LONDON POLITICA

The Sino-American AI Competition: A Breakdown

14 August 2023

A breakdown of the Sino-American AI developmental ecosystems, industrial policy, and sector-sector competition with a consideration of emerging risk.

Report Leads
Marco Zarzana, Yueh Chen, Levi Cursham.

Research Analysts
Campbell Clarke, Armaan Nanda, Ella Startt, Felice Valeria, Gabrielė Eidėjūtė-Strong, Kateryna Anisova, Parul Wadhawan, Piotr Malachinski, Ruyi Liu.

Table of Contents

Executive Summary

This report offers a breakdown of the Sino-American AI competition by examining the two nations' developmental ecosystems, the competition within them, and how industrial policy is playing a role. This is followed by an analysis of some of the emerging risks, particularly how AI will exacerbate modern dilemmas to threaten democracy and civil liberties. Finally, we consider some of the larger questions around AI, such as how to characterise its development, especially in a geopolitical sense, as well as the question of an AI pause.

- **In "Structure of AI Industries"** The report breaks down the structure of the ecosystems in which AI has developed, including their major actors, but also the geographical hubs, alliances, and academic institutes that shaped them.
- **In "Impact of Industrial Policy"** the report delves into the role played by Chinese industrial policy in driving AI progress, largely due to the government's view that it is a core part of national development. Meanwhile, the US has given relatively small attention to industrial policy. Regulation in the US, meanwhile, is a growing topic of importance, despite its fractured nature.
- **In "Deepdive: Sectoral Competition"** the report highlights how the US and China are progressing in three specific fields of AI: Natural Language Processing, Computer Vision, and Autonomous Vehicles. While this a non-exhaustive exploration of competition dynamics between the two countries, it offers an insight into the followership and leadership taking place, and areas where each country has advantages.
- **In "Horizon Scanning"** we take a look at three risks that have emerged in the context of the Sino-American strategic clash. The risks created are by and large not new, and we highlight how AI will exacerbate and complexify risks already confronting the world today. These are a). Its impact on traditional arms racing, b) AI as a tool of mass surveillance, and c). AI as a tool for political disruption. In all three cases the team has outlined how AI development has increased the severity of already present risks. One of the out and out losers from this risk analysis is democracy and civil liberties, with Chinese firms ready to export AI to autocracies around the world.
- **In "Considering AI Competition"** the team examined two issues in the wider AI space, firstly, a conceptual one regarding the 'race' or competition itself. Often described as an arms race, we evaluate the argument that it should instead be termed an industrial revolution, finding it a much more useful framework to understand the complexity it brings. We then broach the issue of the AI pause and the need for regulation in this new technological space, advocating for this drastic, but potentially highly beneficial, move.

Microsoft
TAIWAN
AI
tsmc

Introduction

Levi Cursham

What is Artificial Intelligence?

> *The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.*

Artificial intelligence (AI) is at the forefront of conversations in every field of academia and research. This report broadly approaches AI in the geopolitical space, though does not pretend it can be so neatly confined. The team working on this report have sought to better comprehend the developmental rivalry currently taking place in the field of AI between the United States of America (US) and China. It aims to further understand the different industrial ecosystems that have led to the development of AI, and that are currently propelling its advancement. Furthermore, it also seeks to elucidate some of the political-economy behind its development, looking at how regulation and state planning are playing differing roles in the two countries. A third chapter takes a closer look at how Chinese and American tech firms are progressing in specific sectors of AI development, namely Natural Language Processing, Computer Vision, and Autonomous vehicles.

The result of this study is a better understanding of what has driven success in both nation's AI industries, and offers some insight into the current trajectories and processes at play. While the US and China are in some places considered as peers to be compared like for like, both are highly differentiated and must be understood in their own contexts primarily.

The second half of this report examines risks that are emerging from China's use of AI as a tool of national development, while also considering what lies on the horizon of AI. These two sections are non-exhaustive explorations of the complexity that progress made by the US and China in the field of AI now poses. The research team have noted AI's potential to further exacerbate threats to democracy and civil liberties, which - more than creating new problems - is likely to be the most impactful short term effect. Not for this reason alone, we have chosen against classifying AI development as an arms race, an issue which is explored in more depth below.

Structure of Sino-American AI industries

Campbell Clarke

China's AI development industry:

China's domestic artificial intelligence (AI) ecosystem is dominated by three major industry participants: Baidu Inc., Alibaba Group Holding Ltd., and Tencent Holdings Ltd. Collectively referred to as BAT, these three firms are often compared to Google, Amazon and Facebook because they have dominated the Chinese technology sector – especially across platforms that include e-commerce, digital entertainment, e-finance and, crucially, AI. Baidu, which established its headquarters in Haidian District, Beijing, began as a search engine company but has since evolved into a firm that specialises in various internet-related services and AI, while Alibaba – based in the city of Hangzhou in Zhejiang province – began as e-commerce platform that has since implemented several online services. Tencent, which located its headquarters in the city of Shenzhen in Guangdong province, initially offered a consumer-facing messaging app, although it has since diversified by offering social networks, online music, web portals, e-commerce, internet services, online payment systems, smartphones, and online games. In fact, Tencent is currently one of the highest-grossing multi-media companies in the world and is one of the largest video game companies on earth.

While each firm possesses a core area of expertise – Alibaba in e-commerce, Tencent in social networking, and Baidu in search and information indexing – they collectively constitute the core of China's national AI strategy, through which the state aspires to become the global leader in AI by 2030. While the expertise and funding that these firms possess sets the direction and pace of AI development in China, these firms also engage in intense competition with one another and have, therefore, invested significantly in China's major AI firms. In fact, BAT invests in 53% of China's 190 major AI companies, which reflects their desire to solidify their presence across a wide range of sectors rather than focusing explicitly on the core segments in which they have expertise.

Moreover, many of the firms in which they invest are oriented towards AI applications–such as machine vision and natural-language processing–rather than core technologies, like algorithms and silicon chips. Seeing China's AI industry has benefited from comparative advantages that include its abundance of centralised, easily accessible data, lenient privacy laws and lax regulatory landscape, this strategy might be advantageous in the short-term. Crucially, however, such investments have fostered the formation of an AI industry that includes many companies dedicated to AI applications and far fewer dedicated to developing the algorithms and advanced silicon chips that underpin them, which might adversely affect

China's ability to compete internationally and expand its existing AI capabilities through foundational, private-sector-led research in the dlong-term.

Moreover, each of these firms serve as members of China's "National AI Team," which is a group of companies selected by the Ministry of Science and Technology to coordinate their activities, integrate AI into existing economic sectors, and establish standards to accelerate the development of China's national AI ecosystem. By receiving superior access to capital, preference in government bidding contracts, and regulatory flexibility from the state, members of the National AI Team are responsible for constructing open innovation platforms that are accessible through application programming interfaces (APIs), but also for engaging in research and development (R&D), sharing data and open-source software, actively participating in the AI ecosystem, and supporting the development of small and medium-sized enterprises (SMEs). Interestingly, between 2014 and 2018, Baidu, Tencent, and Alibaba participated in 39 equity deals with start-ups that produce AI software and AI chips, 44% of which were with start-ups based in the United States. Conversely, Amazon.com, Facebook, Google, Apple and Microsoft invested in just one AI start-up in China – Mobvoi – between 2014 and 2018, although investors in the United States funnelled more than $40 billion into 251 AI start-ups based in China between 2015 and 2021. Combined, such measures are intended to help the members of the National AI Team become global leaders within their core business segments, and thereby propel China to the world leading position in AI innovation to which it aspires.

Thus far, the Ministry of Science and Technology has announced two groups of National Team Members–the first in 2017 and the second in 2019–and each member was strategically selected for a specific sector within China's broader AI ecosystem. Unsurprisingly, Baidu, Alibaba, and Tencent were among the first of five major team members selected. Baidu was specifically chosen to lead the development of China's autonomous driving industry, Alibaba was selected to spearhead growth in smart city technology, and Tencent was identified to become both a national and global leader in the field of medical imaging (see Figure 2). While not as large as the three traditional technology titans, iFlytek, a global leader in speech recognition and computational logistics, was selected to lead the development of China's smart audio sector, while SenseTime, a leading player in facial recognition, image recognition and object detection, was chosen to drive the growth of China's smart vision field (see Figure 2). Then, in August 2019, the Ministry of Science and Technology extended China's National AI team to include ten additional firms: YITU Technology (vision computing), Huawei (AI related software and hardware), Hikvision (video perception), Ping An (inclusive finance), MiningLamp Technology (smart marketing technology), Megvii (image perception), JD.com (smart supply chain), TAL Education Group (smart education), Qihoo (cyber security), and Xiaomi (smart homes). Moving forward, the initiative remains open to new applicants that are required to specify the domain of AI platform development they plan to initiate and the range of companies that will benefit from such collaboration.

In addition to China's National AI Team members, there are approximately 1,189 AI companies operating in China's ecosystem, which engage in intense competition. While the national-level policy initiative endeavours to foster the emergence of open platforms in numerous AI sectors through the selection of national members, the CPP is also attempting to ensure it does not suffocate strong firms that are not part of the aforementioned group of companies so that it does not stifle innovation.

China's AI Hubs: Regional Hubs and AI Pilot Zones

Since the turn of the 21st century, several robust economic clusters specialising in technology development and innovation have emerged in China, many of which constitute core pillars in China's AI development strategy. This is largely because many of the technology companies that utilise AI operate in concentrated clusters in certain geographic regions. Specifically, economic clusters have emerged around Baidu, Alibaba and Tencent in the cities of Beijing, Hangzhou, and Shenzhen. Additionally, three major economic clusters have emerged in the Beijing-Tianjin-Hebei region, the Yangtze River Delta region, and the Pearl River Delta region – also known as the Greater Bay Area, if one includes Hong Kong – which are all among the highest ranked regional economic centres for technology development and innovation in China.

To complement its New Generation Artificial Intelligence Development Plan, the Chinese Communist Party (CCP) has also established AI innovation and development pilot zones in strategically selected cities. While the aforementioned clusters have developed organically with the help of local government investment, these pilot zones differ in that they are being established by the central government at the national level. More specifically, these pilot zones are explicitly utilised to promote the development of the AI industry in cities that already possess strong foundations for subsequent development. As such, the CCP and local governments are providing financial incentives and favourable regulations in such pilot zones to ensure that the activities taking place within these areas will produce AI applications that generate economic, social, and environmental benefits for the local areas in which they are being formed. In December 2021, Li Meng, China's Vice Minister of Science and Technology announced that 17 pilot zones had been developed, while the Ministry of Science and Technology endorsed the establishment of three additional pilot zones later that month. When viewed together, this suggests that the CPP's goal of constructing 20 AI pilot zones by 2023 has been reached.

Alliances, Associations and Academic Institutions

While the members of China's National AI Team are crucial to the state's AI development strategy, alliances and collaborative efforts between corporate actors, academic institutions, research organisations, and sectoral associations also constitute core pillars of China’s AI ecosystem. In fact, more than 190 industry alliances – coordinated by both the national and local governments – existed across China’s AI ecosystem by the end of 2019. Unlike the private-sector-led industry alliances that exist throughout many Western, capitalist states, government entities in China generally establish industry alliances because the CCP prefers to maintain control over the private sector and ensure its activities are aligned with its national economic interests. Moreover, government officials and policymakers in China utilise such alliances to gauge the competitiveness of AI firms and clusters across different geographic regions, which further illuminates their importance in the context of China’s AI ecosystem.

Of the AI-oriented industry alliances that exist in China, the China Artificial Intelligence Industry Alliance (AIIA) is the most important. The AIIA was established immediately after the release of China’s New Generation Artificial Intelligence Development Plan by several institutions that include the National Development and Reform Commission (NDRC), the Ministry of Science and Technology (MOST), the Ministry of Industry and Information Technology (MIIT), and the Cyberspace Administration of China (CAC), the AIIA is comprised of senior representatives from key sectors, geographies, and firms in China’s AI ecosystem, including Alibaba, Huawei, Qihoo 360, Tencent, Tsinghua University, Zhejiang University, Zhongxing Telecommunications Equipment (ZTE), and Baidu. While many of the corporate members operate in large companies, there are also members from AI-oriented start-ups and SMEs, many of which specialise in commercial AI applications. The alliance’s primary purpose is to serve as a platform-through the establishment of conferences and programs – to promote cooperation between various levels of government, AI firms, universities, research organisations and end users of AI applications to drive growth and innovation throughout China’s AI ecosystem.

Moreover, the Chinese Association for Artificial Intelligence (CAAI) and the China Computer Federation (CCF) are also crucial institutions within China’s wider AI ecosystem. Established in 1981 and administered by the Ministry of Civil Affairs as a state-level organisation under the China Association for Science and Technology, the CAAI is the only academic association in China that focuses exclusively on AI at the national level. The organisation currently operates through 51 divisions throughout China and includes 43 professional committees and eight working committees that collectively engage in the funding and organising of international conferences, industry awards, and the publishing of academic AI journals. The CCF does not receive funding from the government but instead depends on membership fees from its 55,000 paying members.

More recently, the Beijing Institute for General Artificial Intelligence (BIGAI) was established in 2020 and is backed by China’s Ministry of Science and Technology, the Ministry of Education, and Beijing’s municipal government. The project is comprised of an elite team of scientists educated at prestigious universities in China and the United States, all of whom are led by Zhu Songchun, a researcher from the University of California, Los Angeles (UCLA), whose work in precursor disciplines, professional networks and methodological alternatives bolsters the credibility of the initiative. Unlike the natural language models that are currently being championed by Google, OpenAI, and other technology titans based in the United States and UK (see below), this project openly embraces "general purpose artificial intelligence." It is strategically located in Beijing's Haidian District near Peking University and Tsinghua University, which fosters interaction between the three institutions, whose programs and ambitions are aligned. According to a 2023 report, the program's aim are to replicate all aspects of human cognition, although on a more granular level, it endeavours to build new AI theories and paradigms, resolve "cross-media bottlenecks," and create general purpose artificial intelligence operating systems, general purpose agents, and associated training and testing platforms. These platforms are intended to facilitate a plethora of applications, and will support three-dimensional simulation training, data acquisition, autonomous robot hardware development, high-performance graphics process computing, and audio-visual psychological experiments, among others.

Similarly, the MOST and the National Natural Science Foundation of China launched an AI for Science Program in March 2023, which is intended to accelerate the adoption of AI in science and technology research amid intensifying technology competition with the United States. Xu Bo, the director of the Institute of Automation at the Chinese Academy of Sciences, leads the project, which will attempt to leverage AI to overcome major problems in basic disciplines and research, such as drug development, gene research and biology breeding.

The US's AI development industry:

The United States is the world leader in AI technology and its AI ecosystem is growing rapidly. According to a recent study produced by McKinsey & Company, AI adoption in the corporate sector in the United States increased from just 20% in 2017 to more than 50% in 2022, largely because the dominant industry participants are experiencing higher returns due to their adoption of AI.

The AI ecosystem in the United States has benefitted from a concrete technological and infrastructural foundation and a first-mover advantage in research and AI-oriented economic practices. AI companies first emerged in the United States in 1991, with the first Chinese AI company established in 1996. Furthermore, a substantial proportion of AI companies in China have only emerged during the last few years, with 20.8% of current AI start-ups founded in 2014, 34.5% in 2015, and 16.7% in 2016.

In the same way that China's AI ecosystem is primarily dominated by Baidu, Alibaba, and Tencent, IBM, Microsoft Corporation, Alphabet Inc. (Google), and Amazon.com, Inc., are the leading AI firms in the US's AI ecosystem and dominate the market.

Established in 1911, IBM was the first global leader in computing and became one of the first large technology firms in the United States to pioneer AI technology. Today, it is a global leader in terms of technology innovation and scalability and offers enterprise-grade products and services across numerous verticals.

Alternatively, Microsoft, Alphabet and Amazon Web Services (AWS) – a subsidiary of Amazon.com – have been able to effectively leverage their cloud service offerings – on which AI applications are built – to shield themselves from competition levied by small, disruptive vendors, although they also engage in rigorous competition with one another. Microsoft's AI offerings are built upon its Azure platform – the largest commercial cloud business in the world – and the firm's strengths are rooted in its integrated distribution models, extensive research and development activities, and secure financial performance, which allows the firm's top management team to reallocate capital to develop its burgeoning AI applications. Crucially, since 2019 Microsoft has also invested $13 billion (USD) in Open AI, the San Francisco-based AI company responsible for developing the generative GPT-4 technology that drives ChatGPT, which has empowered it to collaboratively develop a new chat technology called Bing that allows people to converse with AI as part of its search engine. Alphabet Inc., Google's parent company, is a global technology company that provides search and advertising services, operating systems and platforms, as well as business-to-business (B2B) software and hardware products.

Google is currently endeavouring to leverage its existing AI capabilities to differentiate itself within the cloud-computing market, which it views as its best bet for growth as its core search business continues to mature. As such, the firm's computing unit – Google Cloud – began offering consulting services in June 2023 to help clients utilise generative AI to identify trends, summarise information, boost automation, and generate content as businesses across various industries attempt to exploit the advantages associated with the new technology. Google also leverages AI technology to offer consumer-facing products, such as Waymo, its self-driving car service, and recently established a partnership with the Mayo Clinic to expand its use of AI in healthcare.

In much the same way, AWS provides cloud infrastructure services to established enterprises, start-ups, and public-sector entities. The firm has been able to leverage its cloud computing capabilities and data assets to develop AI services that utilise AI-enabled vision recognition to analyse videos and images, but also constructed automated data extraction and analysis services, language-based AI services such as chatbots and speech recognition, and automated data analysis and forecasting services for businesses. Following the launch of ChatGPT, AWS entered the generative AI race by launching a cloud service called Amazon Bedrock that developers can utilise to enhance their software systems with AI that can generate text in a way that closely resembles ChatGPT. Through its Bedrock service, AWS endeavours to offer access to its own first-party language models called Amazon Titan, as well as language models from AI21 Labs, Anthropic and Stability AI, which are all start-ups with technology that allows AWS to aid search accuracy and personalisation, and generate text for blog posts, emails, and documents. Crucially, Amazon.com also utilises AI to build, deliver, and operate physical products, especially through the use of warehouse robots, though the technology primarily drives two of its popular products: Alexa and the Amazon Go Store.

Meta Inc., formerly Facebook Inc., is also in the process of launching generative AI features, although the company's new products will primarily compete with those offered by Google and Microsoft rather than those developed by AWS. On June 8, 2023, for example, Meta's employees were introduced to new products that the company had been developing, which include ChatGPT-like chatbots for Messenger and WhatsApp that will allow users to converse using different personas, as well as a new feature for Instagram that will allow consumers to modify photos via text prompts and create emoji stickers for messaging services. Despite such initiatives, Meta has struggled significantly during the last two years. In 2022, its market value plummeted by approximately $89 billion due to a disappointing earnings report, and the firm has cut approximately 21,000 jobs since November of that year. Since OpenAI launched ChatGPT in November 2022, more than a third of the firm's published AI researchers have left the company, citing burnout and a lack of confidence in Meta's direction and leadership as the dominant reasons for leaving. More recently, the Biden Administration declined to invite Mark Zuckerberg and Meta's leadership to a summit meeting in early May 2023, which was arranged to allow White House officials to discuss AI development with the "CEOs of four American companies at the forefront of AI innovation" as regulators from around the world increasingly scrutinise the new technology and its societal significance.

Most recently, Apple Inc. announced that it has built its own framework - "Ajax" - to develop large language models, and it is also testing a new chatbot service that some engineers have termed "Apple GPT." Although the technology giant has integrated AI into some of its existing products, such as Apple Photos, device texting, and Vision Pro, analysts report that the firm still lags behind its major competitors in incorporating the new technology.

Crucially, these technology titans have established AI labs around the world during the last decade, especially in Asia and Europe. Facebook, Google, IBM, and Microsoft, for instance, had 62 labs conducting AI R&D as of 2020, 68% of which were located outside of the United States. Apple, DeepMind, (a subsidiary of Alphabet that was recently merged with Google Brain) and OpenAI, which has received more than $1 billion in funding from Microsoft, have also established AI labs that are exclusively dedicated to AI development. However, some firms that are based in the United States, like Amazon, do not conduct AI R&D using a lab structure or own stand-alone labs, but instead integrate their R&D activities with their product teams. While some AI researchers believe that DeepMind, OpenAI, and Facebook have the top AI labs in the world, it is difficult – if not impossible – to compare their capabilities with those of Baidus and Tencent in China due to a lack of credible data.

In addition to the four major technology and AI firms operating in the United States, there were more than 2,000 active AI firms competing in the United States as of 2019. The AI ecosystem is dynamic, and new organisations and collaborations between firms continue to emerge as the field evolves. While the CPP has taken the lead on the development of AI strategies and projects and has directed substantial funding into a relatively small number of projects that appear to have the highest probability of the success, the private sector plays a smaller role within such plans compared to its role in the United States, where collaboration between industry and universities drives growth in the AI ecosystem. In terms of the amount of private AI investment, the United States maintains an advantage, as $47.4 billion was invested in AI companies based in the United States in 2022, which is roughly 3.5 times the amount of private AI investment in China ($13.4 billion). The United States also continues to lead in terms of the total number of newly funded AI companies, as those based in the United States received 3.4 times more funding than their counterparts in China.

Geographic Hubs, Key Metropolitan Areas and Academic Institutions

The AI ecosystem in the United States is concentrated into a relatively limited number of geographic aggregations and metropolitan hubs. According to a recent report from Brookings Institution, California's Bay Area – which includes the metropolitan areas of San Francisco and San Jose – is the state's largest centre for both AI research and commercialization. The region is home to two of the world's leading academic institutions in AI research, Stanford University and the University of California Berkeley, and leading companies that invest significantly in AI, such as SalesForce, Facebook, NVIDIA, and Alphabet (Google).

Moreover, the region exhibits a high capacity for innovation – as illuminated by the area's high patenting and start-up rates – which help translate research into efficient AI applications. Crucially, however, high-technology economic clusters have also emerged in 14 additional metropolitan areas, which, when combined with the California Bay Area, possess two-thirds of the nation's AI assets and capabilities. These areas include New York; Boston; Seattle; Los Angeles; Washington, DC; San Diego; Austin, Texas; and Raleigh, North Carolina – while five smaller metropolis – including Boulder, Colorado; Lincoln, Nebraska; Santa Cruz, California; Santa-Maria-Santa-Barbara, California; and Santa Fe, New Mexico – have established burgeoning AI ecosystems. Many of these regions benefit from the presence of national AI leaders like Oracle, IBM, Amazon, and CrowdStrike, and strong research institutions, which both create jobs, and help develop and deploy commercial AI applications by translating research innovations into high-growth companies. However, these regions are not exclusively dominated by large technology firms but also foster the emergence of agile start-ups and SMEs that engage in intense competition and, therefore, foster innovation.

Crucially, these clusters have benefitted tremendously from strategically targeted federal research funding and contracting activities, which have both helped propel innovation in the nation's research and contracting centres. Although AI research in the United States began in the 1950s, its growth has surged since 2010, so much so that federal research and development expenditures at universities and colleges in the United States have increased by 45% during the last decade. As AI science is still in a nascent stage of development, such investments are important as they allow academics and scientists to solve key problems, develop meaningful applications, and engage in higher-risk activities that are needed to drive innovation.

Federal-level research investments have substantially shaped the AI landscape across the United States, as the provision of capital into the nation's leading research and contracting regions has contributed to the growth and competitiveness of 21 highly productive metropolitan areas. These "federal centres" are generally characterised by relatively small populations and the presence of at least one major university or research institution; in fact, apart from Pittsburgh; Durham, NC; Madison, Wisconsin; and New Haven, Connecticut, many of these clusters contain less than 200,000 people and closely resemble "university towns." AI activities that take place within these regions are highly concentrated in major academic institutions, which illuminates the unique role of providing universities with public investment for advancing AI technology in relatively small geographic regions in the United States (see Figure 2). While these areas are especially competent at securing research funding, winning federal contracts and publishing in world-renowned AI journals, their activities are relatively confined to research as they exhibit low commercialization activities, contain fewer AI companies, and, therefore, create less jobs.

Industry Alliances and Associations

In the same way industry alliances and associations constitute a crucial component of China's AI ecosystem, they are also important in the United States. Not only do they provide a framework that fosters cooperation and joint planning, data sharing, and the dissemination of best practices, but they can also help rectify market failures by providing a platform for industry participants to mitigate AI-related risks, enhance the legitimacy of international action, and verify the development and deployment of safe and reliable AI. While it is difficult to determine how many AI-oriented industry alliances and associations exist in the United States due to the general paucity of data, there are nevertheless several major alliances and associations that occupy prominent positions in the nation's AI ecosystem.

The Partnership on AI is one such alliance. Established in September 2016 by Google, Meta, Amazon.com, Microsoft Corporation, and IBM, the non-profit organisation (NPO) is a community comprised of major technology companies, academic institutions, and non-profit organisations that collaboratively endeavour to address the major global challenges associated with AI – such as diversity, job loss, media integrity, transparency, fairness and accountability, and public safety – while promoting best practices to ensure AI benefits society. To do so, it operates five different programs, one devoted to promoting inclusive research and design, one to AI media integrity, one to AI labour and the economy, one to fairness, transparency, and accountability and another to AI and machine learning safety. The organisation benefits from partnerships with more than 105 academic institutions, NPOs, and technology companies which are primarily based in the United States, although some European, Canadian, and Australian entities – such as the Oxford Internet Institute, the Australian National University School of Cybernetics, and the Schwartz Reisman Institute for Technology and Society.

The AI Now Institute at New York University (NYU) is a new organisation that plays a key role in the US's AI ecosystem. Founded in November 2017 by Kate Crawford, a Senior Principal Researcher at Microsoft New York and Meredith Whittaker, a former Google employee who founded Google's Open Research Group before becoming the President of the Signal Foundation, the AI Now Institute is a NPO that produces diagnosis and actionable policy research to address the concentration of power in the technology industry. The organisation primarily produces research, and possesses 10 areas of expertise: algorithmic accountability, antitrust, biometrics & affect, climate, data minimization, global digital trade, labour and tech, large-scale AI models, privacy and competition, and the US/China AI race.

Older associations like the Association for the Advancement of Artificial Intelligence (AAAI) and the Institute of Electrical and Electronics Engineers (IEEE) are also crucial. Established in 1979 with its headquarters in Washington, DC, the AAAI is the premier non-profit scientific society in the United States dedicated to advancing the scientific understanding of the mechanisms underlying thought and intelligent behaviour, as well as their embodiment in machines. The organisation aspires to promote research in, and responsible use of, AI, to increase public understanding of AI, to improve the teaching and training of AI practitioners and to provide guidance for future AI researchers and funders. To do so, it organises and sponsors conferences, symposia and workshops – such as the AAAI Conference on Artificial Intelligence and the AIES AAAI/ACM Conference on Artificial Intelligence, Ethics and Society – publishes a quarterly magazine for its members, advocates for members throughout the world through educational programs, and awards grants and scholarships. Similarly, the IEEE was founded in 1963 as a professional association for electronics engineering, electrical engineering, and related disciplines, although it has since grown to become the world's largest technical professional organisation dedicated to advancing technology for the benefit of humanity. The IEEE operates a Computer Society (IEEE-CS) composed of more than 375,000 members from 168 different countries.

Impact of Industrial Policy

Chinese Industrial Policy

Ruyi Liu

Technological innovation is increasingly being featured as China's developmental pillar, demonstrated by its centralness to the 14th Five-Year Plan (2021–2025). In President Xi Jinping's Speech, he repeatedly emphasised the spearhead role of AI in the technological revolution. From 2017-2021, China launched 105 AI policy programmes. The New Generation Artificial Intelligence Development Plan (AIDP) published in 2017 marked the first national-level unified strategy of China's AI development. Quantitatively, this document sets three general goals(translation):

1. Create an AI industry worth over 150 billion yuan by 2020.
2. Achieve over 400 billion yuan growth in core AI industry by 2025.
3. Target 1 trillion yuan of growth by 2030.

In the short term, China aims to maintain access to foreign technology yet begin to mitigate its dependence. This goal is also reflected in the Made in China 2025 programme to enhance manufacturing power in the context of chip war with the US. The long-term mission, though not clearly defined, is to attain global leadership in AI technology. Categorically, the AIDP stresses key areas including international competition, national security, economic development, and social governance.

Advancement in AI constitutes an important part of the Chinese techno-security state tailored to national defence and strategy. The Chinese government paid particular attention to US AI strategy when formulating its developmental plans. The Chinese government regularly translates, distributes, and analyses AI reports generated by US administrations and think tanks. A notable example is China's focus on the introduction of AI in "military-civil fusion", following the US Department of Defense's announcement of an AI-related "Third Offset" strategy in 2014. China identifies AI as a military "leapfrog development" opportunity, which facilitates the long-term military strategy of upgrading its asymmetric capability in cyber warfare.

In addition to geopolitical pursuit, the Chinese government highly values economic competency driven by AI. This rationale is to consolidate the CCP's legitimacy which relies on delivering economic growth since the Open and Reform. Differing from absolute central planning, the Chinese state seeks to promote market-oriented principles and encourage entrepreneurship and competition. As such, the executive principle of AIDP highlights the division of work between the state and private sectors, as well as coordination between central and provincial governments in the Three-Year Plan.

This AI developmental blueprint outlines an integrated model of AI innovation with close cooperation between academy and industrial enterprise under the guidance of the state. The Chinese AI development strategy conforms to the model of "fragmented authoritarianism", whereby the central government drafts overarching objectives and disseminates overarching missions for local agencies to implement. President Xi personally takes charge of decision-making bodies, notably the Central Military-Civil Fusion Development Committee and the Central and Cyberspace Affairs Commission. This personalised attribute reflects a top-down approach. However, power sharing within the State Council responsible for AI development causes chronic bureaucratic infightings and coordination problems. With 15 agencies involved in the AI Implementation Office, each sub-entity pursues their own programmes to claim a stake in AI development. The AIDP was issued under the authority of the Ministry of Science and Technology (MOST), which mentioned no other agencies within the State Council. The Ministry of Industry and Information Technology (MIIT) then released its own Three-Year Action Plan in December.

The top-down command is also undermined by uneven performance of local governments and competition among regional agencies. After the announcement of AIDP, over 15 provincial units proposed their own local AI policies. The local policy initiatives may not necessarily respond to central directives in a passive manner. Instead, they have their own objectives, prioritising regime stability and regional development . For instance, the province of Guangdong had announced its own '2015–2020 Intelligent Manufacturing Development Plan' in February 2016 even before the publication of AIDP. It is suggested that the central government recognised local initiatives and upgraded them into the national plan. This development demonstrates a combination of bottom-up and top-down approach.

Figure 1: **Local versus central government document creation.**

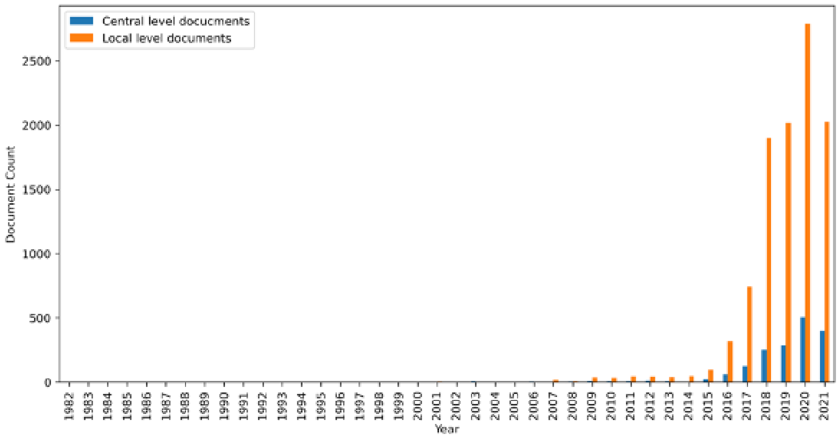
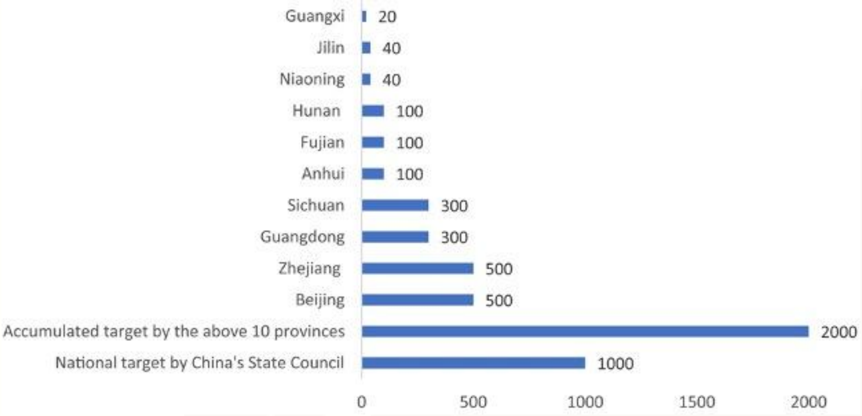


Figure 1. Frequency Distribution of China's local- and central-level policy documents mentioning "artificial intelligence" over time.

Similarly, before being identified as national champions in AIDP, private high-tech enterprises such as Alibaba, Tencent and Baidu have already led their own AI innovation projects. Their concern may be more about market forces and profit-earning behind the AI economy than the state's strategic interests. As such, China's AI planning shows a certain degree of self-motivating autonomy beyond Beijing's instructions.

Figure 2: **Summary of Chinese provincial-level unit target values of AI-related industry by 2020 (unit: 1 billion yuan)**



The Chinese state provides financial assistance to AI programmes. Subsidy schemes include the Central Financing for Science and Technology, a regular central budgetary institution, and The Multiplied Pre-Tax Deduction of Research and Development Expenses for Enterprises, a tax scheme that allows 150% deduction of research expenses for private companies. Research reveals that the state annually supplies a few billion dollars to private-sector AI activity through guidance funds. However, guidance fund investment faces problems such as uncertainty, poor quality and exaggeration.

State funding for AI programmes also follows an unbalanced pattern. "First-tier" cities such as Beijing, Shanghai and Shenzhen receive the most investments, yet they already have well-established research centres compared to inner-land regions such as Guangxi. Less-wealthy provinces may not have critical resources to invest in AI projects. The fragmented governance structure entrenches this developmental gap, whereby the responsibility to execute the central government's goal falls to provincial authorities.

To achieve the goal of global leadership in AI, China has been actively building a state-led AI regulatory framework in partnership with industry and academia. In November 2021, the Ministry of Foreign Affairs released the *Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)*. This document laid out China's ambition in global governance of AI and critical aspects: regulation, Research and Development(R&D), Utilisation and International Cooperation. It also reinstates the importance of national ethic norm, which was first published as New Generation Artificial Intelligence Code of Ethics on 25 September 2021 by MOST. The AI ethic includes the idea of "agile governance" to timely address risks associated with AI and incorporate industry standards into national legislatures. Examples of consultation with non-state stakeholders include Toutiao's Technology Strategy Committee which reviews the internal ethics board and Beijing Zhiyuan Institute of Artificial Intelligence. Although China does not have a unified set of laws, there are several bills under discussion.

Apart from MOST's AI ethics principles, the state takes two other approaches to AI governance. The first draws on rules for online supervision under Cyberspace Administration of China (CAC). The other concerns with the development of "trustworthy AI" systems similar to the US and EU by China Academy of Information and Communications Technology (CAICT). CAC deploys a "vertical approach" to target a specific AI application and every processing stage. It became the first in the world to regulate deep-fake technology through Deep Synthesis Provisions in January 2023, addressing algorithmic transparency that the EU has long debated. By utilising the existing algorithm filtering system, CAC also quickly reacts to generative AI model ChatGPT. However, CAC's regulatory regime serves political censorship and enacts political alignment for private companies. Privacy guidelines only target potential malicious agents, with full access of data in the hands of the state. While sponsored by the state, the CAICT's operation appears less clear because the MITT for which it represents has yet to issue its own policy documents. It thus evokes speculations about bureaucratic struggles behind the scenes.

US Industrial Policy

Parul Wadhawan

Despite the US leading in AI research, development, and investment, the AI regulatory landscape in the US is far from robust or centrally organised. In April 2023, the US Commerce Department's National Telecommunications and Information Administration (NTIA) issued a call for the public's feedback on: "how should 'AI' be defined?," "how to create accountability measures for AI?," and "Should the government vet AI systems before they are released to the public?" At this point in time, the key tenets of Washington's AI policy framework include the 'Blueprint for an AI Bill of Rights', which sets out voluntary AI ethical principles, NTIA's AI risk management framework which sets out voluntary guardrails for companies to adopt when deploying AI systems, and other federal legislation which touch upon the specific risks of AI systems without explicitly regulating AI itself.

AI regulation is still nascent in the US. In October 2022, Washington published the Blueprint for an AI Bill of Rights, a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence. According to the official text, it is "intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems." The blueprint, at the time of publishing, is not legally enforceable and appears to be a skeletal guidance for future policy. As such, it holds potential to influence domestic legislation and regulation. Some analysts in the field perceive it as a "toothless tiger" due to its lack of enforceability, but arguably it offers the US two key strategic advantages: 1) it provides some 'soft' national framework in place to guide behaviour, 2) but allows them to observe how AI regulation in the EU and China plays out.

Following the NTIA's calls for public feedback, the draft text of the Transparency Governance Act was introduced to the US Senate on 7 June 2023. The bill proposes a legal requirement for US government agencies to be transparent when using "automated systems" to make "critical decisions." Although the bill may be deemed as further progress in the US federal AI regulatory process, several factors continue to impede the process, including, but not limited to, political and bureaucratic impasse. Since 2021, only 12 out of 222 AI-related federal bills have been passed.

Experts indicate that the US tends to approach AI as an added element of already regulated tech sectors and is currently lagging behind in regulation as opposed to the EU and China. Washington wants to minimise the harms that AI can cause, but without stifling the innovative brio of its industry-leading tech giants. However, policymakers in Washington are not just charting the path for establishing the nation's supremacy as an AI leader but also to set the rules for how it is likely going to be used around the world. The stakes are particularly high for the US as its regulatory framework will determine the trajectory of democratic values and the concept of open societies in the AI race.

According to Ben Winters, a senior counsel at the Electronic Privacy Information Center, a privacy research nonprofit, federal efforts to address AI have so far largely resulted in additional funding to develop "ethical" AI. In this scenario, the lack of leadership on the issue in Washington has resulted in the sector room having to govern itself. For instance, Sam Altman, CEO of OpenAI, suggests creating licensing and testing requirements for the development and release of AI tools, establishing safety standards, and bringing in independent auditors to assess the models before they are released. Those proposed regulations would ultimately amount to little more than self-regulation, per the AI Now Institute. Amid the lack of urgency from US lawmakers and the administration, digital rights experts are looking at existing law and efforts at the state level to put guardrails on AI. New York, for example, will require companies to conduct annual audits for bias in their automated hiring systems, as well as notify candidates when these systems are being used and give applicants the option to request the data collected on them.

As such, states are developing their own AI legislation, with the top three states being Maryland, California and Massachusetts with the largest quantity of AI bills passed. Currently, California is ramping up state-level regulation on AI to set up guardrails for Silicon Valley, home to many of the world's leading AI companies. On 10 February, the California Civil Rights Council (CCRC) proposed amendments to California's employment law, proposing that: Employers cannot buy/use/administer (and vendors cannot sell) "automated decision systems" (ADM) that discriminate based on "protected characteristics" unless they are shown to be related for the job position in question and are consistent with business necessity. Given that these state laws mostly focus on AI within a specific context rather than setting a comprehensive AI framework, the US AI regulation has yet to be streamlined and centralised, with the federal and state governments currently undertaking independent and unaligned initiatives. This has led to inconsistent regulation across the country, thereby engendering a confusing policy environment for businesses who have operations across the US.

Increasingly, the "command and control" Chinese economy, oft-derided for its lack of a state-private division, is juxtaposed with the freedom of private enterprise in the Western liberal political economy via the "arms race" rhetoric to impede prospective over-regulation by Washington. However, the advancement of US industrial policies in the area of AI and similar strategic technologies intended to address the arms race make this distinction increasingly untenable. In essence, the designation of AI as a strategic national asset would ultimately fuel the competitiveness between the largest technological companies, majority of those being based out of the US, and shield these firms from structural regulation.

Essentially, the "AI race" with China has likely been the most productive justification for the proliferation of policy tools that improve government support and funds for the development of AI. Although the term "industrial policy" has historically been unsettling and divisive in US politics, it is now enjoying rising bipartisan acceptance, reflecting a growing tendency in US politics to link the national interest with the flourishing of particular economic sectors of the country. China regulates its industrial policy through top-down, five-year plans, in contrast to the US. The ultimate goal is to make China into a militarily strong and technologically advanced state that can contend with US commercial and military dominance. Beijing has also developed a complex ecosystem for public-private funding to support these goals. In contrast, the US economy's planning has recently been left to "the market." China's top-down national industrial policy, according to Steve Bank, an adjunct professor at Stanford, implies that the US is being out-planned, out-manned, and out-spent by China. This results in a striking contrast: China is implementing a state-orchestrated industrial plan, which is helping it quickly become a dominating economic and technological force, while the US is responding with a lack of clarity on whether or not the adoption of an industrial policy is the desired regulatory approach vis-a-vis AI.

Deepdive: Sectoral Competition

Gabrielė Eidėjūtė-Strong and Piotr Malachinski

Artificial intelligence is a broad umbrella term that includes multiple computer abilities to perform tasks that typically require human intelligence. Treating it as a generalised topic with a homogenous development landscape makes it hard to evaluate who is truly in the lead. This section aims to break up the broad term into several main types of AI research and discuss key strategies and current development bases in both countries.

The chosen sub-fields of AI are Natural Language Processing (NLP), Computer Vision (CV), and autonomous vehicles (AVs). Although the body of literature discussing AI development provides various categorizations, the three selected types encompass a wide range of applications and showcase AI in critical domains of language, vision, and mobility.

Natural Language Processing

NLP focuses on enabling machines to understand, interpret, and generate human language. It includes speech recognition, sentiment analysis, language translation, text summarization, and chatbots. NLP software can use a variety of techniques, including rule-based systems, traditional machine learning, deep learning, and more recently, Large Language Models (LLMs). LLMs, which are a form of deep learning model, have achieved unprecedented performance on a wide range of LP tasks. They require substantial amounts of training data, with models that can range from millions to even trillions of parameters. The rise of LLMs represents an exciting development in the field of LP.

LP technology first pre-processes the training text to standardise its form for easier analysis. This usually happens through the process of tokenization, which involves breaking down the text into smaller units like words and sub-words, known as tokens. These tokens are often then converted into vector representations, or embeddings, that capture their semantic meanings. In the case of deep learning techniques and LLMs, these embeddings are processed by the neural network - a computing system that emulates the interconnected structure and function of neurons in the human brain - to perform various language-related, logical, analytical or creative tasks. The power of LLMs lies in their ability to generate human-like text, understand context, and provide useful responses or perform tasks based on the input they are given.

Some of the most popular real-world applications of NLP include voice-controlled assistants like Alexa or Siri, writing assistant Grammarly, and the most recent viral sensation OpenAI's ChatGPT chatbot, among others.

Given the vast applications of natural language processing technologies, this is the area where the competition between China and the United States is the most apparent especially given ChatGPT's popularity. Chinese state-run media outlets have expressed that the US authorities may use AI chatbots developed by Western countries to "spread misinformation and manipulate public opinion, " so they quickly blocked these applications in China. It strives to create competitive alternative models specifically designed for the Chinese market and would comply with the censorship rules and regulations.

In terms of the number of large-language models (LLM), the US has always been in the lead. However, since 2020, China has stepped up its NLP development and released 79 large-language models in total. This year, China is taking the lead with 19 LLMs compared to 18 LLMs developed by the US. Most Chinese chatbots like the Ernie Bot developed by the Chinese search engine Baidu, or Alibaba's chatbot Alime, despite being widely used in customer service and beyond, fall short of US' ChatGPT, which uses GPT-3.5 LLM. Due to their shortcomings, some observers claim that the fears of China catching up to the US are blown out of proportion. However, interestingly, not much media attention has been given to China's AI large-language model called GLM-130B. According to its creators at Tsinghua University, it outperforms the GPT-3 in a "wide range of popular English benchmarks". It is deemed by some to be the "most capable" AI language model to date. Looking at its scores at well-acknowledged benchmarks that the creators used, it does appear that the GLM-130B is very competitive at generative tasks, natural language understanding (NLU) tasks, and multilingual tasks. The latter is especially important since the GPT-3 tends to underperform when generating non-English content.

Moreover, contrary to widespread criticism of China's AI development, stating that its research lacks originality and creativity, GLM-130B is not just a Chinese copy of GPT-3. Its design architecture is distinctively different from Western models, using a bidirectional GLM (General Language model) as its backbone instead of only the autoregressive GPT model used by most LLMs. Also, unlike the GPT-3, Tsinghua University's created GLM-130B is open-source and locally runnable on a single consumer GPU due to its small memory footprint. It is currently available on GitHub; however, as it is a raw language model without a chatbot application, it requires training to operate.

Despite China's strides in catching up with the US' NLP development, its strict censorship policies may be why it will remain behind. The censorship rules and demanding regulatory regimes make it difficult for Chinese companies to develop models that could navigate political redlines while still being effective. Before launching new chatbots, companies have to get government approval so they will not potentially generate content undermining the CCP. For example, Baidu's Ernie Bot, created as a response to ChatGPT, refuses to answer a wide range of questions on Chinese politics.

While the focus is often on the spread of disinformation and public opinion shaping, large-language models can also revolutionise military operations. Instead of drawing operation plans on a whiteboard, military personnel could ask a trained Chatbot to provide calculated options, as vividly illustrated by the War on the Rocks commentary. Similarly, American Tech Company Palantir described a scenario wherein military personnel using their software (that allows operating LLM on private networks) could ask the chatbot to generate plans of attack or organise jamming of enemy communications.

Although China is emerging as a worthy competitor in NLP technology and generative AI, most sources still consider the US the leader in this field. Indeed, many of the world's best-known Large Learning Models (LLMs), accessible as chatbots that respond to user-drafted prompts, are owned by Big Tech companies native to Silicon Valley. One state-of-the-art example is ChatGPT, developed by a once-non-profit OpenAI which is also available in its commercial version GPT-4. There are other notable examples – Anthropic, founded by former OpenAI employees, has created a chatbot called Claude, while Google, a shareholder in Anthropic, is developing Bard – an LLM based on the LaMDA technology. A notable characteristic of LLM products developed by American companies is their sensitivity to content deemed harmful.

All the major chatbots are designed to reject prompts deemed offensive or dangerous, but the approach varies depending on the product. For example, ChatGPT has a defined set of offensive, dangerous, or vulgar themes that it refuses to discuss, while Claude was trained through the "Constitutional AI" process, where responses to curated harmful prompts were critiqued by human supervisors in the initial training stage.

In addition to commercial chatbots, novel NLP technology is also being developed in the public sector. The Intelligence Advanced Research Projects Activity (IARPA) has launched several initiatives to create AI-powered tools that would enhance the analytical capabilities of the intelligence community. Many of these projects integrate NLP with Automatic Speech Recognition and Machine Translation to better understand the intentions of individuals from non-English speaking countries that are of interest to the US. One such initiative is the MATERIAL program launched in 2017, which aimed to develop a method of automatically analysing foreign-language media for relevant information and identifying potential threats to US national security.

Computer Vision

CV deals with AI systems that can interpret and understand visual information. It includes tasks like object recognition, facial recognition, emotion recognition, image classification and segmentation, and video analysis. Computer Vision applications are incredibly vast and increasingly controversial. Starting with benign applications like helping social media users to tag photos of their friends, to more complex applications like medical diagnostics, helping autonomous vehicles, population surveillance, and target detection.

Computer vision has an extensive array of applications, ranging from benign uses such as helping social media users tag photos of their friends and to more complex ones like medical diagnosis and industrial robotic automation. The use of such technology by private companies may pose important ethical questions; for example, various American tech giants, from Google to Facebook and IBM, have already patented emotion recognition technology to boost their marketing abilities.

Moreover, as technology advances, further controversial applications have emerged, such as population surveillance and target detection through facial recognition. In the US, no regulatory framework on facial recognition technology exists although there are certain state and city-level laws limiting its use by public authorities. For example, strengthened government oversight of the FRT use by law enforcement has been imposed in Utah and Massachusetts, while Maine and Vermont banned the public-sector acquisition and use of such technology also completely. Nevertheless, facial recognition is increasingly being used by law enforcement agencies – surprisingly, to the relative approval of the population. According to the Government Accountability Office, roughly half of its 42 federal agencies now use facial recognition technologies to enhance their law enforcement capabilities, with Clearview AI being the primary supplier of the necessary technology. In the field of security and intelligence, again, one of the primary organisations at the forefront of computer vision technology development is IARPA. Among its initiatives, the DIVA (Deep Intermodal Video Analytics) project focused on analysing long CCTV video footage in search of suspicious movements.

Despite the US's significant investments in computer vision technology, research and development in this field has fallen behind that of China's. Numbers show that Computer Vision is a priority area for China. According to CSET reports, 39 percent of all Chinese AI research output and 37 percent of all Chinese AI patents are in Computer Vision (Compared to 23 percent of US AI patents in computer vision). The focus on Computer Vision research seems to pay off, placing it ahead of the US in patent applications and granted patents as well as the research output and citations in both computer vision and surveillance AI. Moreover, Chinese firms hold a leading position in the Face Recognition Vendor Test (FRVT) ranking conducted by the National Institute of Standards and Technology. This test is widely recognized as the standard for assessing the precision of facial recognition systems.

Although specifically surveillance tasks constitute a relatively small fraction of computer research output as a whole, the trends show that sub-areas of person re-identification, face spoofing detection, and crowd analysis have been experiencing exceptionally high growth rates (more than 30 percent annually) in China, compared to overall computer vision research growth. In 2019, Chinese researchers published nearly half of global research on crowd analysis and facial spoofing detection.

Observers argue that Democratic countries have an inherent disadvantage in Computer Vision research and development due to the expected norms of privacy, dignity, and respect for human rights. As Svenja Hahn, a German member of Parliament for review, told Politico, facial recognition for mass surveillance has no place in liberal democracies. On the other hand, authoritarian regimes like China do not suffer from similar inhibitions. As Harvard Economics Professor David Yang pointed out, AI is fundamentally a technology for prediction, and "Autocratic governments would like to be able to predict the whereabouts, thoughts, and behaviours of citizens."

One of China's most well-known strategies, which heavily relies on its CV R&D, is to establish a social credit system – a big data-fueled mechanism - to surveil and 'rate' its population, leading to different treatment of individuals based on the rating they receive. Although China has not fully developed nor fully implemented the system, the future scenario where it succeeds in this goal resembles an Orwellian dystopia. A significant concern is the potential export of such systems to other similar regimes or countries experiencing democratic backsliding. From a military perspective, technological advancements in Computer vision are a revolutionising element. It can Enhance Target Detection and Recognition, analysing visual data from various sources, including satellites, drones, and surveillance cameras, to detect and recognize targets in real-time. Computer vision advancements are often in symbiosis with autonomous military system development; therefore, it will be further discussed after the AV section.

Autonomous Vehicles

AVs rely on AI technologies like previously explored computer vision, sensor fusion, and machine learning to partially or entirely replace the human driver. Ironically, the goal to replace the human driver is what "drives" the AI development in the automotive industry. The deployment of more autonomous vehicles would reduce human error and impaired driving on the roads, making traffic not only safer but more energy efficient.

China is late to the game with its AV development and AV testing regulations; however, it is moving fast. According to China's market projections by Mckinsey Center for Future Mobility (MCFM), the automotive, transportation, and logistics sectors have the highest potential economic value from AI.

China has established concrete strategies to integrate autonomous vehicles into its streets to help it catch up with the race. By 2025, China aims to achieve large-scale production of conditionally automated L3 vehicles and market launch L4 vehicles. It also aims to set up transportation systems called C-V2X, underlining the concept of "human-vehicle-road-cloud," which enables vehicles to connect with other vehicles on the road, the road infrastructure, people, and networks.

To achieve this goal, China has been continuously making testing, deployment, and future commercialization of AVs easier. By the end of 2021, Chinese local governments had built more than 20 new test zones and had designated more than 3,500 kilometres of public road for autonomous-car testing. AVs have been widely used during the coronavirus pandemic to transport medical supplies and food. The Chinese government provides more flexible policies for AVs developing companies to enter the roads. Its Tech giant Baidu has been testing their self-driving taxis in over ten cities nationwide and claims to have completed 1 million rides during the last five years. An important step for implementing AVs will be customer acceptance and awareness of the benefits of the technology. Chinese consumers are more enthusiastic about purchasing autonomous vehicles and are more likely to embrace autonomous driving. On the other hand, nearly half of Americans believe that "widespread driverless cars would be bad for society." More positive attitudes could be the reason why driverless cars will go mainstream in China before it does in the US. China is projected to surpass Europe and the USA in Level 2 autonomous driving sales by 2025.

As pointed out in a CSIS discussion, the hardware used for vehicles with driver assistance features, like cameras and sensors, are also the building blocks for highly autonomous vehicles. So, the more data one has on the performance of those building blocks, the better equipped one will be to develop even more advanced systems – systems that can be used not only for civilian purposes.

According to 2021 CSET estimations, China's People's Liberation Army (PLA) was spending up to 2.7 billion USD on AI research, approximately the same as the US. The priority area for the PLA is the development of AVs, with a specific interest in sub-surface and aerial platforms. Last year China launched the world's first crewless drone carrier that can operate autonomously in open water, nicknamed the "mother ship" by the Western media. Beijing claims its purpose is for scientific maritime exploration; environmental monitoring, which contributes to natural disaster mitigation. However, China hawks believe that its explorations in the South China Sea – a highly contested area, are backed by alternative motives. By emerging as a leader in applying AI to military technology uses, China aims to reset the landscape of conventional military competition. Whether it will be successful will depend on continued investment and experimentation robustness in the PLA that could be affected by the potential economic slowdown.

The deployment of more autonomous vehicles has the potential to reduce human error and impaired driving on roads, making traffic safer and more energy-efficient. However, despite the possible benefits of AVs, American society is more concerned about this technology than facial recognition technology used by the police. According to a survey conducted by Pew Research Center, 44% of respondents believed that AVs were a bad idea, while only 26% had positive views of the technology.

Many of the leading companies that produce cars and delivery vehicles with autonomous or semi-autonomous driving systems are based in the US. Tesla, founded by Elon Musk, is considered by many to be the leader in "driverless" technology, despite criticism of the company's promises of full vehicle autonomy still far from being achieved. Other major players in the field include Waymo, a subsidiary of Google's parent company Alphabet, or Nuro – a start-up focused on autonomous delivery vehicles, which has partnered with companies like Domino's Pizza and Kroger to develop and test its technology. Cruise, a subsidiary of General Motors, is also developing autonomous vehicles, and many other established American automakers, such as Ford, are investing heavily in this emerging field.
Among the types of AVs, unmanned armed vehicles, or armed drones, are of special importance to the national security authorities. As of 2023, the US military operates around 11,000 UAVs according to the Department of Defense – the largest armed drone arsenal in the world. While no fully autonomous drones are currently in use besides loitering munitions, many armed drone systems are currently powered by AI technology to improve and partially automate their use, and this level of drone autonomy is poised to increase.

Project Maven is a notable example of cooperation between Silicon Valley and the military-industrial complex, with the Pentagon leading the ongoing initiative to develop comprehensive video analysis and target detection capabilities for armed drones. Google's AI technology supported this between 2017 and 2018. The project aims to enhance the capabilities of the US military's drone fleet and facilitate more precise and effective targeting, particularly in combat situations.

Evaluation

China has made significant strides in the AI development race against the US. It has increased its development efforts for NLP and large-language models (LLMs), however, most of them still underperform when compared to US variants. American LLMs such as ChatGPT and Claude remain the most technologically advanced language models to date, placing the US at the forefront of the NLP market. One exception is China’s relatively under-discussed GLM-130B, which supposedly outperforms GPT-3 and shows originality in its design architecture. Nevertheless, Western states should not take shortcuts in AI regulation policy creation in fear that China would speed up as they slow down, since its strict censorship policies will most likely slow it down and limit its ability to compete globally.

Most notably, China seems to be in the lead regarding Computer Vision development. Various democratic countries face constraints due to privacy norms, and the United States is not an exception. Although there exist no regulations on a federal level, numerous states have limited the use of facial recognition technology by public authorities, some going as far as banning it completely. Meanwhile, China's authoritarian regime allows it unrestricted development and deployment of surveillance systems. This may explain why Chinese firms are at the forefront of facial recognition technology. Two main risks arise from China's leadership and technological advancements in Computer Vision. First, the export of China's high-level 'big-brother' surveillance systems to other authoritarian regimes or weak democracies could lead to widespread violations of human rights. Secondly, CV is incredibly applicable to military purposes - an asset equally recognized by the US military and intelligence community, as shown by their various ongoing R&D projects. The PLA will surely take advantage of the CV benefits, including automated target recognition, which is crucial for over-the-horizon targeting and faster decision-making.

Regarding AVs, China has started relatively late but has been rapidly catching up. Its increasingly favourable regulatory framework and generally more positive consumer sentiment could potentially make China the Top Autonomous Driving Mobility Hub. Autonomous systems also seem to be a priority for PLA military modernization, which is already showing results, although its autonomous weapons arsenal is still only a fraction of that of the US. Whether China can become a leader in military AI, equipped with unmanned systems that could challenge US supremacy, depends on economic factors such as a potential slowdown impacting China's GDP and chip supply.

Although the United States may still be "winning" the AI race, this is becoming more complex to determine, with US dominance no longer the case across all subfields. Whereas the country's arsenal of AI-powered tools from commercial language models to autonomous weapons systems remains unrivalled, Privacy concerns have constrained the American advancements in Computer Vision technology, lagging behind its Chinese in this area. Overall, China's AI development indicates its strong commitment to technological advancement, which may have significant implications for global leadership, information warfare, military capabilities, and international security.

Horizon Scanning: Emergent Risk from the AI Competition

Risk one: The competition for military modernisation

Kateryna Anisova

The international competition to build military AI might intensify into an all-out arms race, with the US and the PRC as the main actors to lead the course of AI militarisation. The absence of an international system of regulation and limitations on the development and use of artificial intelligence in the military sphere creates the risk of an uncontrolled arms race, which will have direct consequences at the level of strategic confrontation between the great powers, the nature of possible wars or conflicts escalation, the threshold for the use of force and less attention to and negligence of safe measure or/and reliability of the system.

From a broader perspective, the coming AI arms race is part of the ongoing Sino-American geopolitical and geostrategic confrontation, where the military dimension of technology development plays a crucial role. In Chinese strategic vision, military modernisation closely intertwines with technological advancement and innovation. China has considerably increased its share of global investment in research and development, with a Chinese share of 24.8% in 2020 (4.9% in 2000) compared to the declining US share of 30.7% in 2020 (39.9% in 2000). By 2026, China is anticipated to have approximately $27 billion invested in AI, specifically, a more than twofold increase. As a result, China will be responsible for 8.9% of all AI investments made worldwide in less than 15 years.

With the military regard, China has a clear military modernisation objective: to surpass the US in terms of the sophistication and advancement of its military technology instead of catching up with the size of the American military. Moreover, China strategically aims to shift from land-based territorial defence to space, cyberspace, and the far seas. In line with it, the plan for the People's Liberation Army's (PLA) modernisation by 2050 includes 'intelligentisation'. The recently established PLA Strategic Support Force (SSF) hybrid branch of the People's Liberation Army encompasses cyber, electronic, space and psychological warfare elements. Although the SSF's exact goal is not officially declared, the SSF looks to be at the vanguard of the PLA's efforts to modernise around cutting-edge technology like AI.

Senior PLA officials and strategists have already published several papers demonstrating desired fields for deploying AI in four key areas. It includes the development of unmanned weapons' autonomy, speeding up big data proceedings and military decision-making, and even cognitive warfare. Moreover, various Chinese journal articles study other possible applications of AI, such as intelligent munitions, AI empowering of intelligence, surveillance, and reconnaissance (ISR) software, automated cybersecurity and cyberattack software.

The U.S. security and defence concerns over Chinese AI development drive American officials to resist and constrain Chinese access to critical infrastructure. For instance, the last year's export restrictions on chips were the most successful in this regard, due to the well-known Chinese inability to design and produce sophisticated logic and memory chips, which are needed to train AI systems. However, such restrictions in a longer perspective might harm American domestic chip companies, significantly decreasing their revenues and thus capabilities for further research and innovation of new chips.

Considering, firstly, the traditional US pioneering role in the militarised AI development and its decisive goal in ensuring ongoing global technological and, thus, military dominance; secondly, the strategic importance of AI development and its currently prioritised position in Chinese military modernisation with increasing budget expenditures, and, finally, the overall Sino-American comprehensive tensions gives a solid ground to assume that Sino-American AI arms race is likely to be inevitable. As the US Department of Defence stated, “AI is poised to change the character of the future battlefield.” AI systems substantially broaden the scope of warfare, variety and performance of military and hybrid operations and even the way of data gathering, analysis and decision-making, enabling to surpass human cognitive capabilities in terms of speed, accuracy and adaptability to new information. Consequently, the country with the most advanced AI sector will gain a decisive strategic advantage, indeed, not only in the military sphere but from the perspective of the overall Sino-American strategic competition.

The lack of transparency in AI development and high reliability on the open-source analysis is already causing mis-/overestimation of the adversary’s capabilities, particularly in the case of the Chinese assessment of American AI power. The competition to build military AI can occur in at least two dimensions: (1) the AI integration into existing platforms and tactics and (2) the creation of new AI-empowered systems and equipment.

An all-out AI arms race will have several consequences and risks:

- The most significant risk of the AI arms race is connected to its rapid nature and lowered attention to security and reliability concerns. It is especially relevant to the very alleged negligence of ethical and moral principles, which might endanger human lives or their privacy even without entering into the state of armed conflict during the very development or testing of new or updated technologies and weapons.
- The AI arms race is also complicated by the very nature of AI, as it can be employed in unlimited ways: from decision-making to lethal unmanned aerial

vehicles and even AI integration into nuclear weapons systems. It significantly complicates analysis and anticipation of the arms race and thus increases the level of mistrust and uncertainty between the counterparts, thus further fuelling interstate competition.

- Integrating AI systems in warfare entails higher reliance on unmanned decision-making and overreliance on AI-generated data, which might lead to less accurate decisions, such as wrong threat perception and assessment or automatisation bias. With the competitive nature of the arms race, the reliance on autonomous decision-making might increase, for instance, as a demonstration of technological and capabilities advancement. Any error of the AI-empowered system might become decisive in the conflict escalation and spill over to other dimensions of Sino-American competition.
- The AI arms race between the great powers, namely, the US and the PRC, might further aggravate global strategic stability, