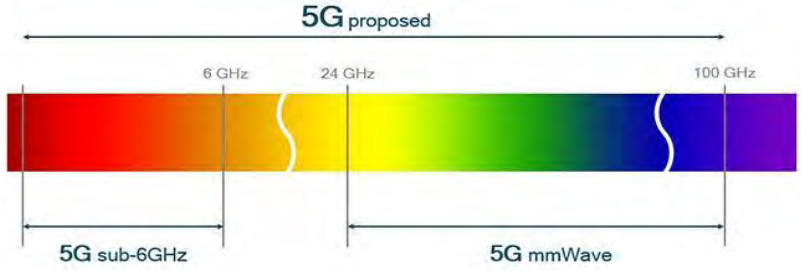
The shift from 4G to 5G will drastically impact the future of global communication networks and fundamentally change the environment in which DoD operates. While DoD will feel the impact of 5G, the rollout itself will be driven by the U.S. commercial sector. This study provides insight into the commercial landscape as well as the DoD landscape to give a comprehensive view of the stakeholders and future of 5G.

5G has the ability to enhance DoD decision-making and strategic capabilities from the enterprise network to the tactical edge of the battlefield. 5G will increase DoD’s ability to link

multiple systems into a broader network while sharing information in real time, improving communication across Services, geographies, and domains while developing a common picture of the battlefield to improve situational awareness. This improved connectivity may in turn enable a host of new technologies and missions, from hypersonics and hypersonic defense to resilient satellite constellations and mesh networks.

Spectrum will play a key role in the operation, development and roll-out of 5G. Peak data rates are driven by the amount of spectrum that is available to a wireless service. In 4G, up to five 20 MHz channels can be bonded together. But in 5G, up to five 100 MHz channels can be bonded together, enabling speeds approximately 20x faster than 4G and 4G LTE. While some 5G technology will be deployed in the currently-used cellular spectrum and achieve modest gains in performance (LTE is already fairly well optimized), full 5G development will require significantly more spectrum to provide another step-change improvement in performance for consumers, DoD or otherwise.

Countries are pursuing two separate approaches to deploy hundreds of MHz of new spectrum for 5G. The first focuses on the part of the electromagnetic (EM) spectrum below 6 GHz ("Low- to Mid-Band Spectrum," also referred to as "sub-6"), primarily in the 3 and 4 GHz bands. The second approach focuses on the part of the spectrum between ~24 and 300 GHz ("High-Band Spectrum," or "mmWave"), and is the approach taken by the United States, South Korea, and Japan (although all three countries are also exploring sub-6 to various degrees). U.S. carriers are primarily focused on mmWave deployment for 5G because most of the 3 and 4 GHz spectrum being used by the rest of the world for 5G are exclusive Federal bands in the United States, extensively used by DoD in particular.



The question of spectrum allocation is at the heart of the 5G competition, for the spectrum band of choice, whether sub-6 or mmWave, impacts nearly every other aspect of 5G development. Spectrum bands in the 3 and 4 Ghz range dominate global 5G activity because of improved propagation (range) over mmWave spectrum, resulting in far fewer base stations needed to be deployed to deliver the same coverage and performance. Because large swaths of the sub-6 bands in the United States are not available for civil/commercial use, U.S. carriers and the FCC (which controls civil spectrum in the US) are betting on mmWave spectrum as the core domestic 5G approach.

U.S. carriers may continue to pursue mmWave, but it is impossible to lead in the 5G field without followers. Leadership in wireless networks requires the global market to subscribe to

and build to the specifications of the leader's spectrum bands of choice, as these 5G subcomponents and products will ultimately drive interoperability across networks. The rest of the world does not face the same sub-6 spectrum limitations as U.S. carriers, and is subsequently pursuing 5G development in that range. As a result, the United States may find itself without a global supply base if it continues to pursue a spectrum range divergent from the rest of the world.

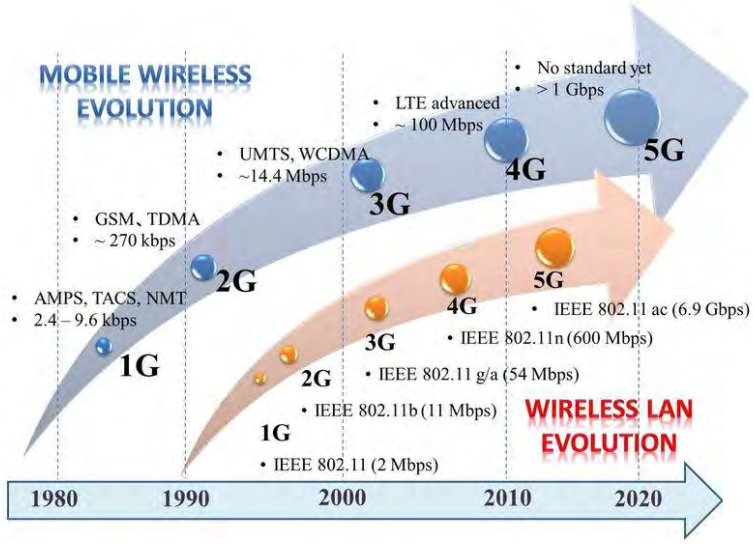
If the future 5G ecosystem adopted by most of the world is built on the sub-6 mid-band spectrum, the United States will also be faced with mmWave device interoperability challenges and sub-6 infrastructure security concerns. As sub-6 becomes the global standard, it is likely that China, the current leader in that space, will lead the charge. This would create security risks for DoD operations overseas that rely on networks with Chinese components in the supply chain. Even if the United States were to restrict use of Chinese equipment suppliers domestically, the United States is not a big enough market in wireless to prevent China's 5G suppliers from continuing to increase market share globally, resulting in significant pressure on a declining set of vendors that would serve the U.S. market. These vendors will in turn be unable to invest R&D towards future 5G offerings due to decreasing market share, limiting the number of competitive products and depriving DoD and U.S. industries of better and cheaper global supply chains.

China plans to deploy the first widespread 5G network, with its first set of sub-6 services becoming available in 2020. First-mover advantage will likely drive significant increases in their handset and telecom equipment vendors market along with their domestic semiconductor and system suppliers. As a result, Chinese internet companies will be well-positioned to develop services and applications for their home market that take advantage of 5G speed and low latency. As 5G is deployed across the globe in similar bands of spectrum, China's handset and internet applications and services are likely to become dominant, even if they are excluded from the US. China is on a track to repeat in 5G what happened with the United States in 4G.

CHAPTER 1: 5G HISTORY AND OVERVIEW

A History of Generation Technology

Mobile wireless technology has been in development for decades, with the first generation (1G) introduced in the late 1970s and fielded in the early 1980s. Since then, new generations of technology and wireless standards have been introduced every decade or so, culminating in our present state of transition between 4G and 5G capabilities. The value of each generation has increased exponentially, as each has enabled a host of other technology advancements across the commercial sector and military. All existing generations work within the low- to mid-band spectrum (less than 6GHz, or sub-6), but 5G has opened the door for millimeter wave (mmWave) spectrum use as well.



1G (Voice Calls): 1G mobile networks were fielded in the early 1980s with voice communications and limited emphasis on data transfer capability (early capability ~2.4 Kbps). 1G networks utilized analog signals to "hand off" cell users between a network of distributed base stations (hosted on cell towers) using standards like AMPS and TACS.

Source: https://www.researchgate.net/figure/Wireless-technology-evolution_fig1_322584266

2G (Messaging): In the 1990s, 2G mobile networks spawned the first digitally-encrypted telecommunications that improved voice quality, data security, and data capacity, while hosting limited data capability by way of circuit-switching using the GSM standard. In the late 1990s, 2.5G and 2.75G technology brought about improved data rates (upwards of 200 Kbps) using GPRS and EDGE standards, respectively. These later 2G iterations introduced data transmission via packet-switching, which served as a stepping-stone to 3G technology.

3G (Limited data: multimedia, text, internet): The late 1990s and early 2000s introduced 3G networks with faster data transfer speeds by fully transitioning to data packet-switching, with some voice circuit-switching that had been standard for 2G. This enabled data streaming, and in 2003 the first commercial 3G service was launched with mobile internet access, fixed wireless access, and video calls. 3G networks have now increased data speeds to 1Gbps when stationary and upwards of 350Kbps when mobile, using standards such as UMTS and WCDMA.

4G and LTE (True data: dynamic information access, variable devices): 4G network services were introduced in 2008 and featured data transfer at 10 times the speed of 3G by leveraging

all-IP networks and relying entirely on packet-switching. 4G networks enhanced the quality of video data due to larger bandwidths allowing for increased network speed. The introduction of the LTE network has since set the standard for high-speed wireless communications on mobile devices and data terminals. LTE is in constant evolution, and is currently on release number 12. "LTE advanced" can support ~300 Mbps.

5G: 5G's precise capabilities and extent of adoption are still to be determined. The speed, volume, and latency of data transfer will depend on the spectrum bands used, as well as the context of network usage (fixed or mobile). For example, a mmWave 5G network could enable incredibly fast speed for fixed local area networks under specific conditions that did not limit wave propagation, but would conversely struggle to maintain those speeds at extended range (on the "cell edge"). A sub-6 5G network might have lower maximum speed than mmWave, but could cover a much broader area without risk of interruption from a range of environmental factors. These conditions will ultimately determine the "standards" for 5G, and are currently in development globally.

History's Lessons: First-Mover Advantage in Generation Transitions

Transitions between wireless technology generations before 5G also had substantial commercial, competitive, and security implications for first-movers. Europe, led by Germany, gained first competitive advantage in 2G, and as a result companies like Nokia and Ericsson were able to roll out more advanced devices earlier and were already transitioning to 3G in the 2000s when the United States was still trying to implement 2G. The European wireless tech industry boomed during this period while U.S. companies struggled to keep pace. Europe lost this edge during the 3G transition, when they were hampered by regulations that required time-consuming auctions of 3G spectrum, rather than simply repurposing existing 2G spectrum bandwidth. Japan took the lead on 3G, and while the United States ultimately caught up to Japan, it took years to roll out 3G networks, which came at a huge cost to U.S. businesses as Japan sprinted forward with its 3G business model. The United States lost thousands of jobs and considerable revenue during this transition, during which multiple wireless technology companies failed or were absorbed into foreign companies.

The United States learned from its previous mistakes when it came to 4G and 4G LTE. Although it had been slow to implement 3G, there was a surge in 3G investment in the later years that ultimately gave the United States a head start when 4G arrived. Additionally, the FCC opened licenses for more bandwidth and set regulations to promote rapid expansion of the 4G network as it was being developed. Japan kept pace at first, but Japanese industry failed move quickly to develop the technology that would ultimately shape the 4G ecosystem. As a result, the United States took an early lead in the smart device market and ultimately displaced Japanese operating systems both in and out of Japan.

In the early 2010s, AT&T and Verizon rapidly deployed LTE across the United States in the 700 MHz spectrum they won at auction in 2008. The United States became the first country (after Finland) to see a comprehensive LTE network that delivered approximately 10x the consumer network performance of existing 3G networks. This step-change in performance drove rapid

adoption of new handsets with new semiconductors that not only could move much more data, but were computationally much faster as well. U.S. companies like Apple, Google, Facebook, Amazon, Netflix, and countless others built new applications and services that took advantage of that bandwidth and those new handset capabilities. As LTE was deployed in other countries, those same handsets and applications spread across the world, driving U.S. dominance in global wireless and internet services.

The United States has benefited significantly from this lead. Recon Analytics published a report in April 2018[1] estimating that the introduction of 4G contributed to 70% growth in the wireless industry between 2011 and 2014, bolstering GDP while increasing jobs in the wireless industry by over 80%. By leading the charge on 4G, the United States was able to build a global ecosystem of network providers, device manufacturers, and app developers that shaped the future of 4G and the experience of all other countries implementing it.

First-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products. For example, China is in the process of laying down fiber optic cables in its own territory and plans to do the same for the countries participating in its Belt and Road initiative, in addition to building 5G networks throughout Europe. This will allow China to selectively grant access to certain 5G companies and products to ride on that infrastructure.[2] China is using this opportunity to promote sub-6 spectrum usage, which will shape the entire 5G product market going forward. If companies want to sell their 5G products into China or into any network with Chinese sponsorship, they will have to build to Chinese preferred specifications and partner with Chinese companies. This increases the risk of product backdoors and vulnerabilities throughout the supply chain.

The shift to 5G will carry the same potential risks and rewards as previous generational transitions, but at an even larger scale. The leader of 5G stands to gain hundreds of billions of dollars in revenue over the next decade, with widespread job creation across the wireless technology sector. 5G has the potential to revolutionize other industries as well, as technologies like autonomous vehicles will gain huge benefits from the faster, larger data transfer. 5G will also enhance the Internet of Things (IoT) by increasing the amount and speed of data flowing between multiple devices, and may even replace the fiber-optic backbone relied upon by so many households. The country that owns 5G will own many of these innovations and set the standards for the rest of the world.

For the reasons that follow, that country is currently not likely to be the United States.

---

[1] "How America's Leading Position In 4G Propelled the Economy," Recon Analytics, 16 April 2018, https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

[2] Susan Crawford, "China Will Likely Corner the 5G Market - And the US Has No Plan," *Wired*, 20 February 2019, https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/.

Spectrum Use and Options

Spectrum use and availability are the most important factors in fielding a viable 5G network, as they will determine the speed, volume, and latency of data transfer going forward. 4G data transfer capabilities cannot keep pace with current demand, and the 5G step-change would address the increasing rate of data consumption by fielding a functioning 5G network using mmWave bands, sub-6 bands, or both. The following sections describe the relative strengths and weaknesses of mmWave and sub-6 approaches, as well as their potential applications and roles in a future 5G ecosystem.

Millimeter Wave (mmWave)

MmWave spectrum operates in high frequencies found between 30 GHz and 300 GHz, and is attractive for a number of reasons. First, the shorter wavelengths of mmWave create narrower beams, which in turn provide better resolution and security for the data transmission and can carry large amounts of data at increased speeds with minimal latency. Second, there is more mmWave bandwidth available, which improves data transfer speed and avoids the congestion that exists in lower spectrum bands (prior to researching potential 5G uses of mmWave frequencies, the only major operators in that area of the spectrum were radar and satellite traffic). A 5G mmWave ecosystem would require a significant infrastructure build, but could reap the benefits of data transferred at up to 20x the speed of current 4G LTE networks. Finally, mmWave components are smaller than components for lower bands of the spectrum, allowing for more compact deployment on wireless devices. Outside of its physical properties, MmWave is also attractive to U.S. 5G developers because the U.S. government owns large swaths of the sub-6 spectrum, particularly in the 3 and 4 GHz range, making it difficult for carriers to purchase dedicated spectrum licenses at FCC auctions or even to share that part of the spectrum.

However, mmWave has its share of challenges. While its short wavelengths and narrowness of its beam allow for improved resolution and security of data transfer, these qualities can also restrict the distance at which mmWaves can propagate. This creates a high infrastructure cost, as a mmWave network would require densely populated base stations throughout a geographic area to ensure uninterrupted connectivity. This challenge is further aggravated by the fact that mmWaves can be easily blocked by obstacles like walls, foliage, and the human body itself. MmWave spectrum can achieve extended range in specific circumstances, such as in large buildings with flat reflective windows above the tree line, but few environments in the United States are conducive to this type of propagation.

Various studies have begun to test the efficacy of mmWave and sub-6 infrastructure builds in the United States. MoffettNathanson LLC recently conducted an analysis of Verizon's 5G mmWave efforts in Sacramento and discovered that after roughly six months in the market, Verizon's ~150 fixed wireless broadband (FWBB) base stations can only offer service to around 6% of residential addresses in the tested areas.[3] Verizon has been targeting particularly dense

[3] Craig Moffet, Ray McDonough and Jessica Moffet, "Fixed Wireless Broadband: A Peek Behind the Curtain of Verizon's 5G Rollout," p. 7, MoffetNathanson, March 20, 2019, https://www.moffettnathanson.com/?Section=Media%20/Telecom.

parts of Sacramento as optimal testing environments and is focused on developing a fixed network, which carries fewer challenges for mmWave deployment than a mobile network. However, even in these optimized circumstances it is clear that scaling this solution to provide more coverage would be a time- and cost-intensive endeavor requiring a massive infrastructure build-out.

Google also performed a preliminary study for the Defense Innovation Board to ascertain the approximate capital expenditure (capex) and base station counts needed for mmWave deployments, using 425 MHz of spectrum at 28 GHz (a mmWave configuration standard for current U.S. 5G trials), compared to 250 MHz of spectrum in the 3.4 GHz band (a sub-6 configuration, standard for Chinese 5G trials and deployment). This equipment was deployed on 72,735 existing macrocell towers and rooftops (the easiest choice for deployment) and was found to provide mmWave coverage to only 11.6% of the U.S. population at cell edge speeds of 100 Mbps, with 3.9% coverage at 1 gigabit. For sub-6, the same tower sites covered 57.4% of the population at 100 Mbps, and 21.2% of the population at 1 Gbps. The study used high-resolution geospatial data that included shadowing from foliage structures, but did not take into account shadowing from the human body or a vehicle, which realistically would exist in a deployed environment and even further disrupt connectivity for mmWave networks.

Most operators are looking at deploying mmWave 5G sites on utility poles, given the poles' ease of accessibility and abundance. Using a database of utility poles in the United States, the study indicated that it would require approximately 13 million pole-mounted 28-GHz base stations and $400B dollars in capex to deliver 100 Mbps edge rate at 28 GHz to 72% of the U.S. population, and up to 1 Gbps to approximately 55% of the U.S. population. Figures 1 and 2 below show the difference in "splat" (propagation) between 28 GHz (mmWave) and 3.4 Ghz (sub-6) deployments on the same pole height in a relatively flat part of Los Angeles (blue represents 100 Mbps speed, red represents 1 Gbps speed):

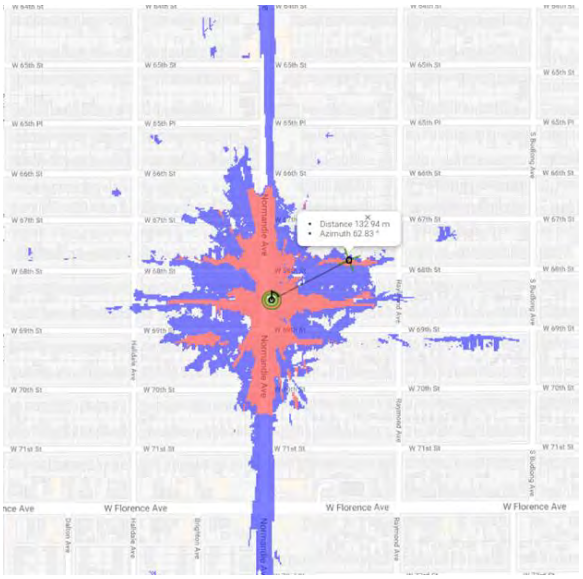


Figure 1: "Splat" chart with mmWave propagation

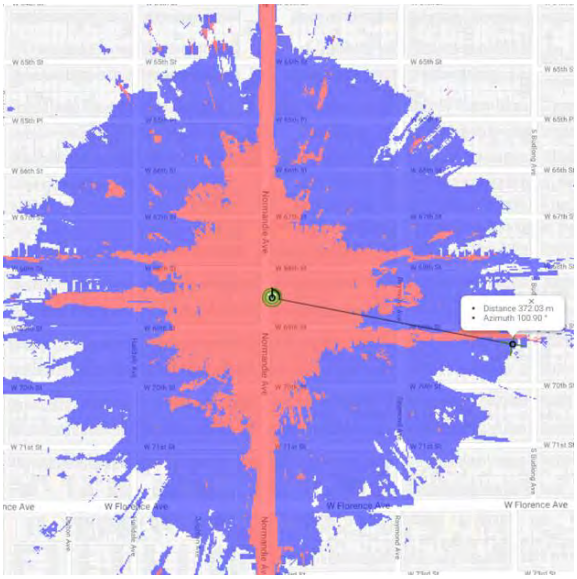


Figure 2: "Splat" chart with sub-6 propagation

There are ongoing efforts to mitigate these physics challenges, such as massive MIMO (multiple-input, multiple-output) and beamforming. Massive MIMO is an antenna array that will greatly expand the number of simultaneous connections and throughput, and will give base stations the ability to send and receive signals from many more users at once and increase the capacity of networks significantly, assuming multiple RF paths to users exist. Beamforming is a technique for identifying the most efficient data-delivery route to a particular user and reducing interference for nearby users in the process. These options can improve the propagation of mmWaves, but challenges remain with maintaining connectivity across a broader area using this part of the spectrum. Significant time and R&D will have to be devoted to solving the mmWave propagation problem before it can be deployed as a more universal wireless network solution.

Sub-6

Sub-6 includes the range of spectrum below 6 GHz. Sub-6 can provide broad area network coverage with lower risk of interruption than mmWave due to its longer wavelength and greater capacity to penetrate obstacles. It therefore requires less capex and fewer base stations, as compared to mmWave. This, together with the ability to leverage existing 4G infrastructure, makes sub-6 the lower hanging fruit for a potential 5G sub-6 ecosystem. Faster time-to-rollout is particularly important given the speed at which China is pushing forward. While mmWave may ultimately be deployed in specific environments where its propagation and cost challenges are not prohibitive, sub-6 will likely provide the broader solution for more wide area 5G coverage in the near term. This in turn will drive product design and manufacturing for the 5G supply chain, given the larger quantity of equipment that will feed that sub-6 network.

Maximizing the potential of 5G requires hundreds of consecutive MHz of bandwidth in order to optimize performance, and the sub-6 spectrum is already crowded with existing systems and uses. In the United States, sub-6 5G technologies will likely be deployed in existing macrocell networks and infrastructure through existing LTE spectrum. This would give modest improvements to RF system performance, but would not yield a 10x performance improvement over modern versions of LTE operating in the same spectrum. This failure to deliver the same disruptive speed improvements that LTE had over 3G would mute the impact of 5G deployment in the United States.

An additional challenge in the United States is that the government owns large portions of the sub-6 spectrum and limits commercial access to them. It is possible to relocate Federal users or share these bandwidths to allow commercial sector to develop 5G capabilities on them, but both of these processes are time-intensive. The average time it takes to “clear” spectrum (relocate existing users and systems to other parts of the spectrum) and then release it to the civil sector, either through auction, direct assignment, or other methods, is typically upwards of ~10 years. Sharing spectrum is a slightly faster process because it doesn’t require a complete upheaval of existing federal users, but even that has historically taken upwards of five years.

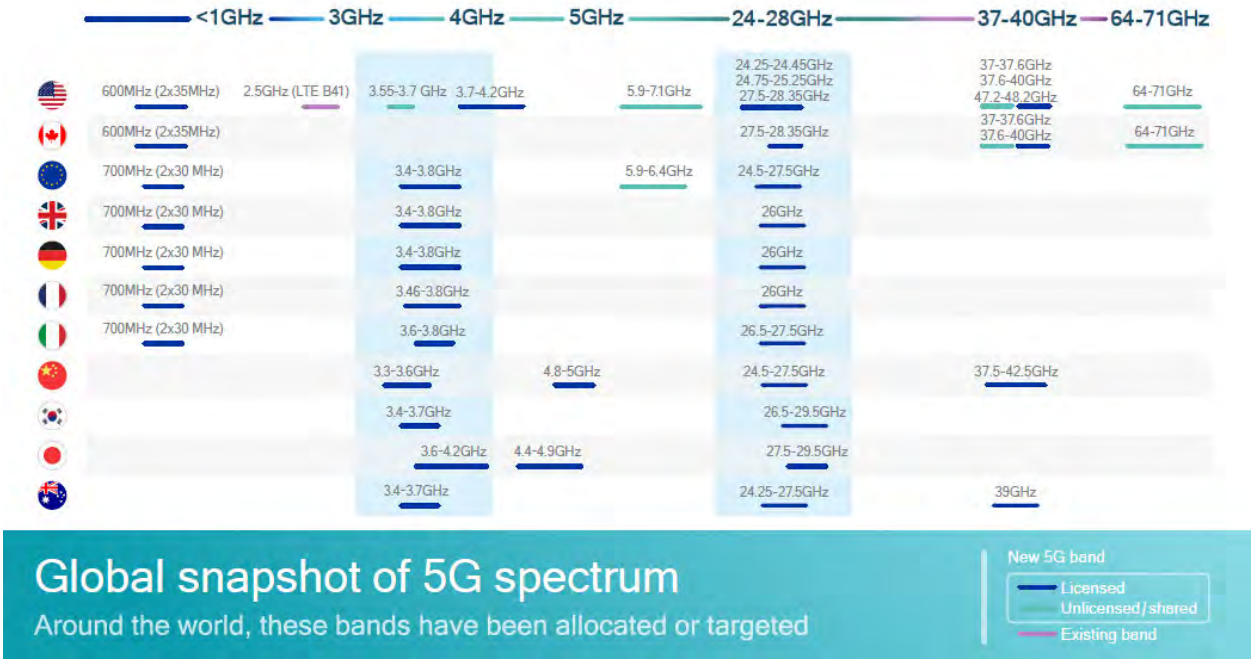
There are also legitimate concerns within DoD that sharing its bandwidths in the sub-6 spectrum will create a number of operational issues, from spectrum optimization to security vulnerabilities.

If DoD operators are forced to share their bands of the spectrum, there is concern that this may reduce the performance of systems. The addition of commercial users would also increase the overall congestion of the sub-6 spectrum, increasing the risk of connectivity interruptions for DoD operators. There is precedent for successful spectrum-sharing - in 2010, the FCC opened up the 3550-3700 MHz bandwidth (known as Citizens Broadband Radio Service, or CBRS) to the commercial sector. However, this process took more than five years, a timeframe that is untenable in the current competitive environment. This paper will explore the CBRS case study in more detail in Chapter 3.

Given these benefits and challenges associated with mmWave and sub-6, the future of 5G may involve some combination of both. Sub-6 is optimized for broad area coverage, which will make up a large part of the network, but mmWave may ultimately be able to provide more exquisite coverage in specific scenarios, and has some distinct military advantages in some topographies by virtue of being harder to intercept. This will require further research and testing in the mmWave spectrum targeting the current physics challenges around propagation, which may in turn lower the capex required for mmWave infrastructure deployment. In the near term, 3 and 4 GHz spectrum will likely serve as the dominant global bands that drive volume in infrastructure and device deployments. In the current state of 5G development and spectrum usage, it is unlikely that the United States will be able to leverage such technology, much less lead the rest of the world in that band of spectrum deployment as it did with 4G almost a decade ago.

CHAPTER 2: CURRENT STATE OF THE 5G COMPETITIVE FIELD

5G capability by country can be compared across five metrics: spectrum availability, widespread 5G trials, 5G roadmaps being established by the national regulator, government commitment (e.g., strategy documents and policies paving the way for 5G implementation), and industry commitment to early 5G launch.[4] Of these metrics, spectrum availability has the largest influence, as many of the other factors are dependent on that availability. For spectrum availability, there is ongoing debate on the merits of sub-6 versus mmWave and how to allocate spectrum in either of those categories, and in the United States there is a larger concern about allocating or sharing government-owned spectrum to the commercial sector. For infrastructure, carriers can take a "non-standalone" approach, which leverages existing 3G and 4G infrastructure as a stepping stone to get to full 5G capability, or a "standalone" approach, which requires a large up-front investment to build out new infrastructure for a 5G network.



Source: https://www.everythingrf.com/community/5g-frequency-bands

China

China has taken the lead in 5G development through a series of aggressive investment and spectrum-allocation initiatives. In addition to investing $180B in capital expenditure for 5G deployment over five years, China assigned 200 MHz of mid-band spectrum to its three state providers and is considering reallocating 500 MHz of C-band spectrum as well.[5] Domestically, China's 5G deployment is being implemented through its major telecommunications companies

[4] David Abecassis, Chris Nickerson and Janette Stewart, "Global Race to 5G - Spectrum and Infrastructure Plans and Priorities," Analysys Mason, April 2018, https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf.
[5] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jefferies, September 14, 2017, https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf.

(China Mobile, China Unicom, and China Telecom). All three are primarily focused on developing a standalone 5G network in China, with plans to deploy pre-commercial application in 2019 and formal commercial application in 2020. China now has ~350,000 5G-operable base stations deployed, which is nearly 10 times as many as are deployed in the United States. Globally, China's large manufacturers (Huawei and ZTE) are pushing 5G deployment through commercial sales of 5G-enabling equipment and devices primarily for non-standalone networks, and Huawei has already shipped upwards of 10,000 base stations overseas.[6]

Overseas, China has been developing partnerships with countries and foreign companies to expand its 5G influence. In Europe, Huawei and ZTE are offering their services to build individual countries' 5G networks, and have signed multiple 5G contracts despite pressure from U.S. officials demanding that allies block Chinese companies. Additionally, China has invested significant time and resources into its Belt and Road Initiative, including a push for Chinese-built network infrastructure to provide connectivity across the length of the route. This strategy has already had some success: in Q3 of 2018, Huawei held 28% share of the global telecommunications equipment market, up four percentage points from 2015.[7] Huawei is expected to continue growing that share as more 5G networks are rolled out relying on Chinese telecommunications equipment. These efforts will allow China to promote its preferred standards and specifications for 5G networks and will shape the global 5G product market going forward.

In aggregate, these approaches have given competitive advantage to China in 5G technology and capability. China's 5G strategy should be viewed in the context of the Chinese Communist Party's (CCP) grand strategy. Like artificial intelligence (AI), 5G development is a crucial component of Xi Jinping's "China Dream" vision and "Made in China 2025" roadmap. Social stability and economic growth are the CCP's top priorities because failures in those two areas are seen as direct existential threats to the regime, and 5G has the potential to transition China from a capital- and labor-intensive manufacturing economy to an innovation-led, consumption-driven economy with reduced dependence on foreign investment. In light of China's slowing growth and its ongoing trade war with the United States, the CCP likely feels pressured to pursue technological advancement initiatives like 5G more aggressively.

**For more detail on China's 5G strategy and capabilities, please see Classified Annex.*

South Korea

South Korea is closely following China in 5G maturity due to its early auction of spectrum and its general commitment to wireless technology. The South Korean government has built a clear roadmap including healthy investment to pursue 5G; in 2014, South Korea committed $1.5B to

[6] Isao Horikoshi and Takashi Kawakami, "Telecom's 5G revolution triggers shakeup in base station market," Nikkei Asian Review, December 25, 2018, https://asia.nikkei.com/Business/Technology/Telecom-s-5G-revolution-triggers-shakeup-in-base-station-market.
[7] Stéphane Téral, "Mobile Infrastructure Market Tracker - Regional," IHS Markit, December 3, 2018, https://technology.ihs.com/597909/mobile-infrastructure-market-tracker-regional-q3-2018.

promote 5G adoption and deployment by 2020, and in 2017, South Korea released its national broadband and spectrum plan ("K-ICT") to further promote 5G.[8] In line with the K-ICT plan, South Korea's Ministry of Science and ICT (MSIT) has since auctioned over 1,000 MHz of spectrum in the sub-6 and mmWave ranges to its three largest telecommunications providers (SK Telecom, KT Corp, and LG Uplus). South Korea has closely partnered with AT&T and Verizon to develop 5G mmWave networks, but has spread its risk in pursuing both sub-6 and mmWave by making its devices functional in both parts of the spectrum (as in the case of its Exynos 5100 5G modem).[9] AT&T is also working with Samsung to release a cell phone with mmWave and sub-6 capabilities at the end of 2019, but these dual-function devices may have less capability in the United States, given the restricted range of sub-6 spectrum available.

South Korea was able to leverage the 2018 Winter Olympics in Pyeongchang to showcase its 5G investment and conduct various network trials. South Korean industry already promotes high-intensity competition for 4G and LTE network technologies, which will fuel further rapid development of 5G. SK Telecom currently leads the field in investment and 5G trials, and was also able to acquire the largest amount of spectrum bandwidth in the 2018 MSIT auction, but all three telecoms providers plan to synchronize their launches of 5G cellular service in early 2019 for "Korea 5G Day." South Korea is well-positioned in the 5G field and will likely continue to be a leader going forward as its major telecoms providers take advantage of their newly-auctioned spectrum bandwidth.

Japan

Japan is following closely behind China, South Korea, and the United States in 5G capability. Japan has not yet auctioned off key parts of its spectrum bandwidth to commercial providers, but has plans to do so in 2019 and is currently developing both mmWave and sub-6 options (mmWave is being applied to limited, densely-populated geographic areas, while sub-6 is being used to cover the rest of the territory). Similar to South Korea, Japan hopes to use the 2020 Olympics in Tokyo to showcase and test 5G technologies and networks, and is driving most of its investment and activity around that 2020 timeline. In 2014, Japan stood up its 5G Mobile Forum (5GMF) to promote 5G research and development, coordinate 5G efforts across organizations, and promote general awareness of 5G.[10] In 2016, Japan's Ministry of Internal Affairs and Communication (MIC) released a strategy document ("Radio Policy to Realize 5G in 2020") that mapped out its commitment to and future deployment of 5G.[11]

---

[8] Lee Kangwook, "South Korean Government to Introduce K-ICT Spectrum Plan," December 23, 2016, http://www.ipnomics.net/?p=16629.
[9] Sean Kinney, "5G modem based on 3GPP Rel. 15, Samsung says," *RCRWireless News*, August 15, 2018, https://www.rcrwireless.com/20180815/5g/samsung-5g-modem-supports-sub-6-ghz-and-millimeter-wave-frequencies.
[10] Kohei Satoh, "Remarks by the 5GMF Secretary General," 5GMF, July 4, 2016, https://5gmf.jp/en/committee/20160704154530/.
[11] Kunko Ogawa, "Radio Policy to Realize 5G in 2020," Ministry of Internal Affairs and Communication (MIC), June 28, 2016, https://www.gsma.com/spectrum/wp-content/uploads/2016/08/MIC_Spectrum-for-5G-MIC-Kuniko-OGAWA.pdf.

Japan's three major telecoms providers (NTT DOCOMO, KDDI, and Softbank) are all in the process of testing 5G technologies with the intention of launching in 2020 before the Olympics. All three companies are conducting trials in the sub-6 and mmWave ranges, and MIC has conducted a "5G System Trial" in Tokyo and rural Japan.

Rest of World (Non-US)

While China, South Korea, the United States, and Japan lead the field, the rest of the world is playing catch-up on 5G deployment. The United Kingdom, Germany, and France can be considered "second tier" 5G developers, while Singapore, Russia, and Canada make up the "third tier," and the rest of the world comes after. These countries are beginning to auction off spectrum bandwidth with varying timelines and volume of spectrum made available, but many lack any formal policies or strategies to enable 5G implementation and most anticipate 5G launches outside of the 2020 timeframe.

Although Europe led the charge into 2G, it has since been hampered by regulations that have limited its ability to rapidly make spectrum bandwidth available, and has continued to lag behind in 3G, 4G, and now 5G. The rest of Asia has made some strides in 5G, but few countries have invested the same time and resources as China, Japan, and South Korea. Russia released its "Digital Economy of the Russian Federation" in 2017 that included a 5G roadmap, but has yet to develop any clear spectrum plan or devote significant resources to that roadmap.[12] Russia used the 2018 FIFA World Cup to launch some of its 5G efforts, but is still highly reliant on foreign 5G technologies and partnerships to move its 5G development forward.

Given the gap in 5G advancement between the first tier and everyone else, the rest of the world will likely be driven to implement the 5G network design and infrastructure of whichever country leads 5G. China is the current leader, and U.S. allies have taken different stances on how to respond to the Chinese drive to set 5G standards. Some are wary of Chinese influence because of security concerns and are actively working to push back on China's 5G roll-out. For example, in December the Czech Republic's cybersecurity agency (NUKIB) issued an official warning that Huawei and other Chinese companies posed a national security risk, citing existing Chinese statutes (*National Intelligence Law*, enacted June 27, 2017)[13] that require Chinese companies to actively cooperate with the intelligence community. This has driven a security review throughout Czech public and private sectors, effectively halting all sales of Huawei 5G goods into the country. Australia and Poland have also taken a hard line against China, and the United States has been heavily pressuring its other allies to follow suit.

---

[12] "The Digital Economy of the Russian Federation," accessed March 20, 2019, http://ac.gov.ru/en/projects/014097.html.

[13] Article 14: "State intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation"; Article 17: "As necessary for their work, the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings." China's *National Intelligence Law,* June 27, 2017.

However, other countries have been less enthusiastic about ousting China from their 5G markets, given the price and quality of China's offerings. Germany has refused to ban Huawei, despite U.S. threats to cut off intelligence-sharing, and the United Kingdom appears likely to take the same approach. Both Germany and the United Kingdom have pushed back on U.S. claims that Huawei and other Chinese telecommunications companies represent an unacceptable risk to national security, claiming that their security organizations could take measures to limit vulnerabilities in their networks. India and Italy have also expressed their hesitancy to exclude Huawei products from their 5G roll-outs, and in recent months New Zealand has eased its initial hard stance against China. In the coming months, Europe will continue to be a battleground for the future of 5G, as it represents one of Huawei's largest markets as well as a major source of U.S. allies. This fight also suggests a more concerning trajectory for the rest of the world's approach to 5G - in particular, developing countries that are more sensitive to cost will find the Chinese 5G price-point difficult to turn down, especially when the offer is sweetened with infrastructure and project-financing incentives like the Belt and Road Initiative.

United States

Private Sector

The telecommunications industry is organizing the effort to develop and deploy 5G in the United States, with increasing support from the U.S. government. Verizon, AT&T, Sprint, and T-Mobile are all developing their own 5G networks and 5G devices, each with their own strategy and method. Verizon and AT&T are focused on developing high-band mmWave networks and are in the process of deploying small cells in various test cities for mobile and fixed applications, Sprint is taking a joint approach of mmWave and mid-band spectrum to build out its network, and T-Mobile is focused on mmWave and low-band spectrum. While all carriers are looking into sub-6 spectrum options to some extent, they are inherently restricted by smaller amount of bandwidth available in sub-6 relative to the hundreds of GHz available in mmWave, and this constraint is exacerbated by the fact that the U.S. government owns large portions of the sub-6 spectrum. Carriers are piggy-backing off of existing 4G infrastructure, but those focused on mmWave will have to build out additional infrastructure to ensure uninterrupted connectivity through a dense network of base stations. There is debate over whether some of the networks deployed have qualified as true 5G, and there is intense competition between these providers to roll out 5G networks within the next few years. 5G development is being overseen by 3GPP (3rd Generation Partnership Project), the standards body that also oversaw the development of 3G UMTS (including HSPA) and 4G LTE standards.

Despite messaging from various marketing initiatives in the United States, very little U.S. territory has seen deployment of 5G infrastructure that can deliver 1 Gbps or even 100 Mbps service at the edges of coverage. Whereas LTE deployment resulted in 10x end user speed improvement across large parts of the United States, carriers to date have not demonstrated deployment capability that would deliver high speeds to large parts of the U.S. population.

As discussed in Chapter One, U.S. carriers have had some success in deploying limited mmWave for small geographic areas, but these have limitations for future scalability. Even in optimized circumstances, it is clear that scaling mmWave to provide more coverage would be a time- and cost-intensive endeavor requiring a massive infrastructure build-out.

There is the risk that these carriers will not even be able to commit the necessary capex to scale those mmWave networks, given the large number of base stations required. At the end of 2018, Verizon held ~$120B in debt with ~4% dividend yields, while AT&T held ~$175B in debt with over 6% dividend yields.[14] T-Mobile holds ~$25B in debt, and Sprint holds ~$40B in debt.[15] These companies are at the forefront of the U.S. effort to develop 5G, but their balance sheets suggest that they may struggle with the cost of a full mmWave network roll-out and the infrastructure it would require.

In the last decade, significant shifts have occurred in the wireless vendor community as well. Chinese telecom equipment giant Huawei grew global revenues from approximately $28B in 2009 to $107B in 2018. Ericsson's revenue during the same period fell from $27.9B to $23.9B,[16] while Nokia's revenue fell from $57.6B to $26.6B.[17] Chinese handset vendors like Huawei, ZTE, Xiaomi, Vivo, and Oppo have grown market share from less than approximately 6% in 2009 to over 30% share in 2018, and are still growing rapidly despite minimal sales in the U.S. market - for example, India represents a wireless market larger than that of the United States, and 59.7% of all handsets sold in India are Chinese.[18] Chinese internet application companies, led by Baidu, Alibaba, Tencent and new companies like TikTock are growing in influence and revenue. In 2009, all of the top 10 Internet companies by revenue were American. Today, four of the top 10 are Chinese.

These shifts have not just occurred because Chinese equipment is cheaper. In many cases, Chinese equipment is also superior to its Western rivals. Huawei and ZTE have been the leader in massive MIMO radio systems, with 64 transmit and receive elements. Many consider Huawei's P series and Mate Android phones the most advanced phones in the world, and these devices are powered by Huawei's own Hi-silicon division. Alibaba's cloud services are fourth in the world, behind Amazon, Microsoft, and Google, and growing quickly.

---

[14] "Schedule of Outstanding Debt," Verizon, accessed March 20, 2019, https://www.verizon.com/about/investors/schedule-outstanding-debt; "Debt Detail as of December 31, 2018," AT&T, accessed March 20, 2019, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/debt/2018/4q18/Debt_List_4Q18.pdf.

[15] "T-Mobile Outstanding Senior Notes And Credit Facilities – Ratings And Maturity Dates (By Year)," T-Mobile, accessed March 20, 2019, https://investor.t-mobile.com/financial-performance/fixed-income/default.aspx; "Q3 News Release," Sprint, accessed March 20, 2019, https://s21.q4cdn.com/487940486/files/doc_financials/quarterly/2018/Q3/01_Fiscal-3Q18-Earnings-Release-FINAL.pdf.

[16] "Ericsson Revenue," Macrotrends, accessed May 31, 2019, https://www.macrotrends.net/stocks/charts/ERIC/ericsson/revenue.

[17] "Nokia Revenue," Macrotrends, accessed May 31, 2019, https://www.macrotrends.net/stocks/charts/NOK/nokia/revenue.

[18] "Just 2 Companies Control 50% of India's Smartphone Market," The Economic Times, February 15, 2019, https://economictimes.indiatimes.com/tech/hardware/just-2-companies-control-50-of-indias-smartphone-market/articleshow/68007602.cms?from=mdr.

Public Sector: White House

U.S. government interest in 5G has been ramping up over the last decade. In 2016, the White House launched a $400 million Advanced Wireless Research Initiative to promote wireless testing platforms, while the FCC passed its "Spectrum Frontiers" policy in which the United States committed to releasing large quantities of mmWave spectrum for both licensed and unlicensed use.[19] Interest in 5G has increased under the current administration, which has offered up a series of initiatives and directives emphasizing the importance of 5G and to develop a clear roadmap. The current administration supports a private sector-led 5G effort, rather than a government-led nationalized 5G plan.

In September 2018, the White House hosted a 5G Summit, during which industry and government leaders convened to discuss the future direction of 5G, promoting private-public sector collaboration while conceding that the United States had fallen behind in developing and fielding 5G. Shortly after, the White House released the "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," highlighting the need for the United States to lead 5G to promote national security and innovation across the public and private sectors.[20] The memo directed departments and agencies to submit a number of reports on current spectrum usage and future requirements, spectrum reallocation options, and the impact of future technologies on spectrum allocation, and also called for 5G legislative, regulatory, and policy recommendations. On the same day as the Presidential memo, the White House released an article titled "America Will Win the Global Race to 5G", looking at U.S. advantages gained from leading 4G (e.g., increased GDP and job opportunities) and comparing them to the potential benefits of leading 5G.[21]

Public Sector: FCC

The FCC plays a large role in the development and fielding of 5G with regard to spectrum allocation and policy for civil-use spectrum. In late 2018, the FCC held a vote to establish a framework for freeing up mmWave spectrum bandwidth to help expedite 5G development and deployment. The FCC controls U.S. spectrum auctions and held its first 5G spectrum auction in late 2018, which opened up the 28 GHz band. A second auction, held on March 14, 2019, made available the 24 GHz band.

---

[19] The White House, "Fact Sheet: Administration Announces an Advanced Wireless Research Initiative, Building on President's Legacy of Forward-Leaning Broadband Policy," 15 July 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/15/fact-sheet-administration-announces-advanced-wireless-research; Harper Neidig, "White House orders Commerce to develop 5G strategy," *The Hill,* 25 October 2018, https://thehill.com/policy/technology/413121-white-house-orders-commerce-to-develop-5g-strategy.

[20] "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," White House, October 25, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-developing-sustainable-spectrum-strategy-americas-future/.

[21] Michael Kratsios, "America Will Win the Global Race to 5G," White House Office of Science & Technology, October 25, 2018, https://www.whitehouse.gov/articles/america-will-win-global-race-5g/.

The FCC released its comprehensive 5G strategy, "Facilitate America's Superiority in 5G Technology (FAST) Plan," in September of 2018.[22] The plan focuses on three main goals: pushing more spectrum into the marketplace, updating infrastructure policy, and modernizing outdated regulations to facilitate 5G in the United States. With regard to the spectrum goal, the FCC plans to hold three more auctions in 2019 to sell bands of mmWave spectrum, and is conducting research to understand options for opening up low- and mid-band spectrum. With regard to the infrastructure goal, the FCC is working to increase the speed of review for small cells at the federal, state, and local levels to facilitate faster fielding of 5G. With regard to the modernization goal, the FCC is focused on adjusting existing regulations and making new ones to support 5G deployment, such as updating its rules on network equipment to allow for more rapid cell fielding and preventing the sale of network equipment from companies that pose a national security threat to U.S. networks.

The FCC has also started a proceeding to enable more flexible use of the 500 MHz of C-band downlink spectrum, which is positioned in the middle of the 3 and 4 GHz bands.[23] In 2015 at ITU's World Radio Conference, the Obama administration opposed the proposal to reclassify this band as an IMT-2000 allocation suitable for 5G use, which would have paved the way for global standardization of this spectrum for 5G mobility services. Even if the spectrum was reclassified as broadband, it would take some time before existing users could be completely removed from the C band. Sharing the band for 5G mobility use is difficult because mobile handsets emit radio energy in a broad pattern, and numbers of users operating near C band antenna could materially cause interference to satellite reception. However, fixed operations could share the spectrum through the use of highly directional antennas or beamforming systems, and this type of equipment would be ideal for providing fixed services to rural areas, as well as possible DoD uses for fixed network extensions.

If the United States were to aggressively pursue sharing and eventual reallocation of the C-band downlink spectrum, it could allow a second round of 5G spectrum expansion that could give the United States a boost in speed and coverage. However, the benefits of this spectrum reallocation would depend on global companies building their devices to operate within C-band, and the United States would need to push for acceptance of that part of the spectrum as a globally utilized band.

Public Sector: Department of Commerce

The Commerce Department's National Telecommunications and Information Administration (NTIA) manages federal-use spectrum allocation. The Department of Commerce is currently developing a "National Spectrum Strategy" to improve spectrum management, identify research and development priorities to create new technologies, and aggregate federal agencies' spectrum operational needs.[24] NTIA will work with members of a new Spectrum Strategy Task Force (established by the Presidential memo) in a multiyear effort to develop and implement this

[22] "The FCC's FAST Plan," FCC, accessed March 20, 2019, https://www.fcc.gov/5G.
[23] "FCC Expands Flexible Use of Mid-band Spectrum," FCC, July 13, 2018, https://www.fcc.gov/document/fcc-expands-flexible-use-mid-band-spectrum.
[24] Neidig, "White House orders Commerce to develop 5G strategy."

national strategy and align research, development, testing, and evaluation efforts.[25] If DoD were to share its spectrum, it would have to work closely with NTIA to manage that sharing process.

[25] McCabe, "White House directs task force to come up with 5G wireless strategy," *Axios*, October 25, 2018, https://www.axios.com/white-house-national-wireless-strategy-task-force-5g-5e884590-8a4b-4b12-9c16-a1b6401f84ad.html.

CHAPTER 3: DoD DEVELOPMENT AND ADOPTION OF 5G TECHNOLOGY

5G Impact on DoD

While much of the discussion around 5G revolves around the commercial sector as the driving force behind its rollout, 5G ecosystems of technology can equally revolutionize DoD operations, networks, and information processes. DoD must be able to communicate, engage, and operate faster to keep up with the changing environment. 5G will enable this new concept of operations, allowing larger volumes of data to be shared in close to real time across geographically dispersed systems. Currently, data sharing at that scale cannot be completed effectively with legacy communication networks. Existing networks will benefit by leveraging lower latency and higher capacity data transfer capability, but 5G's true potential will be in its impact on the battle network of the future. That network will increasingly include a large number of cheaper, more connected, and more resilient systems to function in a rapidly evolving battlefield.

5G has the capability to combine DoD's current fragmented networks into a single network to promote improved situational awareness and decision-making. This expanded reach will enable new technologies like hypersonic weapons and hypersonic defenses to be deployed, and has the potential to strengthen existing missions like nuclear C3. At an enterprise level, 5G can vastly improve day-to-day tasks such as logistics and maintenance, elevating the efficiency and speed of work across DoD.

However, 5G also presents a serious potential risk for DoD going forward. When operating overseas in the future, the vast majority of these networks and systems may depend on 5G infrastructure. If China leads the field in 5G infrastructure and systems, then the future 5G ecosystem will likely have Chinese components embedded throughout. This would pose a serious threat to the security of DoD operations and networks going forward. Additionally, the growth in the number of connected devices increases the potential "attack surface" for adversaries to target across DoD networks, which will require increased vigilance and security across systems. The larger volume of data being transferred will complicate this task, as it will make it more difficult to detect malicious traffic on a network.

Pivot to Sub-6 GHz

The United States may choose to continue down the path of mmWave, but the rest of the world is focused on building out sub-6 infrastructure, with China in the lead. As a government entity that operates overseas, DoD will ultimately have to learn to operate on that sub-6 infrastructure, regardless of how the United States chooses to implement 5G domestically. For this reason, the United States must invest in sub-6 capabilities and take steps to share its spectrum. However, there are legitimate concerns within DoD that opening up sub-6 spectrum will create a number of operational issues, from spectrum optimization to security vulnerabilities. If DoD operators are forced to share their bands of the spectrum, there are concerns that this may temporarily or permanently reduce the performance of systems. The addition of commercial users would also increase the overall congestion of the sub-6 spectrum, increasing the risk of connectivity interruptions for DoD operators.

However, if the United States and DoD do not pivot to sub-6, DoD will face further challenges with acquisition and practical deployment of 5G. Although mmWave components are typically more compact than sub-6 components, mmWave requires many more base stations positioned within close proximity of one another to maintain connection (and even then, there is still the risk that interference such as objects moving in front of the base station or weather will interrupt the connection). This quickly becomes logistically impractical if a person or platform has to carry multiple antennae, particularly at the fighting edge. Additionally, the DoD acquisition system is slow-moving and might take years to deploy the necessary systems for a mmWave network, at which point most of those systems might already be obsolete. Both DoD and the FCC are currently prioritizing mmWave over sub-6 mid-band spectrum with a particular focus on the 28 and 37 GHz bands, but this is a fundamentally flawed focus due to the impracticality of mmWave deployment. DoD must prepare to operate in a sub-6 5G ecosystem, which will require a shift in strategy and a consideration of where DoD is willing to share bandwidth in the sub-6 realm.

This shift may come with some inherent benefits. The anonymity that comes from utilizing the same infrastructure as any other company or country provides an industry-standard form of security all its own. Integration of government and civil use may provide a layer of security by allowing military traffic to "hide in plain sight" as traffic becomes more difficult to see and isolate. Similarly, adversaries might be deterred from jamming this spectrum because they might be operating on the same bands. Government will maintain primary spectrum access while also benefiting from technology advancements from the commercial sector that result from operations in the sub-6 range, which will help the government to close the gap between the commercial sector and current state of military communications. This also creates an opportunity for cyber and communications personnel to learn how to make spectrum more resilient by working regularly with shared spectrum and managing it both domestically and abroad.

A Path Forward for Sub-6 Spectrum Sharing

The idea of spectrum sharing is not new. In 2010, the FCC identified the spectrum band from 3550-3700 MHz, known as Citizens Broadband Radio Service (CBRS), as a potential spectrum-sharing opportunity. CBRS utilizes LTE networks to provide wireless voice, text, and data services, and this spectrum was freed as a result of the FCC's 2010 National Broadband Plan to provide more spectrum for new mobile users.[26] In 2015, the FCC formally authorized the 3.5 GHz band for shared wireless access in an area that was previously utilized by the U.S. Navy and DoD. CBRS will enhance the "last mile" of fiber access to deliver fixed wireless service and also offer point-to-multipoint capabilities. CBRS spectrum can be unlicensed by the user, or they may purchase temporary licenses for periods of use, and it allows services to be deployed in a more rapid and efficient manner. DoD remains the incumbent user of the band, so other users will be limited by the Spectrum Access System (SAS), which ensures that there is deconfliction

[26] "National Broadband Plan," FCC, March 17, 2010, https://www.fcc.gov/general/national-broadband-plan.

to remove interference with military use. SAS gives DoD priority in the band, but keeps the band open for commercial users when not occupied.

This precedent may serve as a guide for future spectrum sharing between DoD and the commercial sector. By offering up its own bandwidths to share, DoD can also encourage a system of "bi-directional" spectrum sharing in which civil and federal users could access one another's spectrum with varying prioritization. This would increase the amount of spectrum available to DoD on a secondary level, while maintaining priority access in its own bandwidths. Additionally, DoD stands to gain significant benefits from 5G development, for reasons listed at the beginning of this chapter. DoD may have some initial growing pains as it begins to share parts of the spectrum, but the net gain in capability from 5G will ultimately make up for that inconvenience. If DoD does not begin to share the sub-6 spectrum, it will increase the risk of dependence on a compromised supply chain as U.S. companies will be blocked from developing and competing their own sub-6 5G offerings, and foreign providers will increasingly embed their offerings in networks and systems globally.

Security Challenges in 5G

Supply Chain Risks

DoD is facing a future 5G environment where its supply chain will be increasingly vulnerable or compromised, from the subcomponent level to the integrated network level, as well as the services associated with each. In previous decades, DoD was able to operate on bespoke systems that fulfilled its unique requirements due to its position as a large user relative to the rest of the commercial world, but that privilege no longer exists. Commercial sector tech development and usage dwarfs that of DoD, and it is no longer practical for DoD to build and operate on siloed, bespoke systems and architecture. As a result, DoD is increasingly dependent on commercial off-the-shelf (COTS) equipment and commercial services, and the same will hold true for the future 5G ecosystem.

DoD can incorporate commercial inputs into its 5G infrastructure at four levels: the RF component, the integrated chipset, the device, and the service. RF components can include subcomponents ranging from semiconductors to switches and amplifiers. Integrated chipsets combine various subcomponents and other subsystems to interface with system components on a motherboard. Devices can range from mobile handsets to fixed computer systems, which include both the subcomponents and integrated chipsets listed above. Finally, each of these inputs comes with a set of service offerings to operate, manage and maintain them.

Commercial companies can supply any and all of the above inputs, but this comes with the risk of inadvertent or malicious security vulnerabilities that put DoD systems and networks at risk. The 5G ecosystem will especially run the risk of including security vulnerabilities if China becomes the global leader supplying 5G infrastructure from the subcomponent-level to the integrated system-level, for even if the United States limits sales of Chinese products into the United States, DoD will still have to operate on foreign networks overseas that will likely be built with a Chinese supply chain.

DoD has made the shift from bespoke to commercial-reliant computing systems over the past decade, but this change in approach carried less risk than is currently faced because the United States dominated the computing systems market and was able to "own" the supply chain and better secure it against vulnerabilities. As a result, DoD now incorporates varying degrees of COTS products into its computing systems while keeping vulnerability risk at an acceptable level. However, in the current 5G competition, neither DoD nor the United States writ large is in a position to dictate the content and integration of the 5G supply chain - our focus on building a mmWave 5G ecosystem leaves us out of the global supply chain for the sub-6 5G ecosystem. This mismatch will create serious security risks for DoD going forward if the rest of the world accepts Chinese products as the cheaper and superior option for 5G.

5G Infrastructure and Services

5G networks have a number of security risks to consider, regardless of what spectrum bands they operate in. While DoD security typically focuses on vendor-installed backdoors that could be used to remotely control a system or exfiltrate information, a wide variety of security issues could also be introduced through poor software development practices both during and after the rollout of 5G. Many of these risks were mentioned in a UK report on the joint effort with Huawei and the UK government to manage security issues with Huawei deployments in the UK.[27] Security issues from poor software development issues are a universal problem, and are not restricted to only Chinese vendors.

Even if the security of a particular release of software for a 5G base station may be secure and well-implemented, there is no guarantee that future releases will continue to be equally secure. Bugs will inevitably be found and require software patches, and these fixes may need to be fielded quickly without fully considering new security issues that might be introduced with the patch. It will become increasingly challenging to validate continued security with each iteration.

Even if base station code is secure and well-managed over time, the business model of the wireless infrastructure providers is such that personnel from the vendor are typically involved in the commissioning, operation, and maintenance of network infrastructure. This requires vendors to access core management systems that operate the network, and allows vendors to deploy software to equipment in the system. In many cases, network operators both in and out of the United States outsource entire operations of the network to the vendor of the equipment, increasing potential vulnerabilities via this third party activity.

Field maintenance is also typically contracted back to the vendor. Service staff visiting field sites are able to upload new software to the network and change network configurations. DoD has a long history of combating malware that has been transmitted into weapons systems through computers that were not patched, did not have multi-factor authentication, or were exposed to

[27] "Huawei Cyber Security Official Oversight Board Annual Report 2019," March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

security breaches through bad usage practices by personnel.[28] All of these issues and more apply to vendor maintenance computers. These support systems are rarely examined by security engineers, and yet they may be equipped with credentials that give them powerful abilities to insert vulnerabilities into the infrastructure.

Radio access network (RAN) vendors often dictate choices of core network infrastructure that manages traffic over backhaul links and across national fiber networks. They also provide core authentication services, the ability to perform legal intercepts, name server functionality and interconnection with the Internet. This control derives from vendor use of non-standard techniques to communicate and manage base stations and the overall radio network. As a result, an operator may have difficulty choosing non-Huawei core infrastructure for Huawei base stations. Multi-vendor networks are typically configured as islands of common vendor equipment, and if a vendor is found to have serious security issues, replacing that vendor in the infrastructure may require a near-complete rebuilding of the network.

5G core infrastructure has additional issues from functionalities like network "slicing" that exposes the network to non-operators. For example, if a virtual reality headset requires a managed slice of network infrastructure to communicate with a cloud-based gaming service, this increases the attack surface of the core network by enabling signaling and control to edge- and cloud-based compute entities.

5G Devices

In addition to 5G network infrastructure, DoD must also consider security risks associated with 5G devices. If the current trends of rising Chinese dominance in the wireless device market continues, Chinese vendors will continue to grow in market share and in sophistication, even if denied access to the U.S. market due to their device popularity with the rest of the world. To the extent U.S. forces deployed overseas use these devices, either for official business or for personal uses, DoD will have to address issues caused by their use.

Evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally. Many of these seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information about domestic users. In a recent case, Nokia android handsets were discovered to have a backdoor that sent a variety of data to a network server located in the network of China Telecom.[29] Nokia had deliberately built this code into devices sold into China, but had then accidentally installed it onto all its other devices. In 2018, software from XIONGMAI, a Chinese camera vendor that manufactures security cameras, was found to have to an undocumented backdoor user named "tluafed" ("default" in reverse) that could access millions of cameras. This is believed to be related to a hash

[28] "Weapon System Cybersecurity, GAO, October 2018, https://www.gao.gov/assets/700/694913.pdf.
[29] Jerry Hildenbrand, "How does a phone maker 'mistakenly' collect user data and ship it off to a server in China?" androidcentral, March 23, 2019, https://www.androidcentral.com/how-does-company-nokia-or-oneplus-mistakenly-collect-user-data-and-ship-it-server-china.

algorithm in the software development library provided by Huawei for its HiSilicon SOC, on which the camera is based.[30]

These and other incidents indicate that Chinese agencies may mandate backdoor access to devices shipped into China to aid their internal surveillance activities. Because of the nature of software development environments, it is difficult to maintain separate sets of code bases with some code options only compiled and installed on devices shipped to specific destinations. When those devices are shipped outside of China, those backdoors can still be used to exfiltrate information.

We can only speculate whether or not the spread of these security vulnerabilities is intentional or inadvertent. However, if Chinese policy does require backdoor access embedded in devices sold in China for internal security purposes, this compromised code applied to such a large market increases the risk that these vulnerabilities will spill over into the rest of the world. If China dominates the market for 5G devices, both as a manufacturer and as a large and attractive market of users, then this potential for vulnerabilities will only continue to spread and put the larger 5G ecosystem at risk.

[30] "Millions of XIONGMAI Video Surveillance Devices Can Be Hacked Via Cloud Feature," SEC Consult, accessed March 31, 2019, https://sec-consult.com/en/blog/2018/10/millions-of-xiongmai-video-surveillance-devices-can-be-hacked-via-cloud-feature-xmeye-p2p-cloud/.

CHAPTER 4: BOARD RECOMMENDATIONS FOR 5G

Board Recommendations

The Defense Innovation Board bases its recommendations on the assumption that mmWave fundamentally cannot be deployed on a large scale in the United States because of the propagation and cost limitations, and that sub-6 GHz mid-band spectrum (in the 3 and 4 GHz range) will become the global standard for broad area networks in coming years. This assumption is based on an assessment of the engineering requirements for mmWave and various studies projecting the required infrastructure and associated cost to support even a limited mmWave network. Additionally, the current financial state of U.S. providers may inhibit their ability to invest the required capex to support a mmWave network, limited or otherwise.

Recommendation #1

DoD needs to make a plan for sharing sub-6 GHz spectrum to shape the future 5G ecosystem, including an assessment of how much and which bandwidths need to be shared, within what timeframe, and how that sharing will impact DoD systems.

- **DoD and the FCC must flip their prioritization from mmWave to sub-6 GHz spectrum for 5G**. DoD and FCC have been prioritizing the 28 and 37 GHz bandwidths as options for 5G development, but this effort is misplaced. This study has covered the broad range of limitations associated with mmWave, and reasons why the rest of the world will adopt a sub-6 GHz 5G ecosystem. In light of this, DoD must prepare itself for that future operating environment by focusing on co-existing, if not explicitly sharing, with civil 5G operations in those bands of spectrum.

- **DoD should particularly focus on the bands of the sub-6 GHz spectrum that are already being used by China**. Chinese 5G systems and infrastructure operate in the 3.2-3.6 GHz range, as well as the 4.8-5.0 GHz range. As a result, the commercial world has developed semiconductors and handsets that are configured for that range, and DoD should angle for the most developed market to expedite 5G sub-6 GHz deployment in the United States. It takes approximately two years to add new frequency bands to complex multiband transceivers, and the United States would be able to avoid those two years of development by leveraging subcomponents and devices already on the market for more mature spectrum usage, such as existing Qualcomm products with functionality in the bands leveraged by China.

- As an additional consideration, **DoD currently occupies ~500 MHz of space in the 4 GHz spectrum.** DoD should take action to share parts of this space, given that it is a material amount of bandwidth that could make a serious impact on 5G development. 5G functions most optimally on large amounts of consecutive bandwidth, and this range could provide the real estate to drive 5G development forward.

  **For more detailed options around DoD spectrum sharing, see Classified Annex.*

- For additional spectrum availability, DoD should recommend that the NTIA, FCC and Department of State should **advocate the reallocation of the C-band satellite spectrum to IMT-2000 5G use** at the World Radio Conference later this year (WRC-19), and take measures to adopt sharing in all 500 MHz of the band in the United States on an accelerated basis for fixed operations. While this will have limited impact on the U.S. 5G mobile ecosystem, sharing in this band could provide broad coverage at 100 Mbps and above for **fixed broadband service** to a large section of the rural United States.

- **DoD should encourage other government agencies to incentivize industry to adopt a common 5G network for sub-6 deployment**. Incentives can include: accelerated depreciation, tax incentives, low interest loans and government purchase of equipment and services.

- **This recommendation does not call for the eviction of DoD systems operating in the sub-6 GHz spectrum, nor does it call for the sharing of ALL DoD spectrum.** DoD must conduct thoughtful but candid analyses of the cost and schedule associated with sharing different spectrum bands, and prioritize accordingly.

- However, DoD must bear in mind that **the status quo of spectrum allocation is unsustainable**. 5G capability requires larger bands of spectrum, and without that additional bandwidth, the United States will not gain true 5G capability beyond the limited range that mmWave can provide. **In the next year, DoD is in the position to enable or inhibit 5G adoption in the United States based on its use of sub-6 GHz spectrum.**

- DoD stands to significantly benefit if it shares some of its sub-6 GHz spectrum. As the commercial sector develops and deploys 5G technologies and networks, DoD will be able to **leverage commercial innovations** to build its own new and improved technologies and networks. At a strategic level, 5G can create a **step-change in situational awareness and decision-making** by integrating more systems into a network that shares more data faster and at lower latency.

- This effort will require **close coordination with NTIA** to clear and reassign spectrum. Timing is critical - it is not enough to simply share spectrum, it must be done quickly to keep the United States competitive with China, South Korea, and Japan.

- **Without aggressive action as outlined in this report, we believe there is a high likelihood that the United States will be unable to convince the rest of the world to adopt mmWave technologies as the standard 5G pathway.** This may bifurcate the global market and result in the majority of the world adopting 5G sub-6 technologies, which will be dominated by the Chinese equipment and handset manufacturers.

Recommendation #2

DoD must prepare to operate in a "post-Western" wireless ecosystem. This plan should include R&D investments towards system security and resiliency on an engineering and strategic level.

- Sharing parts of the sub-6 spectrum will certainly help the U.S. 5G effort, but gaining a competitive edge over China would require action at a rate and magnitude previously unseen within DoD. For this reason, it is probable that most of the world outside of the United States will adopt a sub-6 5G solution, forcing DoD to operate on a "post-Western" wireless ecosystem. In this event, **DoD should assume that all network infrastructure will ultimately become vulnerable to cyber-attack from both an encryption and resiliency standpoint.**

- **DoD must adopt a "zero-trust" network model.** Perimeter defense models have been proven to be ineffective, and 5G will only exacerbate this problem as more systems are linked into a common network. Information access should no longer be granted simply through attachment to a specific network, and instead should be granted through various security checks within the network. DoD should also plan to move to quantum-resistant key exchange mechanisms to deal with the eventual fall of public key exchange algorithms, particularly given China's investments in quantum computing.

- While "zero-trust" networks can protect context exchange through cryptography, these exchanges will still be subject to traffic analysis and detection of surges in network utilization. **DoD should work to keep large amounts of data flowing on a constant basis so that increases in operational tempo will not be noticed.**

- In addition to these security precautions, DoD must brace for cyber-attack and penetration by **improving resiliency and building in layers of redundancy throughout its networks** to ensure uninterrupted connectivity**.**

- DoD will need to consider options for defending against a compromised supply chain, where Chinese semiconductor components and chipsets are embedded across multiple systems. DoD should invest in R&D to study the impact of compartmentalizing systems to limit an attacker's ability to move laterally into other systems. This will come with performance costs, and **DoD must find the line where it can balance baseline capability with security.**

- **DoD should advocate for aggressive protection of U.S. technology intellectual property rights (IPR) in an effort to slow down China's telecommunications ecosystem expansion.** The United States should leverage export controls to slow the rate of market loss for Western vendors, even if it may increase the pace at which China becomes self-sufficient.

- **DoD will increasingly be driven to operate on shared commercial networks without their own bespoke infrastructure** (as in the case of nuclear C3). DoD must analyze the risks and benefits associated with that shift, and **adjust its concept of operations to account for it.**

  **For a more detailed assessment of 5G impact on nuclear C3, see Classified Annex.*

- DoD needs to consider the broader implications of a compromised supply chain, such as risk to personal devices and information that can be derived from activity on those

devices. If China is able to collect this data, **DoD should consider discrete directives to defend against these vulnerabilities that fall outside the traditional DoD systems and platforms**, such as training to limit inadvertent sharing of PII through personal device use.

- In addition to these efforts, **DoD should initiate testing and experimentation on its bases for future generations of wireless technology beyond 5G**. This testing and experimentation will occur over a longer timeframe to ensure that the United States is prepared to lead the next generational transition. These activities can include testing for sub-6 sharing, as well as future mmWave deployment and propagation improvement.

Recommendation #3

DoD should advocate for adjusted trade policies to discourage vulnerabilities in its supply chain on the grounds that they put national security assets and missions at risk.

- The **compromised supply chain issue** poses a serious threat to national security by introducing vulnerabilities into networks and systems, which can be leveraged by a hostile actor to disrupt DoD operations. The spread of these vulnerabilities creates an increasingly unstable environment by lowering barriers to offensive action while weakening defensive positions.

- The proliferation of security vulnerabilities creates incentives for all nations to take offensive action in a conflict, as the barrier to offense decreases while the difficulty of defense increases. This reality is reflected in the new U.S. Cyber doctrine of “forward defense”.

- To counter this threat, DoD should advocate that trade policy **reward good security/coding and penalize vulnerabilities through tariffs** (“monetization” of good development practices). For example, the United States could automatically impose a heavy tariff (say, 75%) on any goods **from any nation** found to have backdoors or serious security vulnerabilities. This would impose a market cost for insecurity, and would also create incentives for domestic companies to fund security researchers to find vulnerabilities in competitors’ products, thereby triggering the tariff. This would improve the overall security of DoD ecosystems without having to disclose vulnerabilities found by Title 50 entities.

- The United States should **encourage Five Eyes and NATO partners to adopt the same tariffs,** regardless of product country of origin. The United States stands to benefit the most in a trade conflict over security of devices.

- DoD should also encourage CFIUS to **block transactions of companies with a history of selling products with documented backdoors and security vulnerabilities.**

- Additionally, the United States should continue to **encourage partner nations to secure their own supply chains** and deny access to Chinese state-owned enterprises (SOEs) selling 5G wares.

  **For more information on Chinese 5G strategy and current state, see Classified Annex.*

Recommendation #4

See Classified Annex.

SEMICONDUCTORS: THE FOUNDATION OF MODERN TECHNOLOGY

Semiconductors form the foundation for nearly all modern technologies. They have transformed our lives and our economy for the better and are giving rise to the technologies that will shape our future. They have the unique distinction of being all around us, yet mostly unseen. They are embedded in the digital goods we depend on for communication, transportation, healthcare, business, national security, and countless other applications.

"Continual advancement of semiconductor technologies during the past 50 years in accordance with Moore's Law – which posits that the overall processing power of computers will double every two years – has been a key driver of the information technology revolution that underpins many U.S. economic and security advantages."

Worldwide Threat Assessment of the U.S. Intelligence Community (May 2017)

Semiconductors were invented in America, and the U.S. still leads the world in leading-edge semiconductor research, design, and manufacturing. **U.S. semiconductor companies commanded nearly half of the $469 billion global semiconductor market in 2018.**

Advancements in semiconductor technology have been measured by "Moore's Law," the observation that the number of transistors on an area of silicon will double roughly every 18 to 24 months. For more than 50 years, the ability of the semiconductor industry to maintain this rapid pace of innovation has propelled a technology revolution through massive increases in computing power at lower costs.

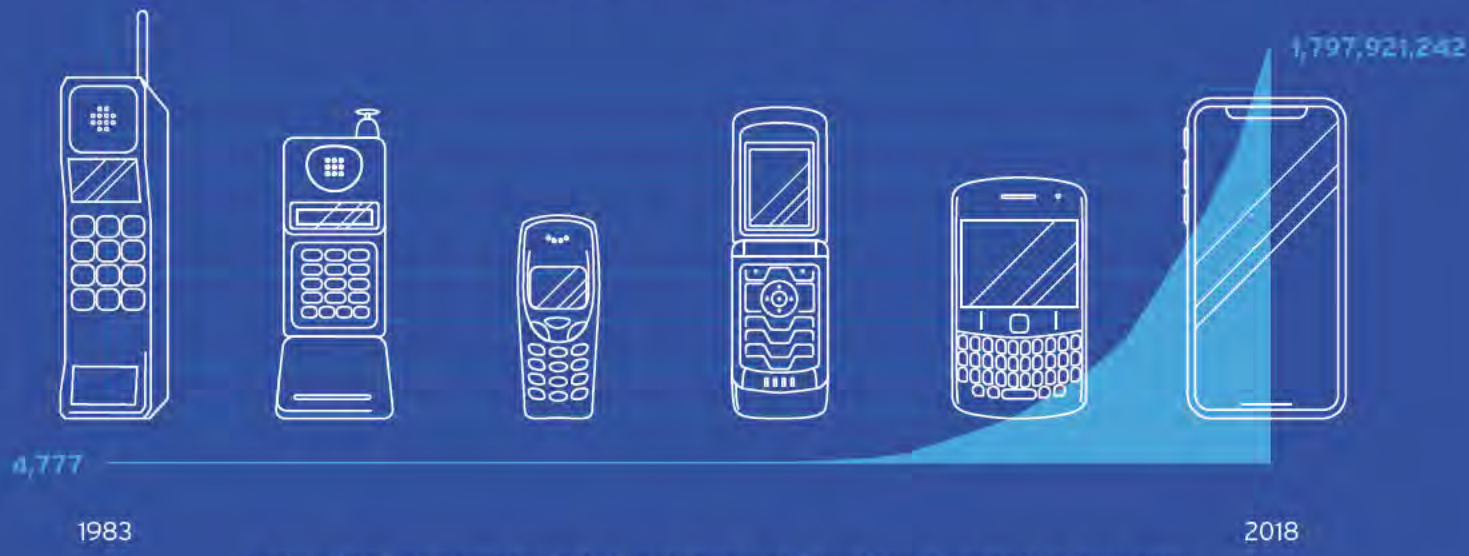
The industry has followed Moore's Law to levels once unimaginable, pushing the limits of material science, photonics, engineering, and design. Today's semiconductors have billions of transistors on a chip the size of a square centimeter, and circuits are measured at the nanoscale. Leading-edge semiconductors contain transistors **10,000 times thinner than a human hair**. As a result of dramatic advancements in semiconductor technology, consumers have benefitted from more innovative products at lower prices. This rapid pace of innovation has boosted America's economy, created U.S. jobs, and transformed our very way of life for the better.

To maintain our innovation trajectory for the next 50 years and win the competition for global leadership in the technologies of the future, the U.S. must lead the world in semiconductor innovation.

The U.S. has a positive trade balance in semiconductors with virtually all our major trading partners, including China, and provided a net surplus of $4.5 billion to the overall trade balance in 2018.

DRIVING UNPARALLELED INNOVATION THROUGH MOORE'S LAW

THE AVERAGE NUMBER OF TRANSITORS ON A SINGLE SEMICONDUCTOR



Innovation has propelled a technology revolution through massive increases in computing power at lower costs. The first cellphones went on sale in the U.S. in 1983 for almost $4,000 each. Today, phones with exponentially higher computing power are affordable to most.

CHALLENGES TO CONTINUED INNOVATION AND U.S. LEADERSHIP IN SEMICONDUCTOR TECHNOLOGY

The breathtaking pace of semiconductor innovation over decades is at risk from technology barriers and ambitious efforts by overseas competitors, bolstered by government investment.

The industry's ability to advance semiconductor technology is pushing against barriers of physics, and breakthroughs to move beyond these limits are constrained by massive capital costs.

In addition, while America leads the world with nearly half of global market share, overseas governments are seeking to displace U.S. leadership through huge government investments in both commercial manufacturing and scientific research. For example, the Chinese government has announced efforts to invest well over $100 billion over the next decade to catch up to the United States in semiconductor technology, artificial intelligence, and quantum computing. While China may not meet all its goals, the size and scale of its effort should not be ignored.

These challenges and others pose risks to American leadership in semiconductor design, research, and manufacturing and our position in the global race for the technologies that will define our future. Semiconductors enable the key "must-win" technologies of the future, including artificial intelligence to power self-driving cars and other autonomous systems, quantum computing to analyze massive volumes of data and enhance digital encryption, and advanced wireless networks to seamlessly connect people at unprecedented speeds. These core technologies will fuel future innovations in other fields essential to future economic growth, such as personalized healthcare, robotics, and intelligent products.

SEMICONDUCTORS AND THE 'MUST-WIN' TECHNOLOGIES OF THE FUTURE

The future economy will be characterized by technologies that use sensors to collect immense amounts of data, networks to store and move the data, and advanced computers and systems to analyze and use the data in productive ways. **Semiconductors are core to each of these functions**, and we must make further advances in semiconductor technology to meet the needs of the technologies of the future.

THE ROLE OF SEMICONDUCTORS IN HARNESSING THE TECHNOLOGIES OF THE FUTURE

Artificial Intelligence

Artificial intelligence refers to technologies that imitate human learning and decision-making. AI has the potential to dramatically transform the economy. It will be critical to autonomous vehicles, machine learning, and countless "smart" devices and applications. Experts have estimated that **artificial intelligence could add $13 trillion to global economic output by 2030.**

Without advances in semiconductor process technology and chip design, AI could not have moved so rapidly from futuristic speculation to present-day reality. Indeed, semiconductors are critical in all three areas of a typical AI process flow: 1) data generation or data source through smartphones, automobiles, and multiple "Internet of Things" devices; 2) training the AI/deep learning algorithms using graphics processors, microprocessors, or other heavy performance-centric processors; and 3) AI inference in real-world uses.

"The United States must drive technological breakthroughs in AI across the federal government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security."

- President Donald Trump, Executive Order on Maintaining American Leadership in Artificial Intelligence (Feb. 11, 2019)

Quantum Computing

Quantum computing promises to magnify the power of computers exponentially. **A quantum computer is 100 million times faster than a personal computer and thousands of times faster than existing supercomputers.** Achieving this level of computing power would transform entire industries and sectors of the economy.

The very development of quantum information sciences is closely linked with the semiconductor industry's research to overcome the computing power limitations of Moore's Law. Academic and government researchers have made advances in quantum computing in tandem, or in partnership, with the semiconductor industry.

Quantum computing requires sophisticated fabrication capabilities, specialized materials, and advanced technologies. Quantum hardware researchers believe that advances in quantum computing could help researchers working to answer difficult questions in the most widely used fields of AI and machine learning.

"Quantum information science (QIS) applies the best understanding of the sub-atomic world – quantum theory – to generate new knowledge and technologies. Through developments in QIS, the United States can improve its industrial base, create jobs, and provide economic and national security benefits."

- National Science and Technology Council, "National Strategic Overview for Quantum Information Science" (September 2018)

Advanced Wireless Networks

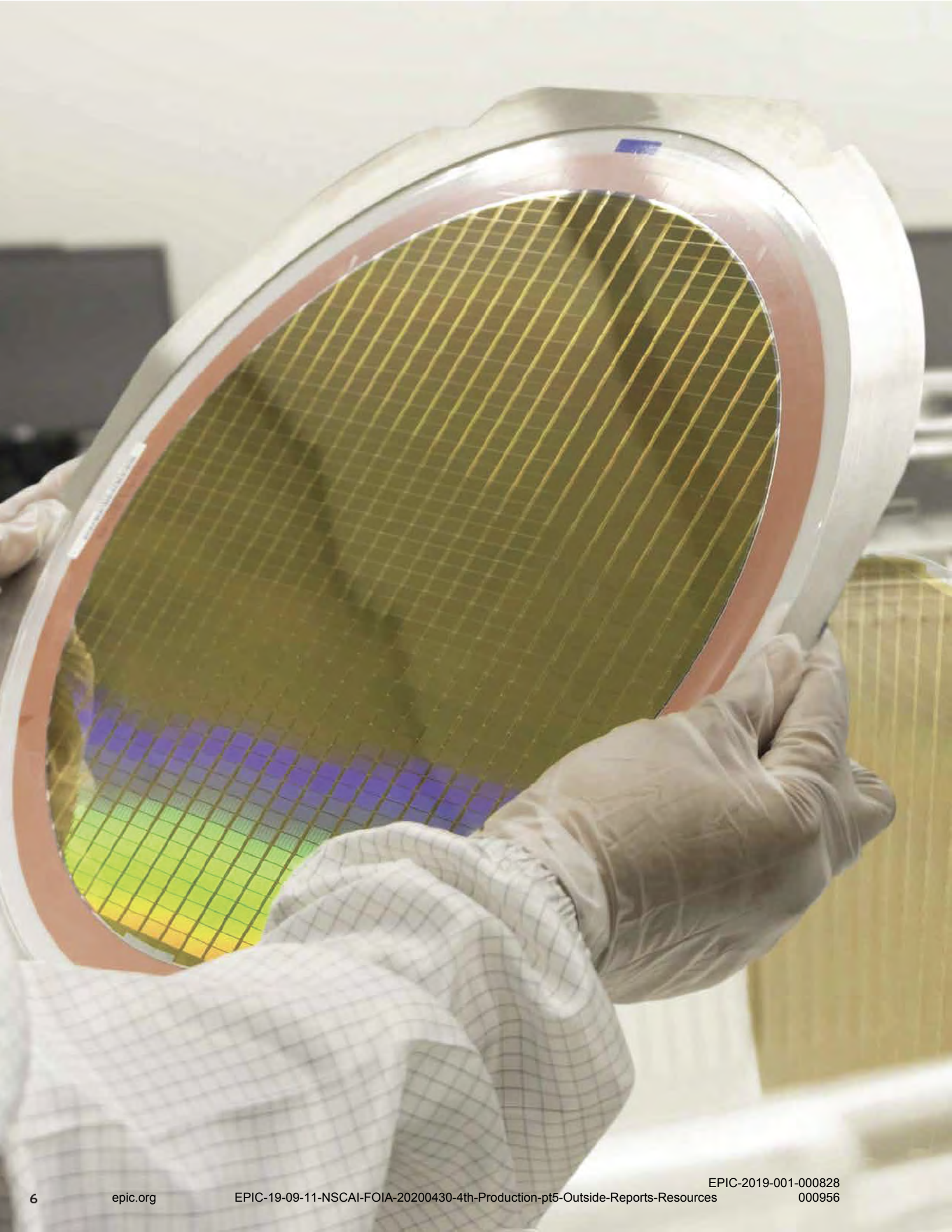
With promised low latency and ultra-high speeds up to 100 times faster than current networks, advanced wireless networks will be the foundation for the new economy and provide the backbone for the next generation of digital technologies, such as the Internet of Things, autonomous vehicles, and robotics – all paired with robust mobility.

Because of the huge promise of advanced network speeds and their entirely new architectures, the full potential of the underlying semiconductor hardware solutions has not yet been realized. **The nation that achieves advancements in semiconductor technology for next-generation wireless networks, such as 5G and beyond, will reap significant economic benefits.**

Leading in advanced wireless networks requires a national policy that augments the R&D efforts of the semiconductor industry, builds up the engineering and tech workforce, and supports both private and public R&D. NSF supports fundamental research in wireless data and advanced wireless networks. It also funds testbeds and research platforms for prototyping advanced wireless network systems using an array of research infrastructure programs at U.S. universities through the Platform for Advanced Wireless Research.

"Wireless communications and associated data applications establish a foundation for high wage jobs and national prosperity."

- Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future (October 2018)



THREE POLICIES TO ENSURE U.S. LEADERSHIP IN SEMICONDUCTOR TECHNOLOGY

The strategy to sustain and strengthen U.S. semiconductor leadership consists of three overarching policy initiatives:

1. **Invest in research** that will promote American semiconductor innovation.
2. **Attract and develop a skilled workforce** that will ensure U.S. leadership in semiconductor research, design, and manufacturing and in the development and implementation of future growth technologies.
3. **Ensure access to global markets and protect intellectual property** so the U.S. semiconductor industry can compete, innovate, and grow in the future.

By implementing these policies, Congress and the Administration would be taking key steps to protect American leadership in semiconductor technology and win the global competition for the technologies of the future. Implementing these policies will help steer America toward a future of innovation leadership and economic growth, while also bolstering our national security.

1 INVEST IN SEMICONDUCTOR RESEARCH

To make breakthroughs in the key technologies expected to drive future economic growth and to maintain American leadership in the face of global competition, the U.S. needs to invest ambitiously in semiconductor research. Unfortunately, federal investment in research has been declining or been flat for many years. In contrast, key competitors are dramatically increasing their research spending, including targeted investments in semiconductor research. **The U.S. risks losing its innovation edge and the global competition for technology leadership if under-investment persists.**

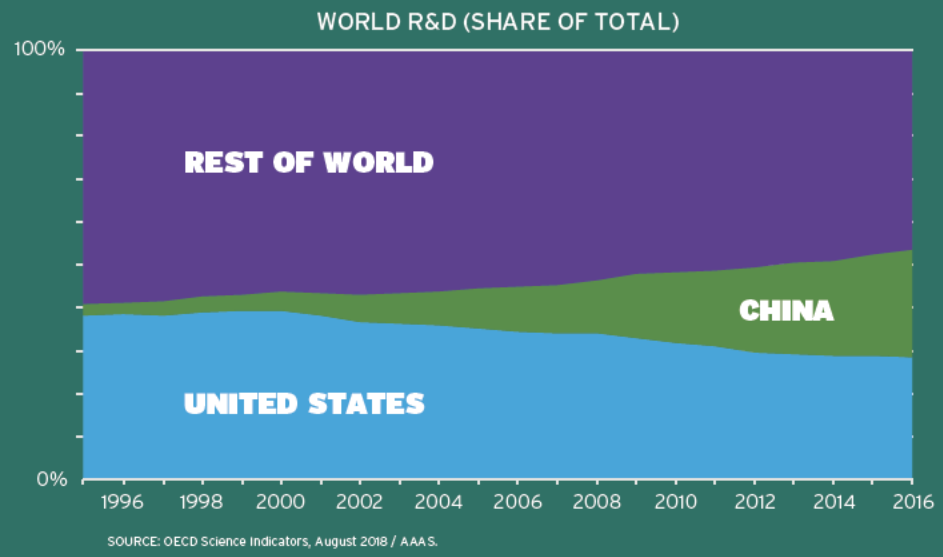
The U.S. semiconductor industry already invests heavily in its own research and development to stay competitive and maintain its technology leadership. Nearly one-fifth of U.S. semiconductor industry revenue is invested in R&D, amounting to approximately $36 billion in 2017, triple the amount invested 20 years ago.[1] This is among the highest shares of any industry, and the vast majority of this research is conducted in the U.S. The industry's investment is primarily targeted at applied research and product development, not the basic research needed for long-range, fundamental technology breakthroughs. To supplement this private-sector commitment, the U.S. needs to increase federal investments at universities, national labs, and other entities to maintain our leadership in this critical industry.

The decades-long success of Moore's Law was driven by research investments in materials and chemicals sciences, computer science and applied math, electrical engineering, and fabrication technologies. Continued semiconductor innovation will require research in new materials, designs, and architectures through a whole-of-government approach and public/private partnerships to apply the best research from academia, industry, and government research centers.[2]

The U.S. semiconductor industry annually invests approximately one-fifth of revenue in research and development, amounting to approximately $36 billion in 2017. This is among the highest R&D investment rates of any industry.

DECLINING FEDERAL SUPPORT FOR RESEARCH – A RISK TO AMERICAN LEADERSHIP

The federal scientific enterprise is a crown jewel of American society, yielding countless innovations that have contributed to U.S. economic strength and national security. Unfortunately, federal investment in research has been declining in comparison to our global competitors.



SOURCE: OECD Science Indicators, August 2018 / AAAS.

RESEARCH POLICY RECOMMENDATIONS

We urge Congress and the Administration to:

- **Triple U.S. investments in semiconductor research** across federal scientific agencies from approximately $1.5 billion to $5 billion annually to advance new materials, designs, and architectures that will exponentially increase chip performance. The federal government currently invests approximately $1.5 billion in research programs specifically focused on the semiconductor industry. These programs fund critical research in nanoelectronics, security, energy efficiency, and other important areas. To meet current technology challenges and keep up with global competition, funding of these semiconductor research programs should be tripled over the next 5 years.
- **Double U.S. research investments in semiconductor-related fields such as materials science, computer science, engineering, and applied mathematics** across federal scientific agencies to spur leap-ahead innovations in semiconductor technology that will drive key technologies of the future, including artificial intelligence, quantum computing, and advanced wireless networks. Semiconductor advances also benefit from programs addressing broader fields of scientific inquiry that span the range of the U.S. scientific enterprise. Research programs in areas such as materials science, computer science, engineering, applied mathematics, photonics, and chemistry are essential to future innovations in semiconductor technology. Funding for these programs should be doubled over the next 5 years.

Increased research funding alone, however, will not meet the challenges without increased engagement with industry. **The federal government plays an essential convening role and must drive public-private research partnerships that not only increase the general scientific research knowledge base, but also connect that knowledge to real-world applications.** Doing so is necessary to ensure scientific breakthroughs benefit society and sustain American leadership in semiconductor technology that is key to national security and industrial competitiveness.

RESEARCH – DEVELOPING THE PIPELINE OF TALENT

In addition to providing the foundation for technological innovation, investments in research also support the "pipeline" of talent for the next generation of semiconductor innovators. Given the critical importance of developing a high-skilled, high-knowledge workforce that can continue advancement in semiconductor technology, research funding is an important component of facilitating an innovative workforce in the U.S.

2 ATTRACT AND DEVELOP A SKILLED WORKFORCE

To maintain global semiconductor industry leadership and ensure America wins the worldwide race to develop and implement the technologies of the future, the U.S. needs a highly skilled workforce.

Leadership in semiconductor research, design, and manufacturing requires access to the best and brightest scientists and engineers from around the world. In the global race for talent, the U.S. educational system is failing to produce a sufficient number of American workers and students with the necessary STEM expertise to meet the needs of the semiconductor industry and other technology fields. As a result, allowing top minds from abroad to fill open jobs in the U.S. is critical to the U.S. semiconductor industry. **Every highly educated immigrant who stays and works in the U.S. creates nearly three additional American jobs,**[3] and many of America's most innovative companies – including several leading U.S. semiconductor companies – were founded and led by immigrants.

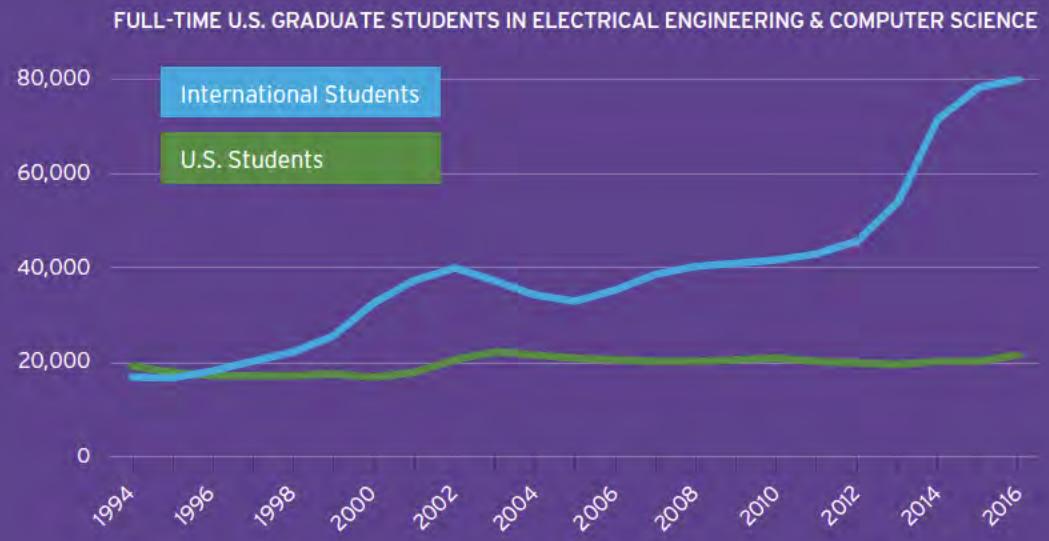
The U.S. is also falling behind its global competitors in most education benchmarks. China is producing many more bachelor's degrees in STEM fields. At the graduate level – which generates the expertise in materials science, physical chemistry, electrical engineering, and other fields of importance to the semiconductor industry – a large percentage of students in relevant fields at U.S. colleges and universities are from foreign countries. In electrical engineering and computer science graduate degree programs at U.S. colleges and universities, the NSF indicates that approximately 80 percent of students are from foreign countries, a rapidly increasing trend.

The U.S. needs a comprehensive long-term plan to attract young students – **particularly underrepresented women and minorities** – to science and engineering and expose them to work in labs, advanced manufacturing, and apprenticeships.

The semiconductor industry directly employs nearly a quarter of a million workers in the U.S. and supports more than one million additional jobs in the U.S., with major manufacturing operations in 19 states.

AMERICA'S TALENT CHALLENGE

International students make up a growing share of science and engineering graduate students at U.S. institutions, outnumbering their American counterparts by a ratio of nearly four to one.



SOURCE: National Science Foundation, National Center for Science and Engineering Statistics, Graduate Students and Postdoctorates in Science and Engineering Survey.

WORKFORCE POLICY RECOMMENDATIONS

We urge Congress and the administration to:

- **Reform the high-skilled immigration system by eliminating counterproductive caps on green cards** so qualified STEM graduates from U.S. colleges and universities, as well as STEM graduates from around the world, can work, innovate, and contribute to U.S. leadership in the semiconductor industry and boost our economy. Foreign nationals in STEM fields, particularly those with advanced degrees, should be automatically eligible to work in the U.S. and contribute to our economy.
- **Increase U.S. investments in STEM education by 50 percent and implement a national STEM education initiative** to double the number of American STEM graduates by 2029. Policymakers should support apprenticeships and training programs and work with industry and academia to develop curricula to match the needs of growing technologies that are critical to the future of the semiconductor industry, such as artificial intelligence, quantum computing, and advanced wireless networks.

3 ENSURE ACCESS TO GLOBAL MARKETS AND PROTECT INTELLECTUAL PROPERTY

Free and fair access to global markets is essential to the industry's success. **Semiconductors are America's fourth-largest export, contributing positively to America's trade balance for the past 20 years.** More than 80 percent of revenues of U.S. semiconductor companies are from sales overseas. Revenue from global sales sustains the 1.25 million semiconductor-supported jobs in the U.S., and is vital to supporting the high level of research and development necessary to remain competitive. Additionally, most of this R&D is conducted in the United States. The semiconductor industry relies on a complex and global supply chain for raw materials, equipment, R&D, technology, human talent, testing, and distribution.[4] As a result, continued access to global markets and supply chains is critical for continued U.S. industry leadership.

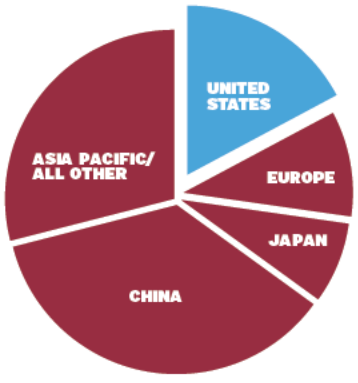
All phases of the semiconductor value chain – research, design, manufacturing, assembly, and packaging – occur in a globally integrated network. The semiconductor industry in the U.S. has leveraged this global network to maintain its competitiveness, and it is a key aspect of the industry's success.

Today, the global semiconductor ecosystem is under threat from government policies that seek to localize supply chains and build state-backed national champions to compete abroad. These policies employ massive state subsidies, top-down approaches, centrally planned industrial policies, and other non-market efforts, including forced technology transfer and intellectual property theft. They also have the potential to disrupt markets and harm innovation. While China stands out today, there are fears this "supply-chain localization" trend will spread to other nations. **America's global leadership of the semiconductor industry can be maintained only by promoting access to global markets and ensuring fair competition.** In addition, all nations have an interest in maintaining this global value chain. The U.S. government should work with like-minded nations to promote effective trade policies to sustain this critical aspect of our industry.

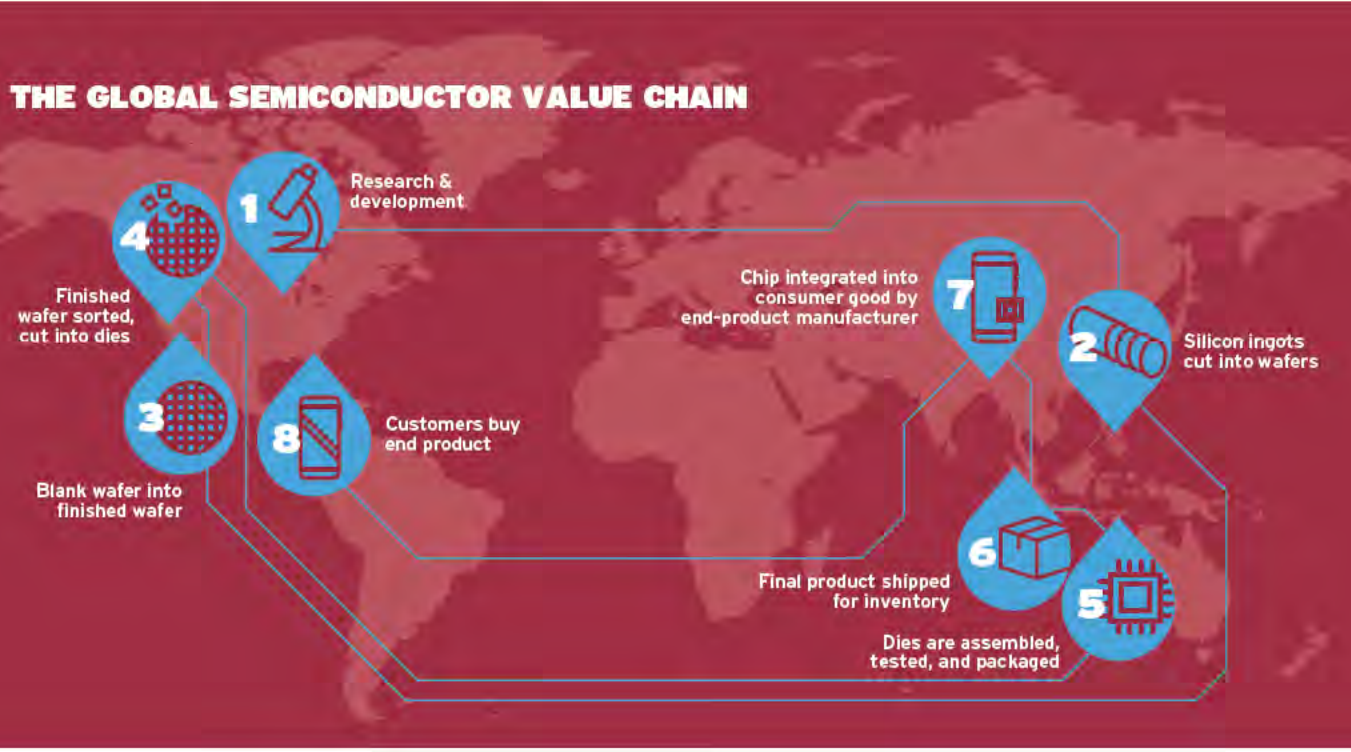
Open markets and fair trade require strong intellectual property protection and enforcement. Intellectual property is the lifeblood of the semiconductor industry, and enforcing intellectual property rights is essential to the industry's global competitiveness. The industry's high level of investment in research and development results in valuable intellectual property (patents, trade secrets, source code, etc.), and protection of this intellectual property is critical to the industry's competitive position in the world.

THE IMPORTANCE OF FREE AND OPEN MARKETS

OVERSEAS MARKETS ACCOUNT FOR OVER 80% OF SALES FOR U.S. SEMICONDUCTOR COMPANIES



SOURCE: World Semiconductor Trade Statistics and SIA



TRADE POLICY RECOMMENDATIONS

We urge Congress and the administration to:

- **Approve and modernize free trade agreements,** including the United States-Mexico-Canada Agreement, that remove market barriers, protect IP, and enable fair competition. U.S. policymakers should expand access to global markets and combat discriminatory and market-distorting policies by approving new and updating existing free trade agreements. Modern U.S. trade agreements should:
  - Strengthen safeguards and increase penalties to protect trade secrets and other forms of intellectual property.
  - Ensure access to global markets for the most innovative and effective encryption products by eliminating technical barriers to trade.
  - Ensure state-owned or subsidized enterprises compete fairly and transparently based on market considerations, by removing government subsidies that are illegal or lead to adverse effects.
  - Eliminate duties on semiconductor-rich products, applications and electronic transmissions.
  - Prevent forced localization of digital infrastructure and local content requirements.
  - Prohibit forced technology transfer.
  - Simplify and harmonize customs and trade procedures.

  Specifically, we urge approval of the United States-Mexico-Canada Agreement, which includes many new and higher-standard trade disciplines that will strengthen the digital economy and the global semiconductor supply chain.
- **Increase resources for law enforcement and intelligence agencies** to prevent and prosecute semiconductor intellectual property theft, including the misappropriation of trade secrets. Robust intellectual property protection is essential to preserving incentives for innovation.

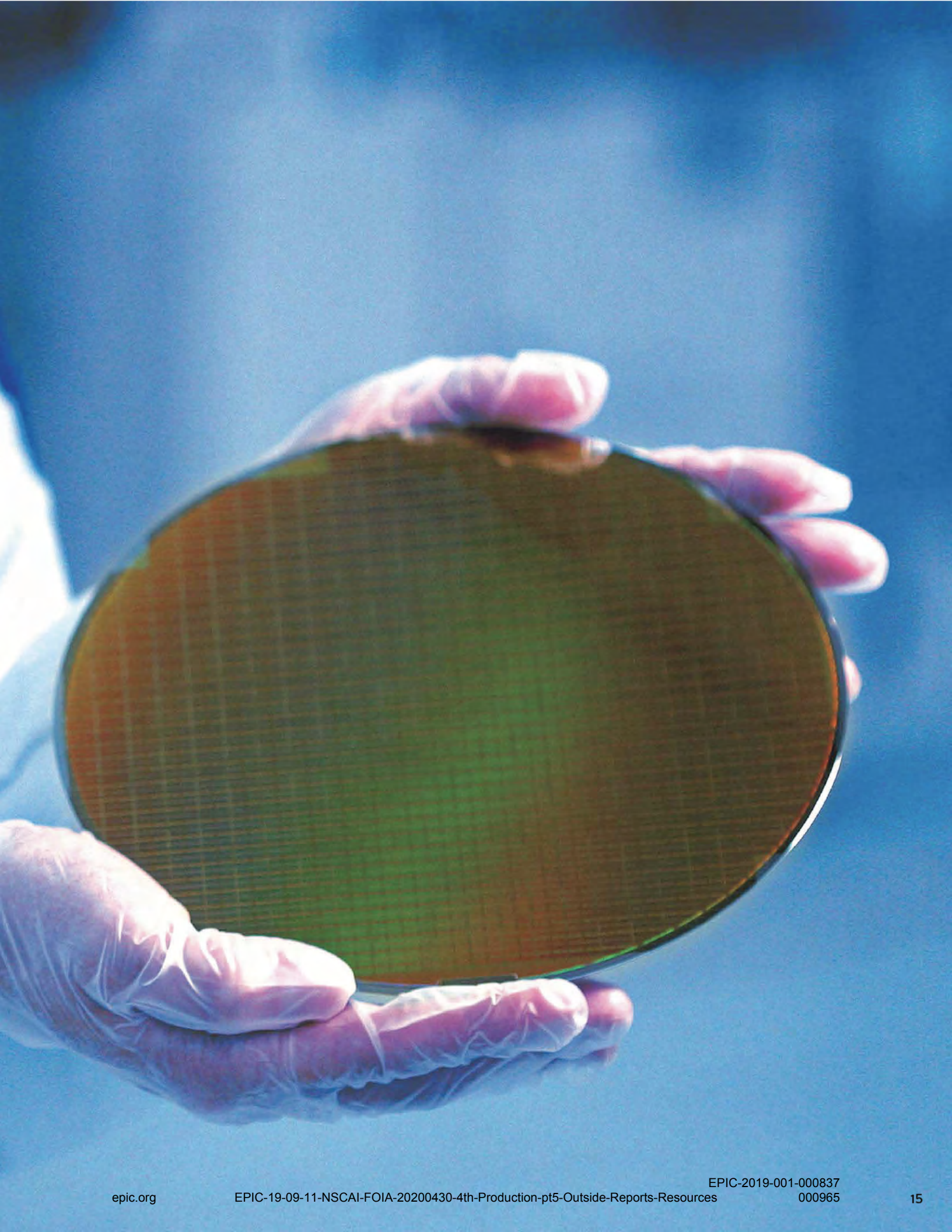
Semiconductors are America's fourth-largest export after aircraft, refined oil, and crude oil.

CONCLUSION

Semiconductors are a key enabling technology that shapes our nation's economy, job creation, technology leadership, and national security. To maintain America's position as the global leader in semiconductor technology, the federal government must establish policies that invest in our innovation base, human talent, and ability to compete globally.

When the U.S. has faced challenges to its leadership in semiconductor technology in the past, it rose to the moment through cooperation and collaboration. In the 1980s, government and industry partnered to form SEMATECH, a far-sighted collaborative effort to maintain U.S. semiconductor industry leadership. SEMATECH is widely regarded as having driven the technological innovations of that era by making strategic research investments and building the semiconductor workforce.[5] The effort was further advanced by the opening of global markets and supply chains, leading to the unparalleled growth and innovation that we have today.

The U.S. now faces a similar challenge to its industry leadership, and government, academia, and industry must again work together to overcome it. The obstacles we face today are different than those of the past, so this moment calls for strategic thinking and fresh solutions to achieve our common goal of continued U.S. semiconductor leadership.



ENDNOTES

1 SIA Factbook https://www.semiconductors.org/resources/2018-sia-factbook/ (2018)

2 More detail on the research agenda for the semiconductor industry is available at "Semiconductor Research Opportunities: An Industry Vision and Guide" (March 2017). https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-SRC-Vision-Report-3.30.17.pdf and Office of Science, Department of Energy, "Basic Research Needs for Microelectronics" (February 2019), https://science.energy.gov/~/media/bes/pdf/reports/2018/Microelectronics_Brochure.pdf

3 Help Wanted: The Role of Foreign Workers in the Innovation Economy. http://www.renewoureconomy.org/sites/all/themes/pnae/stem-report.pdf

4 Beyond Borders – The Global Semiconductor Value Chain: How an Interconnected Industry Promotes Innovation and Growth. https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Beyond-Borders-Report-FINAL-June-7.pdf

5 For more information about the role of SEMATECH in the 1980s, please see "Rising to the Challenge: U.S. Innovation Policy for the Global Economy," National Research Council of the National Academies, National Academies Press, 2012, pages 324-353. https://www.nap.edu/catalog/13386/rising-to-the-challenge-us-innovation-policy-for-the-global

winthefuture.tech

National Science Foundation
Office of the Director

July 11, 2019

Personnel Policy on Foreign Government Talent Recruitment Programs

Background

Basic research is one of the underpinnings of America's ability to sustain its position as an innovation leader, its economic strength, and its national security. Openess, transparency, and collaboration are essential for basic research. These are the values that have driven NSF and its global research partners since our inception.

However, open scientific exchange and research faces a challenge from programs sponsored by some foreign governments or affiliates, sometimes referred to as "foreign government talent recruitment programs." In general, such programs disregard intellectual and other proprietary rights, and reflect *foreign state-sponsored attempts to acquire U.S. funded scientific research through foreign government run or funded recruitment programs* that target scientists, engineers, academics, researchers, and entrepreneurs of all nationalities working or educated in the United States. Foreign government talent recruitment programs threaten to compromise the values of openness, transparency, collaboration, and integrity of science and engineering research.

These foreign government talent recruitment programs differ greatly from the international scientific research collaborations in which NSF actively participates. Productive international scientific research collaboration relies on reciprocal scientific exchange for mutual benefit, which NSF continues to pursue and which is vital to our mission. NSF is working with the scientific community, our federal partners, and other stakeholders to understand the challenges of talent recruitment programs. The goal is to protect researchers and the public while continuing to promote collaboration and innovation.

This policy provides guidance about the obligations of NSF personnel and IPAs with respect to foreign government talent recruitment programs.[1]

---

[1] Distinguishing features of a foreign government talent recruitment program covered by this policy include:
(a) Compensation provided by the foreign state to the targeted individual in exchange for the individual transferring knowledge and expertise to the foreign country. The compensation can take several forms, such as cash, research funding, honorific titles, career advancement opportunities, promised future compensation, or other types of remuneration or other consideration.
(b) Recruitment refers to the foreign state sponsor's active engagement in attracting the targeted individual to join the foreign-sponsored program and transfer their knowledge and expertise to the foreign state. The targeted individual may be employed and located in the United States, or in the foreign state. Note that, generally, an invitation by a foreign state to simply attend or present work at an international conference would not constitute recruitment.

Obligations of NSF Personnel and IPAs

As a longstanding obligation of public service, NSF personnel (all NSF employees, including Federal temporary employees; employees appointed under the Visiting Scientist, Engineer, and Educator Program (VSEE); fellows; students; and intermittent experts), as well as Intergovernmental Personnel Act (IPA) assignees have a responsibility to the United States Government and its citizens to place loyalty to the U.S. Constitution, laws, and ethical principles above private gain (5 CFR § 2635.101(a)). Employees of the Federal Government may not accept employment, gifts, or compensation from any foreign government, including any entity which is owned or operated by the foreign government, which may include public research institutions or universities. This prohibition is found in the "emoluments clause" of the U.S. Constitution (Article I, Section 8, Clause 8).

NSF personnel and IPAs must adhere to the following principles of ethical conduct, per Executive Order 12674, as amended by Executive Order 12731:

1) Public service is a public trust, requiring NSF personnel and IPAs to place loyalty to the Constitution, the laws, and ethical principles above private gain.
2) NSF personnel and IPAs shall not hold financial interests that conflict with the conscientious performance of duty.

There is a risk that participation in foreign government talent recruitment programs by NSF personnel and IPAs will compromise these ethical principles. Such participation poses significant risks of inappropriate foreign influence on NSF policies, programs, and priorities, as well as risk to the integrity of NSF's merit review process and to U.S. national interests.

Policy

To mitigate these risks, NSF personnel employed at and IPAs detailed to NSF are not permitted to participate in foreign government talent recruitment programs. NSF personnel and IPAs must comply with this policy. Failure to do so could result in disciplinary action up to and including removal from Federal Service and referral to the Office of Inspector General. Any questions regarding this policy and whether an affiliation with a foreign government falls within the definition of foreign government talent recruitment programs should be directed to the NSF Designated Agency Ethics Official.

Summary of the

2018
National Defense Strategy

of

The United States of America

Sharpening the American Military's Competitive Edge

Table of Contents

INTRODUCTION

The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win. Reinforcing America's traditional tools of diplomacy, the Department provides military options to ensure the President and our diplomats negotiate from a position of strength.

Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.

China is a strategic competitor using predatory economics to intimidate its neighbors while militarizing features in the South China Sea. Russia has violated the borders of nearby nations and pursues veto power over the economic, diplomatic, and security decisions of its neighbors. As well, North Korea's outlaw actions and reckless rhetoric continue despite United Nation's censure and sanctions. Iran continues to sow violence and remains the most significant challenge to Middle East stability. Despite the defeat of ISIS's physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly.

This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation's history. In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force. America's military has no preordained right to victory on the battlefield.

This unclassified synopsis of the classified *2018 National Defense Strategy* articulates our strategy to compete, deter, and win in this environment. The reemergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict require a Joint Force structured to match this reality.

A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order. Collectively, our force posture, alliance and partnership architecture, and Department modernization will provide the capabilities and agility required to prevail in conflict and preserve peace through strength.

The costs of not implementing this strategy are clear. Failure to meet our defense objectives will result in decreasing U.S. global influence, eroding cohesion among allies and partners, and reduced access to markets that will contribute to a decline in our prosperity and standard of living. Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people.

STRATEGIC ENVIRONMENT

The *National Defense Strategy* acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business.

The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.

China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage. As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future. The most far-reaching objective of this defense strategy is to set the military relationship between our two countries on a path of transparency and non-aggression.

Concurrently, Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor. The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough, but when coupled with its expanding and modernizing nuclear arsenal the challenge is clear.

Another change to the strategic environment is a *resilient, but weakening, post-WWII international order*. In the decades after fascism's defeat in World War II, the United States and its allies and partners constructed a free and open international order to better safeguard their liberty and people from aggression and coercion. Although this system has evolved since the end of the Cold War, our network of alliances and partnerships remain the backbone of global security. China and Russia are now undermining the international order from within the system by exploiting its benefits while simultaneously undercutting its principles and "rules of the road."

Rogue regimes such as North Korea and Iran are destabilizing regions through their pursuit of nuclear weapons or sponsorship of terrorism. North Korea seeks to guarantee regime survival and increased leverage by seeking a mixture of nuclear, biological, chemical, conventional, and unconventional weapons and a growing ballistic missile capability to gain coercive influence over South Korea, Japan, and the United States. In the Middle East, Iran is competing with its neighbors, asserting an arc of influence and instability while vying for regional hegemony, using state-sponsored terrorist activities, a growing network of proxies, and its missile program to achieve its objectives.

Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.

Challenges to the U.S. military advantage represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested—air, land, sea, space, and cyberspace.

We face an ever more lethal and disruptive battlefield, combined across domains, and conducted at increasing speed and reach—from close combat, throughout overseas theaters, and reaching to our homeland. Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression.

The security environment is also affected by *rapid technological advancements and the changing character of war*. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future.

New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.

States are the principal actors on the global stage, but *non-state actors* also threaten the security environment with increasingly sophisticated capabilities. Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption. There is a positive side to this as well, as our partners in sustaining security are also more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership. Terrorism remains a persistent condition driven by ideology and unstable political and economic structures, despite the defeat of ISIS's physical caliphate.

It is now undeniable that the *homeland is no longer a sanctuary*. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Rogue regimes, such as North Korea, continue to seek out or develop *weapons of mass destruction* (WMD) – nuclear, chemical, and biological – as well as long range missile capabilities and, in some cases, proliferate these capabilities to malign actors as demonstrated by Iranian ballistic missile exports. Terrorists likewise continue to pursue WMD, while the spread of nuclear weapon technology and advanced manufacturing technology remains a persistent problem. Recent advances in bioengineering raise another concern, increasing the potential, variety, and ease of access to biological weapons.

DEPARTMENT OF DEFENSE OBJECTIVES

In support of the *National Security Strategy*, the Department of Defense will be prepared to defend the homeland, remain the preeminent military power in the world, ensure the balances of power remain in our favor, and advance an international order that is most conducive to our security and prosperity.

Long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future. Concurrently, the Department will sustain its efforts to deter and counter rogue regimes such as North Korea and Iran, defeat terrorist threats to the United States, and consolidate our gains in Iraq and Afghanistan while moving to a more resource-sustainable approach.

Defense objectives include:

- Defending the homeland from attack;
- Sustaining Joint Force military advantages, both globally and in key regions;
- Deterring adversaries from aggression against our vital interests;
- Enabling U.S. interagency counterparts to advance U.S. influence and interests;
- Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere;
- Defending allies from military aggression and bolstering partners against coercion, and fairly sharing responsibilities for common defense;
- Dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction;
- Preventing terrorists from directing or supporting external operations against the United States homeland and our citizens, allies, and partners overseas;
- Ensuring common domains remain open and free;
- Continuously delivering performance with affordability and speed as we change Departmental mindset, culture, and management systems; and
- Establishing an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.

STRATEGIC APPROACH

A long-term strategic competition requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military. More than any other nation, America can expand the competitive space, seizing the initiative to challenge our competitors where we possess advantages and they lack strength. A more lethal force, strong alliances and partnerships, American technological innovation, and a culture of performance will generate decisive and sustained U.S. military advantages.

As we expand the competitive space, we continue to offer competitors and adversaries an outstretched hand, open to opportunities for cooperation but from a position of strength and based on our national interests. Should cooperation fail, we will be ready to defend the American people, our values, and interests. The willingness of rivals to abandon aggression will depend on their perception of U.S. strength and the vitality of our alliances and partnerships.

Be strategically predictable, but operationally unpredictable. Deterring or defeating long-term strategic competitors is a fundamentally different challenge than the regional adversaries that were the focus of previous strategies. Our strength and integrated actions with allies will demonstrate our commitment to deterring aggression, but our dynamic force employment, military posture, and operations must introduce unpredictability to adversary decision-makers. With our allies and partners, we will challenge competitors by maneuvering them into unfavorable positions, frustrating their efforts, precluding their options while expanding our own, and forcing them to confront conflict under adverse conditions.

Integrate with U.S. interagency. Effectively expanding the competitive space requires combined actions with the U.S. interagency to employ all dimensions of national power. We will assist the efforts of the Departments of State, Treasury, Justice, Energy, Homeland Security, Commerce, USAID, as well as the Intelligence Community, law enforcement, and others to identify and build partnerships to address areas of economic, technological, and informational vulnerabilities.

Counter coercion and subversion. In competition short of armed conflict, revisionist powers and rogue regimes are using corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground. Some are particularly adept at exploiting their economic relationships with many of our security partners. We will support U.S. interagency approaches and work by, with, and through our allies and partners to secure our interests and counteract this coercion.

Foster a competitive mindset. To succeed in the emerging security environment, our Department and Joint Force will have to out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors.

We will expand the competitive space while pursuing three distinct lines of effort:

- First, rebuilding military readiness as we build a more lethal Joint Force;
- Second, strengthening alliances as we attract new partners; and
- Third, reforming the Department's business practices for greater performance and affordability.

Build a More Lethal Force

The surest way to prevent war is to be prepared to win one. Doing so requires a competitive approach to force development and a consistent, multiyear investment to restore warfighting readiness and field a lethal force. The size of our force matters. The Nation must field sufficient, capable forces to defeat enemies and achieve sustainable outcomes that protect the American people and our vital interests. Our aim is a Joint Force that possesses decisive advantages for any likely conflict, while remaining proficient across the entire spectrum of conflict.

Prioritize preparedness for war. Achieving peace through strength requires the Joint Force to deter conflict through preparedness for war. During normal day-to-day operations, the Joint Force will sustainably compete to: deter aggression in three key regions—the Indo-Pacific, Europe, and Middle East; degrade terrorist and WMD threats; and defend U.S. interests from challenges below the level of armed conflict. In wartime, the fully mobilized Joint Force will be capable of: defeating aggression by a major power; deterring opportunistic aggression elsewhere; and disrupting imminent terrorist and WMD threats. During peace or in war, the Joint Force will deter nuclear and non-nuclear strategic attacks and defend the homeland. To support these missions, the Joint Force must gain and maintain information superiority; and develop, strengthen, and sustain U.S. security relationships.

Modernize key capabilities. We cannot expect success fighting tomorrow's conflicts with yesterday's weapons or equipment. To address the scope and pace of our competitors' and adversaries' ambitions and capabilities, we must invest in modernization of key capabilities through sustained, predictable budgets. Our backlog of deferred readiness, procurement, and modernization requirements has grown in the last decade and a half and can no longer be ignored. We will make targeted, disciplined increases in personnel and platforms to meet key capability and capacity needs. The *2018 National Defense Strategy* underpins our planned fiscal year 2019-2023 budgets, accelerating our modernization programs and devoting additional resources in a sustained effort to solidify our competitive advantage.

- *Nuclear forces*. The Department will modernize the nuclear triad—including nuclear command, control, and communications, and supporting infrastructure. Modernization of the nuclear force includes developing options to counter competitors' coercive strategies, predicated on the threatened use of nuclear or strategic non-nuclear attacks.

- *Space and cyberspace as warfighting domains*. The Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.

- *Command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR)*. Investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.

- *Missile defense*. Investments will focus on layered missile defenses and disruptive capabilities for both theater missile threats and North Korean ballistic missile threats.

- *Joint lethality in contested environments*. The Joint Force must be able to strike diverse targets inside adversary air and missile defense networks to destroy mobile power-projection platforms. This will include capabilities to enhance close combat lethality in complex terrain.

- *Forward force maneuver and posture resilience*. Investments will prioritize ground, air, sea, and space forces that can deploy, survive, operate, maneuver, and regenerate in all domains while under attack. Transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that include active and passive defenses will also be prioritized.

- *Advanced autonomous systems*. The Department will invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages.

- *Resilient and agile logistics*. Investments will prioritize prepositioned forward stocks and munitions, strategic mobility assets, partner and allied support, as well as non-commercially dependent distributed logistics and maintenance to ensure logistics sustainment while under persistent multi-domain attack.

Evolve innovative operational concepts. Modernization is not defined solely by hardware; it requires change in the ways we organize and employ forces. We must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking. We must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality.

Develop a lethal, agile, and resilient force posture and employment. Force posture and employment must be adaptable to account for the uncertainty that exists in the changing global strategic environment. Much of our force employment models and posture date to the immediate post-Cold War era, when our military advantage was unchallenged and the primary threats were rogue regimes.

- *Dynamic Force Employment.* Dynamic Force Employment will prioritize maintaining the capacity and capabilities for major combat, while providing options for proactive and scalable employment of the Joint Force. A modernized Global Operating Model of combat-credible, flexible theater postures will enhance our ability to compete and provide freedom of maneuver during conflict, providing national decision-makers with better military options.

  The global strategic environment demands increased strategic flexibility and freedom of action. The Dynamic Force Employment concept will change the way the Department uses the Joint Force to provide proactive and scalable options for priority missions. Dynamic Force Employment will more flexibly use ready forces to shape proactively the strategic environment while maintaining readiness to respond to contingencies and ensure long-term warfighting readiness.

- *Global Operating Model.* The Global Operating Model describes how the Joint Force will be postured and employed to achieve its competition and wartime missions. Foundational capabilities include: nuclear; cyber; space; C4ISR; strategic mobility, and counter WMD proliferation. It comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland.

Cultivate workforce talent. Recruiting, developing, and retaining a high-quality military and civilian workforce is essential for warfighting success. Cultivating a lethal, agile force requires more than just new technologies and posture changes; it depends on the ability of our warfighters and the Department workforce to integrate new capabilities, adapt warfighting approaches, and change

business practices to achieve mission success. The creativity and talent of the American warfighter is our greatest enduring strength, and one we do not take for granted.

- *Professional Military Education (PME)*. PME has stagnated, focused more on the accomplishment of mandatory credit at the expense of lethality and ingenuity. We will emphasize intellectual leadership and military professionalism in the art and science of warfighting, deepening our knowledge of history while embracing new technology and techniques to counter competitors. PME will emphasize independence of action in warfighting concepts to lessen the impact of degraded/lost communications in combat. PME is to be used as a strategic asset to build trust and interoperability across the Joint Forces and with allied and partner forces.

- *Talent management.* Developing leaders who are competent in national-level decision-making requires broad revision of talent management among the Armed Services, including fellowships, civilian education, and assignments that increase understanding of interagency decision-making processes, as well as alliances and coalitions.

- *Civilian workforce expertise.* A modern, agile, information-advantaged Department requires a motivated, diverse, and highly skilled civilian workforce. We will emphasize new skills and complement our current workforce with information experts, data scientists, computer programmers, and basic science researchers and engineers—to use information, not simply manage it. The Department will also continue to explore streamlined, non-traditional pathways to bring critical skills into service, expanding access to outside expertise, and devising new public-private partnerships to work with small companies, start-ups, and universities.

Strengthen Alliances and Attract New Partners

Mutually beneficial alliances and partnerships are crucial to our strategy, providing a durable, asymmetric strategic advantage that no competitor or rival can match. This approach has served the United States well, in peace and war, for the past 75 years. Our allies and partners came to our aid after the terrorist attacks on 9/11, and have contributed to every major U.S.-led military engagement since. Every day, our allies and partners join us in defending freedom, deterring war, and maintaining the rules which underwrite a free and open international order.

By working together with allies and partners we amass the greatest possible strength for the long-term advancement of our interests, maintaining favorable balances of power that deter aggression and support the stability that generates economic growth. When we pool resources and share responsibility for our common defense, our security burden becomes lighter. Our allies and partners provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options. Allies and partners also provide access to critical regions, supporting a widespread basing and logistics system that underpins the Department's global reach.

We will strengthen and evolve our alliances and partnerships into an extended network capable of deterring or decisively acting to meet the shared challenges of our time. We will focus on three elements for achieving a capable alliance and partnership network:

- *Uphold a foundation of mutual respect, responsibility, priorities, and accountability.* Our alliances and coalitions are built on free will and shared responsibilities. While we will unapologetically represent America's values and belief in democracy, we will not seek to impose our way of life by force. We will uphold our commitments and we expect allies and partners to contribute an equitable share to our mutually beneficial collective security, including effective investment in modernizing their defense capabilities. We have shared responsibilities for resisting authoritarian trends, contesting radical ideologies, and serving as bulwarks against instability.

- *Expand regional consultative mechanisms and collaborative planning*. We will develop new partnerships around shared interests to reinforce regional coalitions and security cooperation. We will provide allies and partners with a clear and consistent message to encourage alliance and coalition commitment, greater defense cooperation, and military investment.

- *Deepen interoperability.* Each ally and partner is unique. Combined forces able to act together coherently and effectively to achieve military objectives requires interoperability. Interoperability is a priority for operational concepts, modular force elements, communications, information sharing, and equipment. In consultation with Congress and the Department of State, the Department of Defense will prioritize requests for U.S. military equipment sales, accelerating foreign partner modernization and ability to integrate with U.S. forces. We will train to high-end combat missions in our alliance, bilateral, and multinational exercises.

Enduring coalitions and long-term security partnerships, underpinned by our bedrock alliances and reinforced by our allies' own webs of security relationships, remain a priority:

- *Expand Indo-Pacific alliances and partnerships*. A free and open Indo-Pacific region provides prosperity and security for all. We will strengthen our alliances and partnerships in the Indo-Pacific to a networked security architecture capable of deterring aggression, maintaining stability, and ensuring free access to common domains. With key countries in the region, we will bring together bilateral and multilateral security relationships to preserve the free and open international system.

- *Fortify the Trans-Atlantic NATO Alliance.* A strong and free Europe, bound by shared principles of democracy, national sovereignty, and commitment to Article 5 of the North Atlantic Treaty is vital to our security. The alliance will deter Russian adventurism, defeat terrorists who seek to murder innocents, and address the arc of instability building on NATO's periphery. At the same time, NATO must adapt to remain relevant and fit for our time—in purpose, capability, and responsive decision-making. We expect European allies to fulfill their commitments to increase defense and modernization spending to bolster the alliance in the face of our shared security concerns.

- *Form enduring coalitions in the Middle East.* We will foster a stable and secure Middle East that denies safe havens for terrorists, is not dominated by any power hostile to the United States, and that contributes to stable global energy markets and secure trade routes. We will develop enduring coalitions to consolidate gains we have made in Afghanistan, Iraq, Syria, and elsewhere, to support the lasting defeat of terrorists as we sever their sources of strength and counterbalance Iran.

- *Sustain advantages in the Western Hemisphere*. The U.S. derives immense benefit from a stable, peaceful hemisphere that reduces security threats to the homeland. Supporting the U.S. interagency lead,

the Department will deepen its relations with regional countries that contribute military capabilities to shared regional and global security challenges.

- *Support relationships to address significant terrorist threats in Africa.* We will bolster existing bilateral and multilateral partnerships and develop new relationships to address significant terrorist threats that threaten U.S. interests and contribute to challenges in Europe and the Middle East. We will focus on working by, with, and through local partners and the European Union to degrade terrorists; build the capability required to counter violent extremism, human trafficking, trans-national criminal activity, and illegal arms trade with limited outside assistance; and limit the malign influence of non-African powers.

Reform the Department for Greater Performance and Affordability

The current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive. We must transition to a culture of performance where results and accountability matter. We will put in place a management system where leadership can harness opportunities and ensure effective stewardship of taxpayer resources. We have a responsibility to gain full value from every taxpayer dollar spent on defense, thereby earning the trust of Congress and the American people.

Deliver performance at the speed of relevance. Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting. Current processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter. Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change. Delivering performance means we will shed outdated management practices and structures while integrating insights from business innovation.

Organize for innovation. The Department's management structure and processes are not written in stone, they are a means to an end–empowering the warfighter with the knowledge, equipment and support systems to fight and win. Department leaders will adapt their organizational structures to best support the Joint Force. If current structures hinder substantial increases in lethality or performance, it is expected that Service Secretaries and Agency heads will consolidate, eliminate, or restructure as needed. The Department's leadership is committed to changes in authorities, granting of waivers, and securing external support for streamlining processes and organizations.

Drive budget discipline and affordability to achieve solvency. Better management begins with effective financial stewardship. The Department will continue its plan to achieve full auditability of all its operations, improving its financial processes, systems, and tools to understand, manage, and improve cost. We will continue to leverage the scale of our operations to drive greater efficiency in procurement of materiel and services while pursuing opportunities to consolidate and streamline contracts in areas such as logistics, information technology, and support services. We will also continue efforts to reduce management overhead and the size of headquarters staff. We will reduce or eliminate duplicative organizations and systems for managing human resources, finance, health services, travel, and supplies. The Department will also work to reduce excess property and infrastructure, providing Congress with options for a Base Realignment and Closure.

Streamline rapid, iterative approaches from development to fielding. A rapid, iterative approach to capability development will reduce costs, technological obsolescence, and acquisition risk. The Department will realign incentive and reporting structures to increase speed of delivery, enable design tradeoffs in the requirements process, expand the role of warfighters and intelligence analysis throughout the acquisitions process, and utilize non-traditional suppliers. Prototyping and experimentation should be used prior to defining requirements and commercial-off-the-shelf systems. Platform electronics and software must be designed for routine replacement instead of static configurations that last more than a decade. This approach, a major departure from previous practices and culture, will allow the Department to more quickly respond to changes in the security environment and make it harder for competitors to offset our systems.

Harness and protect the National Security Innovation Base. The Department's technological advantage depends on a healthy and secure national security innovation base that includes both traditional and non-traditional defense partners. The Department, with the support of Congress, will provide the defense industry with sufficient predictability to inform their long-term investments in critical skills, infrastructure, and research and development. We will continue to streamline processes so that new entrants and small-scale vendors can provide cutting-edge technologies. We will also cultivate international partnerships to leverage and protect partner investments in military capabilities.

CONCLUSION

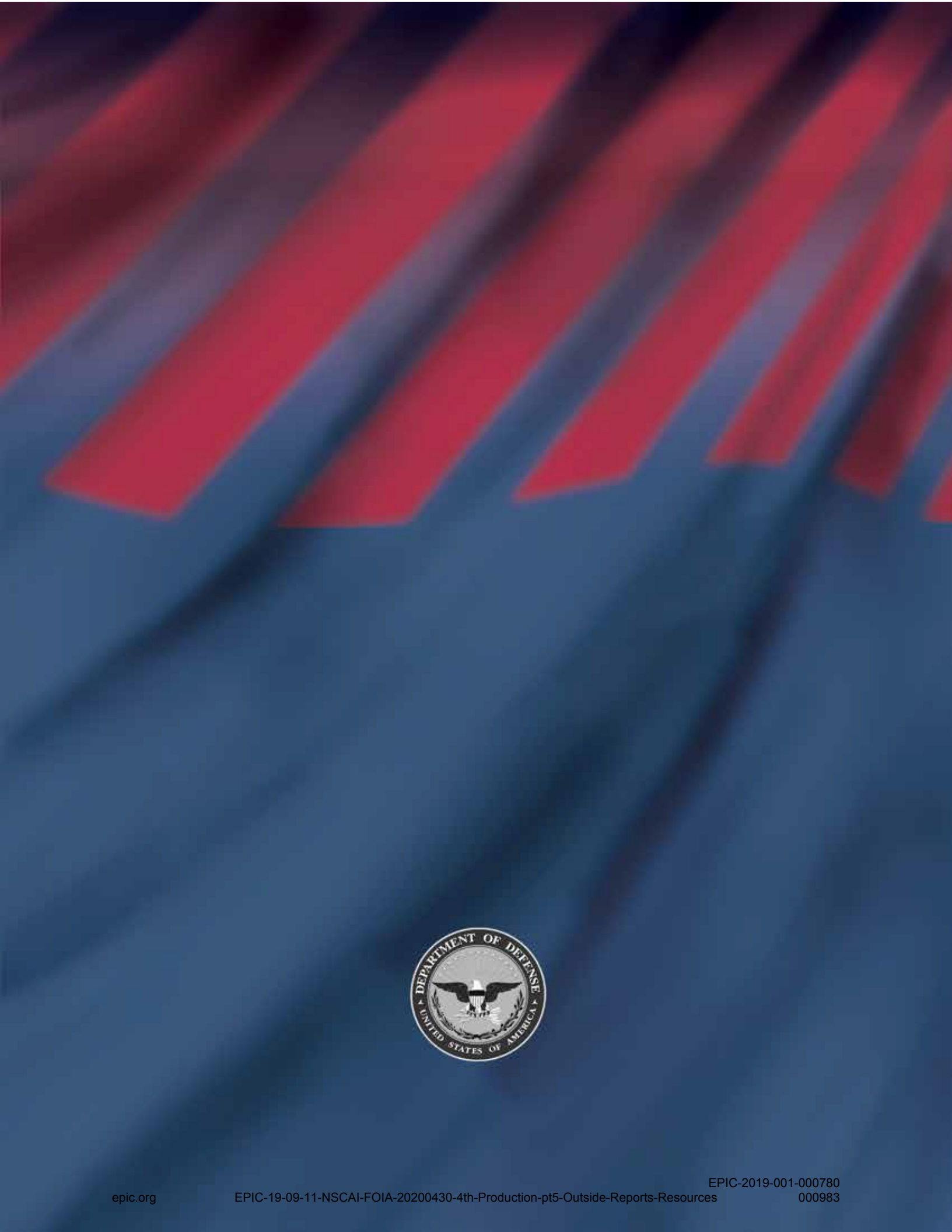
This strategy establishes my intent to pursue urgent change at significant scale.

We must use creative approaches, make sustained investment, and be disciplined in execution to field a Joint Force fit for our time, one that can compete, deter, and win in this increasingly complex security environment. A dominant Joint Force will protect the security of our nation, increase U.S. influence, preserve access to markets that will improve our standard of living, and strengthen cohesion among allies and partners.

While any strategy must be adaptive in execution, this summary outlines what we must do to pass intact to the younger generation the freedoms we currently enjoy. But there is nothing new under the sun: while this strategy will require sustained investment by the American people, we recall past generations who made harsher sacrifices so that we might enjoy our way of life today.

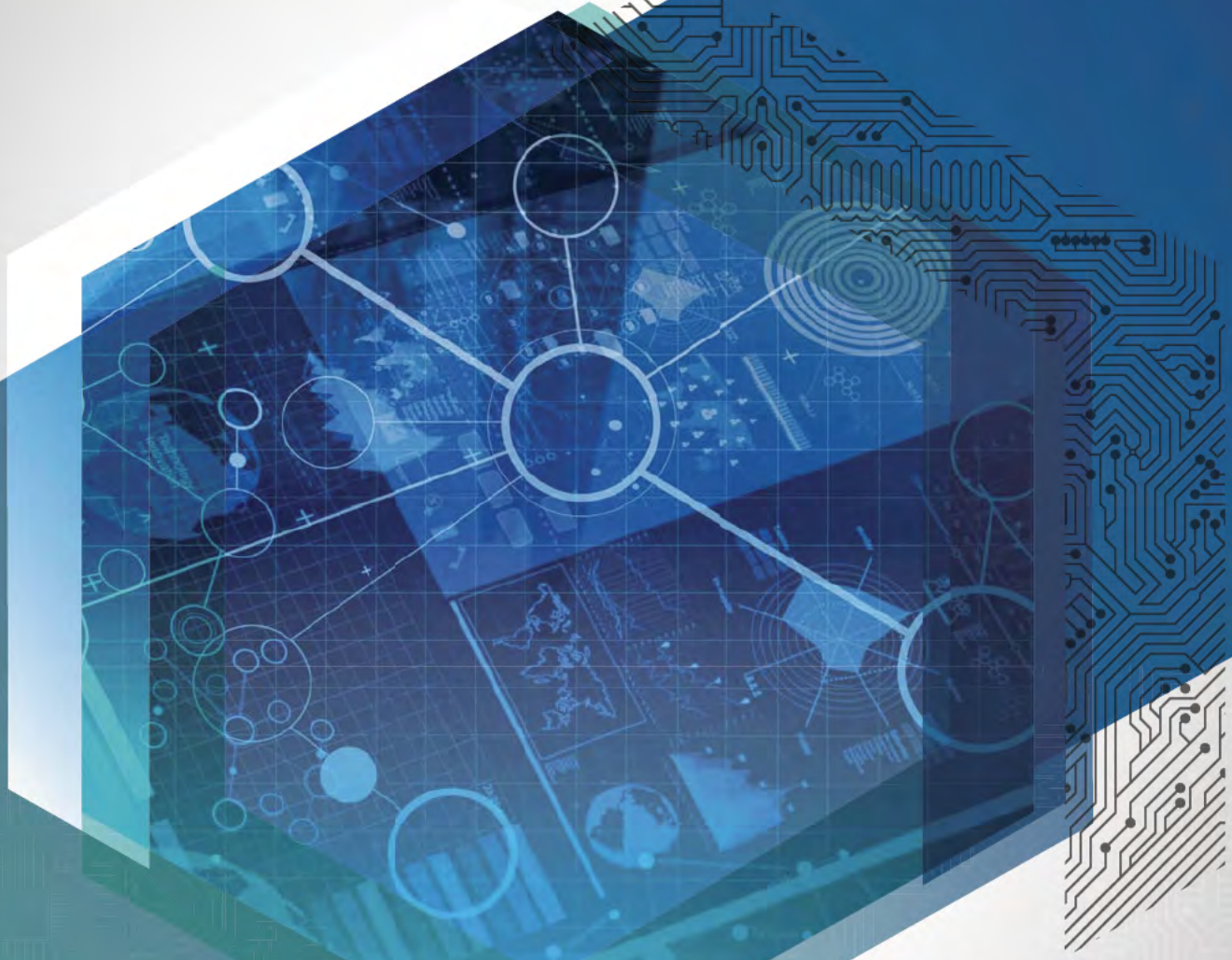
As it has for generations, free men and women in America's military will fight with skill and valor to protect us. To carry out any strategy, history teaches us that wisdom and resources must be sufficient. I am confident this defense strategy is appropriate and worthy of the support of the American people.

Jim Mattis


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

THE AIM INITIATIVE

A STRATEGY FOR AUGMENTING INTELLIGENCE USING MACHINES



Contents

This page intentionally left blank.

THE AIM INITIATIVE

Augmenting Intelligence using Machines Increasing insight
and knowledge through Artificial Intelligence, Automation, and Augmentation

FOREWORD

FROM THE DIRECTOR OF NATIONAL INTELLIGENCE:

Closing the gap between decisions and data collection is a top priority for the Intelligence Community (IC). The pace at which data are generated and collected is increasing exponentially—and the IC workforce available to analyze and interpret this all-source, cross-domain data is not. Leveraging artificial intelligence, automation, and augmentation technologies to amplify the effectiveness of our workforce will advance mission capability and enhance the IC's ability to provide needed data interpretation to decision makers. The Augmenting Intelligence using Machines (AIM) Strategy provides the framework for the incorporation of AIM technologies to accelerate mission capability development across the IC. I challenge the IC workforce, based on the principles outlined in the AIM Strategy, to establish and implement an IC-wide AIM framework, inclusive of mission partners—be big but be practical—to provide real capability to close the gap between decisions being made and data collection.

Dan Coats
Director of National Intelligence

FROM THE PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE:

To meet its vision of ensuring intelligence advantage, the IC must adapt to the rapid global technological democratization in sensing, communications, computing, and machine analysis of data. These trends threaten to erode what were previously unique USIC capabilities and advantages; going forward, we must improve our ability to analyze and draw conclusions from IC-wide data collections at scale. I have identified AIM technologies as key transformative elements that will enable our analytic workforce to effectively leverage the increasing data volume for decision advantage. This document provides the overarching strategy and objectives for effective incorporation of AIM into the IC baseline. I welcome your feedback on this document.

Susan Gordon
Principal Deputy Director of National Intelligence

Executive Summary

It is the job of the IC to analyze data, connect disparate data sets, apply context to data, infer meaning from data, and ultimately make analytic judgments based on all available data. The pace at which data are generated, whether by collection or publically available information (PAI), is increasing exponentially and long ago exceeded our collective ability to understand it or to find the most relevant data with which to make analytic judgments. AIM AAA technologies (Artificial intelligence, process Automation, and IC officer Augmentation) as key transformative elements are crucial for future mission success and efficiency.

This document outlines how the IC will incorporate AIM capabilities in a manner that resolves key IC legal, policy, cultural, technical, and structural challenges while producing optimally effective analytic and operational contributions to the intelligence mission.

Artificial intelligence (AI), especially its sub-discipline machine learning (ML), has shown dramatic advances in autonomous systems, computer vision, natural language processing, and game playing. These AI systems can perform tasks significantly beyond what was possible only recently (e.g., autonomous systems) and in some cases even beyond what humans can achieve (e.g., chess and Go). In light of these recent advances, the IC is carefully considering methods for fully automating well-defined processes and augmenting human expertise with analytics or planning capabilities for their potential benefit. The IC is also monitoring these same technologies with respect to their vulnerabilities in development and adoption. Accordingly, AIM seeks to determine how the IC can best manage uncertainty by achieving acceptable risk suited to the demonstrable analytic and operational advantages in AIM-enabled solutions and tradecraft.

Due to the widespread commercial application of these AI technologies, the private sector is making considerable investments in related infrastructure and people. Therefore, we must carefully monitor and leverage private investment, focus our efforts on areas of unique mission need, and rethink how we attract and retain human expertise. This strategic imperative exists because our adversaries, notably Russia and China, also recognize the potential for AI to transform military and intelligence operations and are investing aggressively to make that advantage a reality.

Individual components of the IC have already recognized the value of AAA technologies. It is the goal of the AIM initiative to bring those disparate efforts together in order to maximize impact and accelerate development. Increases in data volume and velocity are putting pressure on existing workflows, and our adversaries are putting significant effort into AI technologies that can blind or deceive the IC. By adopting AIM, the IC will be able to meet those challenges. This initiative leverages lessons learned from current and past AI efforts; strengthens the collaboration between the IC and industry, research agencies, and academic talent; and grows the talent pool of expertise for the IC. We will continue to expand our interagency approach to AIM development to ensure that the implementation plan we deliver is the IC's plan as opposed to the Office of the Director of National Intelligence's (ODNI) AIM plan for the IC.

The AIM initiative will enable the IC to fundamentally change the way it produces intelligence. We will achieve superiority by adopting the best available commercial AI applications and combining them with IC-unique algorithms and data holdings to augment the reasoning capabilities of our analysts. Simply stated, our goal is the following:

"If it is knowable, and it is important, then we know it." – Sue Gordon

The AIM initiative is an IC-wide strategy for three reasons:

- First, there is intense competition in the private sector for AI and especially ML talent. The IC needs to establish new incentive and hiring models and stop competing internally for the same scarce resources.
- Second, AI and ML systems require large high-quality tagged data sets that must be shared with IC partners to the maximum extent allowable. Rule sets, algorithms, and expert knowledge bases that capture the tacit knowledge of intelligence domain experts must be available to all appropriate and relevant mission areas.
- Third, to rapidly accelerate AI adoption, the IC must have a solid digital foundation. This means leveraging the investment we have already made in the IC Information Technology Enterprise (IC ITE) and continuing to invest in and improve the IC ITE infrastructure.

The AIM initiative has four primary investment objectives:

Objective 1 – Immediate and ongoing – Digital Foundation, Data, and Science and Technical Intelligence (S&TI): AI activities are not a substitute for an enduring, secure, standardized, and measurable IC-wide digital infrastructure and data ecosystem; they are dependent on that foundation. In addition, the IC must improve foundational understanding of many aspects of AAA, to include a deeper understanding of the commercial supply chain, identification of ongoing developmental programs within the federal government that can be leveraged for a wider audience, and identification of adversarial uses of AI.

Objective 2 – Short term – Adopt Commercial and Open Source Narrow AI Solutions: The IC must leverage the existing private sector and government investments by rapidly transitioning the best available commercial and open source Narrow AI capabilities.

Objective 3 – Medium term – Invest in the Gaps (AI Assurance and Multimodal AI): To create and maintain strategic advantage, the IC must develop both the capability and capacity to take advantage of available data across all INTs and open source, and develop AI solutions that process and relate information from multiple modalities. To facilitate this, the IC must continue to implement policies to break down traditional INT stovepipes.

Objective 4 – Long term – Invest in Basic Research Focused on Sense-Making: It is not enough to simply fuse information from multiple modalities together in response to a single, narrow task. The construction of shared models is needed to provide the basis for trust between human and machine teams. This level of understanding demands basic research advances in representing knowledge; goals and intent; entity extraction from incomplete, multimodal data; and discourse generation.

Inclusive of all four objectives, it is critical for the IC to address issues of AI assurance, transparency, and reliability as well as potential adversarial uses of AI. The AIM initiative must include a continuous effort to both understand how AI algorithms may fail.

The AIM initiative is about much more than technology. Implementing the strategy will entail addressing workforce challenges and understanding and shaping the policies and authorities governing how the IC deploys and uses AI. The global nature of the challenge and the rapidly evolving technological and societal frameworks dictate that the IC must have strong partnerships with other government agencies, the private sector, foreign partners, national laboratories, Federally Funded Research and Development Centers (FFRDC), University Affiliated Research Centers (UARC), and academic institutions. Lastly, the AIM initiative includes a robust communication and outreach plan for the workforce, Congress, members of the Executive Branch, industry and foreign partners, and the American people.

This page intentionally left blank.

Mission Imperative

The business of the IC, both in its raw material and its product, is intelligence, which comes from data. It is the job of the IC to analyze, connect, apply context, infer meaning, and ultimately make analytic and operational judgments based on all available data. The pace at which data are generated is increasing exponentially and is stressing our collective abilities. Some examples:

- By 2021, it is estimated that the data generated by global web traffic will reach 3.3ZB/year (up from 1.2ZB/year in 2016); this corresponds to 3.5 networked devices per global capita.[1]
- The Director of NGA has publically estimated that at the current, accelerating pace of collection, we would need over 8 million imagery analysts by 2037 to process all imagery data.[2]

One particular area of concern for the IC is related to AI mission assurance, especially in light of recent commercial efforts that utilize AI to generate high-quality, affordable forgeries of audio and video media. This could lead to widespread difficulties separating truth from fiction. Adding to this challenge is the problem that AI expertise is scarce, distributed around the world, and very limited in the IC.

Overview

In addition to the vision and guiding principles, this document provides guidance on:

- Investments
- Partnering with industry, academia, research agencies, and national laboratories
- Creating a new policy framework and tradecraft expectation that enable AI and ML while simultaneously promoting safe use and mitigating risk
- Reshaping the IC workforce
- Engagement with the Department of Defense (DoD) and international partners
- A strategy for creating a classified activity to generate strategic advantage for years to come
- Research and development
- Governance and IC collaboration models
- A robust communications strategy for all of our constituents including Congress, the work force, our industry and international partners, and the American people
- Establishing consistent classification/declassification processes through AI that promote secure information sharing and facilitate appropriate transparency to the public

1 "The Zettabyte Era: Trends and Analysis", June 2017. Cisco Report. https://www.cisco.com/c/en/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

2 Remarks from Director Robert Cardillo at 31st Annual Small Sats Conference, Utah, 8/7/2017 http://www.nga.mil/MediaRoom/speechesremarks/Pages/Small-Satellites/Small-Satellites---Big-Data.aspx

Vision

The AIM initiative seeks to secure and maintain a strategic competitive information advantage for the IC through focused development and rapid adoption of AAA technologies.

The leading private sector companies, both in market capitalization and prospects for growth, all recognize the importance of digital infrastructure and have made massive and ongoing investments in related technologies such as cloud services and big data. Since each new generation of technology builds on the previous one, it is critical that the IC continue to invest in its digital foundations. This initiative will guide the IC to accelerate the adoption of digital and analytics transformation, identify mission use cases, build a coherent data ecosystem, acquire the appropriate AI tools, reshape the workforce, adapt new workflow processes, and change the culture.

The IC can and must do this. Our IC ITE investments in cloud technology and data services have paved the road to harness the power of unique data collections and insights to provide decision advantage at machine speed.

Guiding Principles

The following guiding principles define the set of unwavering precepts that influence and guide the direction of the AIM strategy to facilitate cultural, political, and legal adoption across the IC.

The opportunity is great; the threat is real; the approach must be bold: Recognizing that strategic advantage is fleeting and fragile, the IC must be willing to rethink or abandon processes and mechanisms designed for an earlier era, establish disciplined engineering and operations practices, and maintain an absolute focus on assuring advantage in an intensely competitive global adversarial environment.

ML models are IC assets: Building on the IC ITE principle that "Data is an IC asset," machine learned models are also IC assets (as opposed to agency or INT-specific assets).

- Training and validation data sets: Most ML methods require large, high-quality, tagged data sets. These data sets are important IC assets and must be shared with IC partners to the maximum extent allowable.
- Rule sets, algorithms, and expert knowledge bases that capture the tacit knowledge of intelligence domain experts are also IC assets that must be shared with all appropriate and relevant mission areas.
- This community approach must also recognize and act on the need for INT-specific improvements, as they will be the main drivers for transformative capabilities in the near term.
- While improving INT-specific technologies, the community approach must take into account the need for correlated cross-INT data sets.
- Even when the actual training data cannot be shared, sharing the models derived from these training sets, along with the lessons learned from them, increases the value of these assets.

AI can be a powerful tool, but we must recognize challenges:

- ML classifiers are only as good as the data that is used to train them. For example, an image classifier that is trained with ground-based imagery may fail to classify images collected from overhead.
- Even state-of-the-art AI models are vulnerable to adversarial exploitation.
- AI and ML models are subject to "concept drift," i.e., the notion that in the real world data often arrives in streams and evolves over time in non-obvious ways. Therefore, the models must continually adapt to changes in the data environment so that opportunities to improve their accuracy are not missed.
- The IC should be aware of popular trends in AI but should stay focused on how we can best use the technology. When the media hype dies down, the IC must be ready to perform the long-term and difficult task of creating lasting operational value from these technologies.
- Many ML models do not include a description of their decision-making process in their standard output, and thus their results can be misunderstood by the casual user.

AI assurance models and adversarial AI must be addressed in parallel with AI systems: The level of effort to fool an AI algorithm is considerably lower than to develop them. Therefore:

- Intelligence systems must account for failure modes. For example, image classifiers may be fooled by very small changes in the input data, reinforcing the need for recurring human involvement in AI activities.[3]
- The IC must understand and anticipate how foreign entities may use AI and develop techniques and tactics to deny and disrupt those activities.
- The IC must develop intelligence systems that can demonstrate the underlying rationale behind decisions and responses to both users and overseers. For intelligence systems that make critical decisions regarding classification, dissemination, or life-critical decisions, such decisions and responses must be able to evince some degree of proof of correctness in addition to transparency.
- Recent developments in computer vision have resulted in approaches that can generate fake (altered or fabricated) images and audio recordings that are difficult to distinguish from unaltered digital media. The IC needs to develop ways of countering this capability.

AI is not a substitute for developing a solid digital foundation; it requires that foundation:

- The IC must continue to invest in and improve the IC ITE infrastructure and develop strategies for shared state-of-the-art hardware and/or other High Performance Computing (HPC) systems.
- The IC must accelerate activities that make data widely shareable. Need-to-know requirements and operational sensitivities will be honored but must not be used as an excuse to unnecessarily limit data sharing.
- The IC must create a sustained program of investment in the creation of high-quality training sets for the most important intelligence priorities.

3 Su, J., Vargas, D., Sakurai, K., "One Pixel Attack for Fooling Deep Neural Networks", arXiv 1710.08864, Feb. 2018

Despite the perceived investment gap, the IC has opportunities:

- U.S. Government (USG) investment in AI is dwarfed by investment of the private sector, and the IC investment is a fraction of what Department of Defense (DoD) is investing.
- The IC must not only leverage the investment of the DoD and private sector, but we must also be prepared to invest in areas of unique interest to the IC.
- The IC should invest in areas critical to the IC mission where the private sector has few incentives to invest, such as low-shot learning and adversarial AI/AI assurance.

Common services are a priority, however, there is still a need for specialization:

- The IC must create common services for common capabilities in computer vision, human language technology, identity intelligence, process modeling, analytic discovery, automated planning, and other areas, while encouraging principled approaches to mission-specific specialization where appropriate.

Investments in the workforce must be made: The IC must develop a more technologically sophisticated and enterprise aware workforce. We must:

- Embrace strategic workforce planning and workforce analytics to address AAA workforce requirements and skill gaps.
- Invest in programs for training and retooling the existing workforce in skills essential to working in an AI-augmented environment.
- Redefine recruitment, compensation, and retention strategies to attract talent with high-demand skills.
- Develop and continually expand partnership programs with industry, including internship and externship programs, to increase the number of cleared individuals with relevant skills both in and out of government.
- Leverage the IC Joint Duty (JD) Program more strategically to share expertise across the IC in a seamless manner.
- Understand and maximize human capital authorities, policies, and programs to augment the AAA workforce.

Engagement with partners is essential:

- A successful AI strategy requires engagement USG-wide, with the private sector, educational institutions, FFRDCs, national laboratories, and international partners (particularly Five Eye [FVEY] Partners).

Maintaining an understanding of the foreign threat is an intelligence priority:

- The IC must place an emphasis on S&TI integrated with operations and focused on AI in order to maintain strategic advantage, effectively counter these threats, and develop appropriate intelligence policies.

Investment Strategy

Worldwide private sector investment in AI, ML, and related technologies is growing rapidly. Estimates of global private sector investment in 2016 range from $26B to $39B (McKinsey).[4] This investment strategy acknowledges the significant private sector investment and prioritizes investments that 1) allow the IC to rapidly adopt the best commercial and open source capabilities, and 2) accelerate research in those areas unique to the IC and where the private sector is not currently focused. A successful investment strategy also recognizes we must maintain momentum on foundational infrastructure gains, such as completing the IC's HPC architecture as well as accelerate data conditioning, storage, and sharing activities. This four-part investment plan, illustrated in Figure 1, addresses each aspect of basic research, applied R&D, and development and adoption.

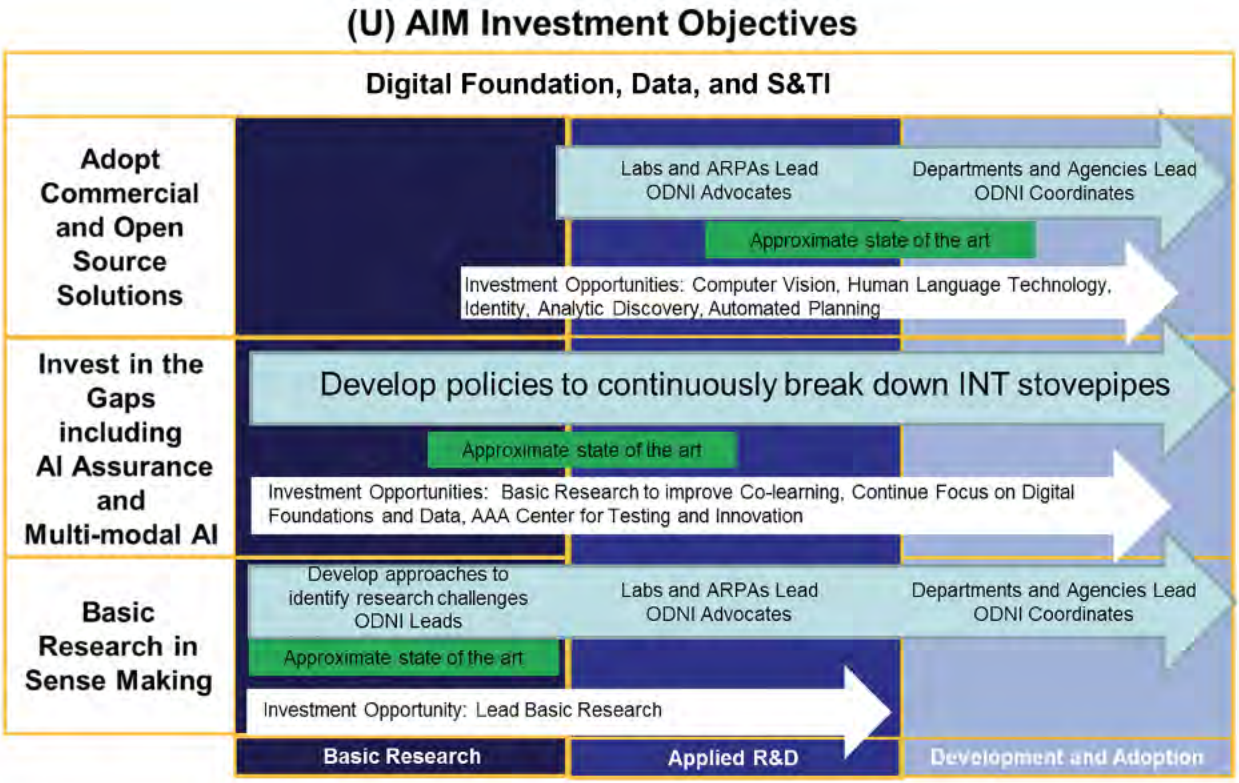


Figure 1: AIM Investment Strategy

4 "Artificial Intelligence – The Next Digital Frontier", June 2017, McKinsey Global Institute

Objective 1 – Immediate and ongoing – Digital Foundation, Data, and S&TI: AI activities are not a substitute for an enduring, secure, standardized, and measurable IC-wide digital infrastructure and data ecosystem. The IC will:

- Make data accessible to a wide variety of analytic platforms and models.
- Establish and maintain relevant training data across all INTs and disciplines.
- Adapt policies and tradecraft to enable more automated methods of assembling and vetting training data.
- Seek to future-proof data. Establish standards for data labeling and metrics for evaluation.
- Undertake a program of continuous growth in computational resources to ensure sufficient numbers of current generation hardware are available to IC AI practitioners.
- Improve foundational S&TI for AI, including adversarial uses of AI.
- Research co-learning and AI assurance models, especially vulnerabilities and standards.

Objective 2 – Short term – Adopt Commercial and Open Source AAA Solutions: The IC must leverage the massive private sector investment by rapidly transitioning the best available commercial and open source AAA capabilities. This will be accomplished as follows:

- **Aggressively pursue shovel-ready opportunities across IC Agencies**
- **Establish an IC AIM Center:** To foster innovation and rapidly prototype transformative solutions, the IC will establish an AIM Center staffed with AI and ML talent from across the IC, augmented by experts from industry.
- **Collaborate with key partners to identify opportunities:** Strengthen partnerships with the Intelligence Advanced Research Projects Activity (IARPA), the Defense Advanced Research Projects Agency, In-Q-Tel, the national laboratories, Defense Innovation Unit-Experimental, and industry. Advocate for those activities that address gaps with a minimum amount of duplicative effort, which will facilitate rapid transition of appropriate AAA capabilities to operations.

Objective 3 – Medium term – AI Assurance and Multimodal AI: In order to create and maintain strategic advantage, the IC must develop AI solutions that process and relate information from multiple modalities. To facilitate this, the IC must continue to implement policies that break down traditional INT stovepipes.

Objective 4 – Long term – Invest in Basic Research Focused on Sense-Making: The IC must understand multimodal information in context and look for ways that substantially augment the activities of IC Officers.

The massive investments to date as well as those currently planned (both public and private) will not be sufficient to meet the unique, foundational, and all-source sense-making needs of the IC. Therefore, basic research will focus on those areas and facilitate collaboration across the public and private sectors.

Policy and Authorities

As part of the AIM strategy, the IC will examine the current tradecraft landscape and address emerging policy issues with appropriate efforts internal to the USG and, where needed, international venues. Policies to codify AIM activities (e.g., acquisition, enterprise management, classification, and analytic integrity) will be developed with consultation from appropriate general counsel, civil liberties, privacy, and policy personnel. ODNI will provide a dedicated, integrated policy and legal effort to break down barriers to information sharing, particularly INT-specific data, so that we do not inadvertently slow the pace of technological progress.

Workforce Strategy

The IC must develop a more technologically sophisticated and enterprise-aware workforce. We must:

Embrace strategic workforce planning and analytics: Workforce planning will aid in accurately identifying current and future skill gaps, and will also enhance the IC's ability to determine the most appropriate mitigation strategies (e.g., training, compensation, etc.).

Invest in programs for training and equipping the workforce in essential AI skills: This does not mean everyone in the workforce needs to become an expert in deep learning or Python coding, but everyone does need to understand how AIM fits into the new workflow and how they can contribute. Specific actions include:

- Leadership – must understand the implications on the intelligence process, have a sophisticated understanding of the threat environment and foster an environment that enables an open and collaborative culture while reskilling the workforce to operate in an AI accelerated environment.

Build on the IC 2025 workforce transformation to attract talent with high-demand AI skills: The role descriptions for people with these skills have gone by many different terms in recent years. Therefore, individuals with these skills may be available but under different keywords. These alternative terms include analytics, data science, data wrangling, statistics, ML, deep learning, and modeling. These cover both the researchers who propose and test new methods, as well as model builders who use these algorithms to create and validate models.

Develop partnership programs with industry and academia to increase the pool of people inside the IC with awareness of best practices and available tools in this fast moving area, and to encourage individuals outside of the IC to build capabilities that meet the needs of the IC. Specific actions include:

- Recruit talent before graduation, and before competition with industry salaries, through service-for-education agreements ("ROTC"), expansion of IC postdocs, and internship/externship programs.
- Support temporary non-government to government (internship, externship) rotations.
- Expand sabbaticals, part-time industry Intergovernmental Personnel Act positions, and consultancies that grant clearances to faculty to increase the available technical skill available to the IC.

- Investigate changes in policy or funding to improve retention and attraction of U.S. national and foreign-born graduates in technical fields, including staff roles that do not require a clearance, and "fast-track" hiring that allows experts to perform productive work before obtaining a clearance.
- Expand use of open challenge problems (e.g., IARPA) and develop data and proxy problems that focus external communities on IC regions of interest.
- Identify unclassified equivalent domains for researchers to pursue. While the IC represents a unique environment, often similar domains give uncleared researchers an opportunity to develop and test algorithms on data that has many of the same qualities as IC data. This also fosters an interest in public service.

Leverage the IC JD Program: As competition for talent continues to increase outside of the IC, the community must leverage the IC Civilian JD program to share and retain talent across the IC and provide the workforce opportunities in other IC missions. We should:

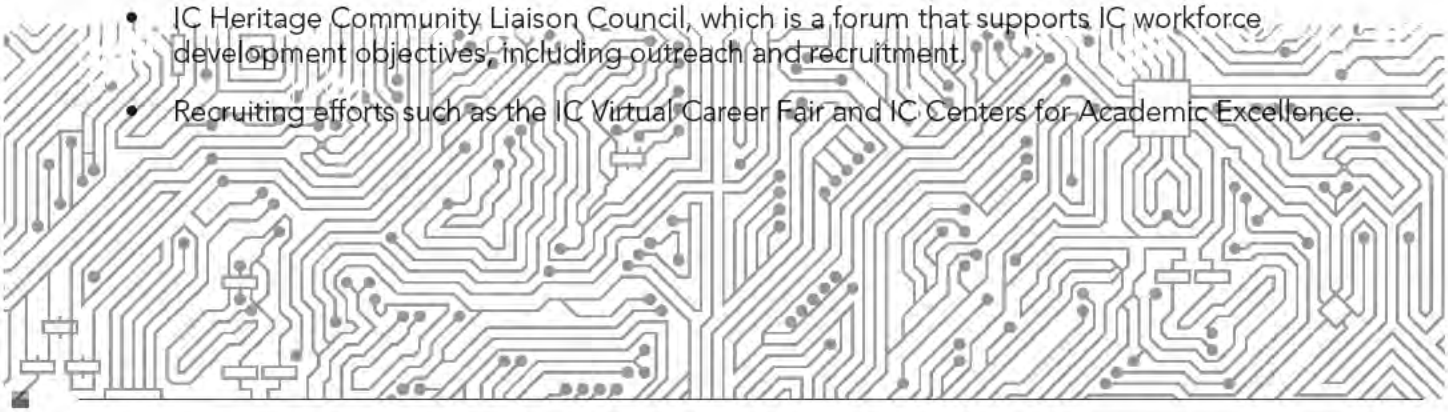
- Identify related positions in each agency that will benefit from the JD program.
- Track JD opportunities for professionals and the AI community's use of the JD program.
- Ensure that the return on investment of personnel participating in the JD program meets AI objectives and is sustainable through the sense-making investment stage.

Understand and maximize human capital authorities and policies to augment the AI workforce: IC elements and the DNI have certain authorities at their disposal to assist in the management of the IC employment lifecycle. In order to ensure the most effective use of these authorities, we should:

- Identify and implement authorities that will create efficiencies in recruiting, hiring, compensation, training, and retention of AI professionals.
- Ensure that human capital policies enable IC elements to support the employment of AI personnel and do not erect barriers that may disengage the AI workforce.

Leverage current human capital programs and monitor implementation and user feedback: AI managers must continually collaborate with human capital professionals to take advantage of programs that enable the IC workforce to meet mission objectives. Examples include:

- Scholarships and other educational financial aid (e.g., Stokes Scholarships).
- Well-rounded recruiting programs that include outreach to diverse schools (e.g., Adopt-A-School, IC Wounded Warrior Program, STEM Outreach).
- IC Heritage Community Liaison Council, which is a forum that supports IC workforce development objectives, including outreach and recruitment.
- Recruiting efforts such as the IC Virtual Career Fair and IC Centers for Academic Excellence.



Industry Partnership Strategy

Since the bulk of the nation's AI resources reside in the private sector, partnership is essential to the IC. Yet the barriers working with government often require considerable effort to clear. This requires a more flexible acquisition paradigm. This includes cooperative agreements that may trade data for algorithms or "Analysis-as-a-Service," as well as public prize challenges to solve IC problems. With the bulk of development occurring outside the IC, we must collectively prioritize Certification and Accreditation of new software so that code can more quickly be deployed on secure networks. ODNI, in collaboration with the IC elements, will develop an industry partnership plan for AIM capabilities. Elements of the plan will include:

- Industry access to USG data for algorithm development
- Enabling human resource strategies to simplify the development and sharing of AI skills between government and industry to include new approaches to security
- ODNI advocacy for AI basic research funding
- Creating AI services of common concern or specific capability contracts
- Update intelligence and industry data- and capability-sharing policies and oversight

Roles for USG Agencies, National Labs, FFRDC, UARC, Commercial and Academic Institutions

To capitalize on the combined capabilities of the USG, national laboratories, private industry, and academic institutions, the ODNI must facilitate partner integration. Therefore, partner roles include:

IC:

- Promote communications between AIM partners
- Promote development of shared analytic services where feasible
- Share datasets and computing
- Capture and share expert knowledge from IC systems and analytics
- Capture and share mission data for future training datasets and simulations
- Develop defensive and offensive techniques for adversarial/counter AI
- Coordinate R&D activities
- Modernize multi-agency data sharing practices
- Improve S&TI on foreign AIM capabilities and intentions

Whole-of-USG:

- Share datasets across labs, private industry, and academic institutions
- Acquire and retain experts on immigration policy, IPAs, or service-for-education agreements ("ROTC")
- Coordinate DoD and IC R&D, computing and data purchases, and data-labeling efforts
- Synchronize funding for basic and applied research efforts

National Labs/FFRDC/UARC

- Provide expert advisors to USG
- Verify and validate algorithms and data sets, testing and evaluation (T&E), and AI methodology
- Conduct mission-focused research
- Develop AIM-related algorithm and systems prototyping
- Support talent pipeline development

Industry

- Provide commercial tools accessible through USG acquisitions and/or investment
- Conduct mission-focused, AIM-related research and development
- Provide expert advisors to USG
- Appropriately share datasets through a legal, supportable business model

Academic Institutions

- Perform the research needed to develop long-term scientific breakthroughs
- Provide expert advisors to USG
- Train the next generation to be a highly skilled workforce equipped to develop AAA tools and develop skills to utilize AAA systems

Five Eye Foreign Partner Engagement

Allied and partner nations can enhance our joint development of intelligence products. Expanding international partnerships will provide opportunities to increase collection access and reliability, improve the quality and quantity of partner data and analysis, align strategic capabilities and emerging technologies, and promote compatibility across digital architectures and analytic tradecraft.

AI Assurance – Secure and Maintain Competitive Advantage

The unique data and tools that the IC creates using those data are important IC assets that provide competitive advantage for USG missions. That advantage is fleeting and fragile, requiring disciplined engineering and operations practices, and an absolute focus on assuring advantage in an intensely competitive global adversarial environment. Commercial and USG needs differ in important ways but largely overlap with the concomitant requirement for continuous investment in data, tradecraft, tools, T&E, security, and S&TI.

AI technologies have clearly demonstrated that they can provide powerful capabilities. They have also demonstrated their brittleness and vulnerabilities. There are some principles and best practices that can be used today.

- **Data:** ML systems are only as good as the data used to train them. Acquiring those data in volume from the intended operational environments is a critical advantage. These data must be continuously monitored and reacquired as necessary. This is an engineering tradecraft best practice, akin to standard software test suite discipline.
- **Software:** The leading edge AI/ML software suites were written to support science, not national security operations. There is no notion of cyber security. USG needs are not aligned exactly with those of industry and universities; we need to differentiate in the state-of-the-evolving-art tools in a robust, sustainable way.
- **Systems:** Continuous evaluation of performance is required. There is very little theory to inform us as to when ML systems fail, or even whether they will work as expected[5]. This situation is not acceptable for any safety-critical or national security system. We must always incorporate performance monitoring, and we should support theory development.
- **Test and Evaluation:** Too many AI/ML projects launch without metrics to allow the IC to understand whether the investment is on track to succeed or fail. Create the discipline to define metrics up front and establish rigorous testing regimes and schedules.

Concept Drift must be addressed. "Concept Drift" is the idea that all computer tools are built with specific assumptions about the real world and that the basis for these assumptions generally changes over time, requiring the tools be monitored and updated. Best practices in established disciplines such as control systems theory can help structure how this challenge is attacked; we must detect issues and— when possible—automatically correct.

Adversarial AI techniques represent opportunities and risks. We have highly sophisticated adversaries with access to the same tools, their own data, and experts trained in the same universities as our own people. AI is merely one of the new battlegrounds for a technology-based arms race.

S&TI is a priority. We must develop a better understanding of foreign adversary tactics, techniques, and procedures.

5 Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z., Swami, A., "The Limitations of Deep Learning in Adversarial Settings", IEEE European Symposium on Security and Privacy, IEEE 2016, Saarbrucken, Germany.

Understanding when AAA techniques fail is critical. The technical literature is replete with examples of how to deceive AAA systems.[6] We need to know how and where adversarial systems are in use against our assets.

Outreach / Communications Strategy

A key factor in the success of transformation efforts like the AIM initiative comes through awareness and education of all of the varied constituents of the enterprise. Therefore, the ODNI will establish and maintain a robust communications engagement strategy for each of the following audiences:

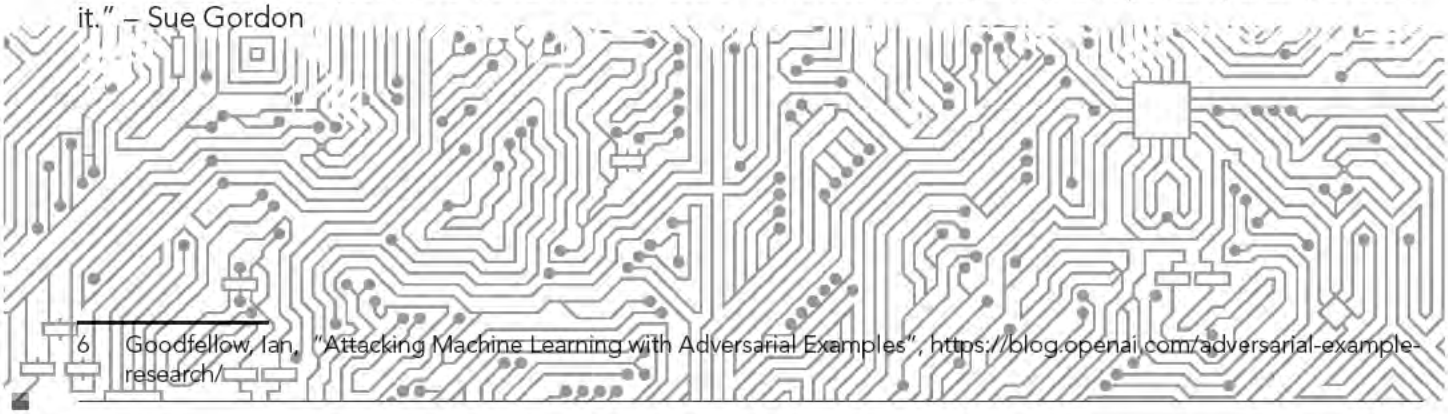
- The IC, including leadership and the workforce
- The DoD and other government agencies
- Congress and the White House
- The private sector
- The national laboratories and academia
- The American people

Governance

Following the example of private sector firms that are successfully implementing AI and recognizing that strong executive leadership goes hand in hand with stronger AI adoption, the PDDNI will, along with the IC Deputy Executive Committee (DEXCOM), serve as the executive sponsors for the strategy.

Conclusion

AIM technologies will have a transformative effect on how the IC operates. Increases in data volumes and velocity require the IC to dramatically rethink how we perform our mission. Additionally, our adversaries have recognized the importance of AIM methods and are putting significant effort into these technologies. The principles and strategies laid out here will allow us to meet those challenges. Most notably, those strategies will build on and leverage lessons learned from current and successful AIM efforts; strengthen the collaboration between the IC and industry, research agencies, and academic talent; and grow the talent pool of AIM technology expertise for the IC. Our goal in all of this is to meet our IC objective now and into the future. "If it is knowable, and it is important, then we know it." – Sue Gordon



6 Goodfellow, Ian, "Attacking Machine Learning with Adversarial Examples", https://blog.openai.com/adversarial-example-research/

Appendix A: Background on AI

Artificial Intelligence (AI): The IC defines AI as "the branch of computer science focused on programming machines to perform tasks that replicate or augment aspects of human cognition," a term coined in the 1950s.[7] At that time, scientists began to harness nascent computer capabilities to perform advanced information manipulations much more rapidly. In particular, it was realized that computers could be used not only to perform calculations on numbers, but also to perform inference on other types of information such as symbols, data, and text. This popularized the idea of a "thinking machine" that could, if filled with all the right knowledge and rules for access and retrieval, simulate a human response.[8]

Technologies and research areas generally considered to be sub-domains to AI:

- Automated Planning and Scheduling
- Computer Vision
- Decision Support, Predictive Analytics, and Analytic Discovery
- Distributed Artificial Intelligence/Agent-based Systems
- Human Language Technologies
- Identity Intelligence
- ML
- Process Modeling
- Robotics/Autonomous Systems

Ideal AI System: A machine capable of ideal human intelligence with a computer's speed, capacity, and precision.[9]

Adversarial AI: A subset of AI focused on understanding how AI systems behave in the presence of a malicious adversary.

Artificial Narrow Intelligence (ANI): Also known as "Narrow AI" or "weak" AI, this is an AI system that is specialized for a single purpose and cannot be generalized. All current applications are ANIs.

Artificial General Intelligence (AGI): Also known as "General AI" or "strong" AI, this is an AI system that can handle any human intellectual task—memory, learning, abstraction, and creativity. There are no AGI systems in existence, although building an AGI has been the goal of the field since it was founded in the 1950s.

The AIM INITIATIVE—Augmenting Intelligence using Machines

Narrow AI and Multimodal AI: Nearly all current commercial applications of AI are narrow solutions in that they solve a single problem with a single kind of data. Image classification, face recognition, and human language translation are all examples of narrow AI solutions. The IC must bring together

7 National Intelligence Council Sense of the Community Memorandum SOCM 2016-039C, 24 June 2016

8 Fiscal Years 2019-2030 Major Issue Study Final Report, Advanced Analytics, Deep Learning, and Artificial Intelligence.

9 Yost, Kirk, "Threats Posed by Advances in Artificial Intelligence", MITRE Technical Report sponsored by OSD Office of Net Assessment, 2016

data from multiple INTs to provide context and meaning to analysts over a variety of different data. Multimodal AI presents a whole new group of challenges in a number of areas that the IC must overcome. The challenges include:

- Representation - Presenting and summarizing multimodal data in a way that exploits its complementarity and redundancy. For example, development of representations that allow simultaneous analysis of audio derived from SIGINT with imagery and video.
- Translation – Learning how to translate or map one mode to another while recognizing that the relationship between modalities is often subjective. For example, there are any number of correct ways to describe an image with words, but a perfect translation from image to text may not exist.
- Alignment – Understanding how to identify direct relationships between elements and sub-elements to derive meaning from multiple modalities. For example, aligning a verbal description of an event with sequences in a video requires measuring similarity between modalities and understanding long-range dependencies and ambiguity.
- Fusion – Understanding how to join information from multiple modalities, which may have different predictive power and noise characteristics. For example, in audio-visual speech recognition, the visual description of the lip motion is fused with the speech signal to predict spoken words.
- Co-learning – Exploring how knowledge gained learning from one modality can help computational models trained on a different modality.

Automated Planning: A branch of AI focused on generating strategies or action sequences necessary to achieve a goal.

Automation: Computational systems designed to perform repetitive tasks.

Autonomous Systems: Systems that carry out tasks without human intervention. In AIM we are especially focused on computational systems that perform complex reasoning tasks.

Catastrophic Forgetting: A learning problem which occurs when performance learned in earlier tasks in a series is entirely or mostly lost after being given examples of later tasks.

Co-learning: A sub area of machine learning focused on either understanding how multiple agents can simultaneously learn, or how a single agent can use learning from one modality to improve computational models trained on a different modality.

Computer Vision: A field of study that aims to analyze, extract, and understand objects and relationships from within single or multiple images.

Concept Drift: The notion in ML that the concept being learned will change over time. Differentiating between different types of malware, for example, is a classification task that changes as new malware is produced.

Deep Learning: "Representation-learning methods with multiple levels of representation, obtained by composing simple but non-linear modules that each transform the representation at one level (starting with the raw input) into a representation at a higher, slightly more abstract level. With the composition of enough such transformations, very complex functions can be learned." (LeCun, Y., Bengio, Y., and Hinton, G., "Deep Learning", Nature, Vol 521, 2015.)

Graphical Processing Unit (GPU): Specialized electronics designed to perform rapid mathematical functions to render images, animations, and videos.

Human or Intelligence Augmentation: Use of information technology to augment human intelligence in the performance of some task. Unlike autonomous systems which aim to replace human activity, augmentation is designed with humans as central.

Knowledge Discovery: A process of discovering useful knowledge from a collection of data.

Low-shot Learning: An object recognition, ML classification task where learning must take place despite having only one, or a few, example images for training.

Machine Learning: The field of study interested in building computational systems that can improve their own performance of some task.

Machine Learning Classifier: A ML model designed to assign given examples into known discrete categories (i.e., classification).

Machine Learning Model: An explicit summary of data which is useful for performing some task. The product of ML systems like decision tree algorithms or neural networks are generically known as models.

Multimodal AI: A subset of AI focused on methods that emphasize the integration of linguistic, acoustic, and visual data in the completion of some task.

Natural Language Processing: A field of study that aims to analyze and understand human language communications both spoken and textual. Can include analysis and generation of language.

Sense-making: A process of creating understanding in situations of high complexity.

Technical Debt: Complications accumulated during the construction and use of software or ML models that make maintenance of these models difficult (e.g., hidden feedback sources, undeclared consumers, data dependencies, and changes in the external world).

Testing data: A collection of examples used to evaluate the performance of a ML Model.

Training data: A collection of examples used to inform the construction of a ML model.

Appendix B: Acronym List

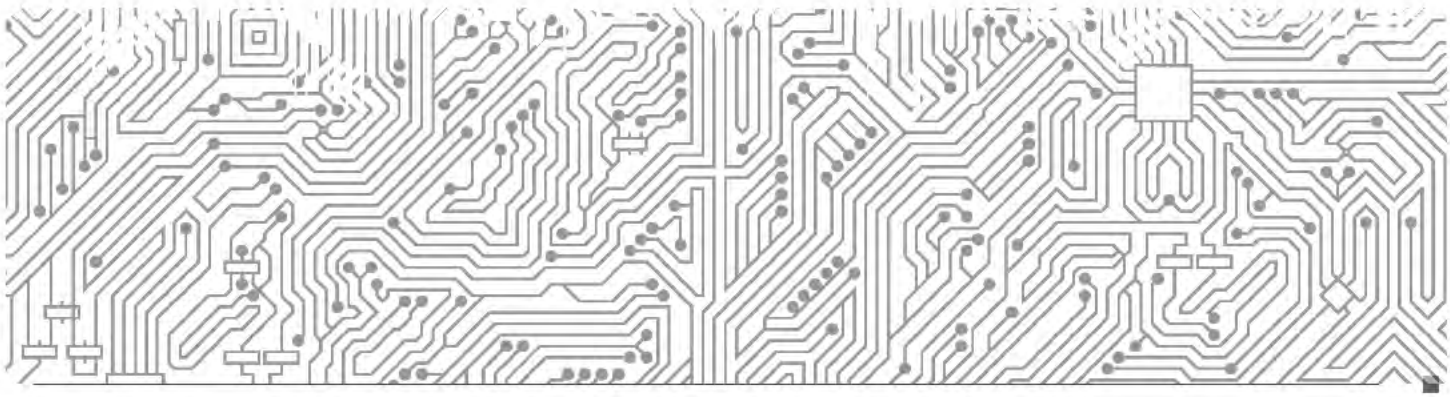
- AAA Artificial Intelligence, Automation, and Augmentation
- AGI Artificial General Intelligence
- AI Artificial Intelligence
- AIM Augmenting Intelligence using Machines
- ANI Artificial Narrow Intelligence
- ASIC Application-Specific Integrated Circuit
- CIA Central Intelligence Agency
- DEXCOM Deputy Executive Committee
- DIA Defense Intelligence Agency
- DNI Director of National Intelligence
- DoD Department of Defense
- FBI Federal Bureau of Investigation
- FFRDC Federally Funded Research and Development Center
- FVEY Five Eye
- GPU Graphical Processing Unit
- HPC High Performance Computing
- IAA Identity, Authentication, and Authorization
- IARPA Advanced Research Projects Activity
- IC Intelligence Community
- IC ITE IC Information Technology Enterprise
- ICAIP Intelligence Community AAA Implementation Plan
- JD Joint Duty
- ML Machine Learning
- NGA National Geospatial-Intelligence Agency
- NRO National Reconnaissance Office
- NSA National Security Agency
- ODNI Office of the Director of National Intelligence

- PAI Publically Available Information
- PDDNI Principal Deputy Director of National Intelligence
- R&D Research and Development
- S&TI Science and Technical Intelligence
- SEI Software Engineering Institute
- STEM Science Technology Engineering Math
- T&E Testing and Evaluation
- UARC University Affiliated Research Center
- USG US Government
- ZB Zettabyte

Acknowledgements

This document was created by the AIM Implementation Team with representatives from:

- ODNI
- CIA
- DIA
- FBI
- NGA
- NRO
- NSA
- USD(I)




OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA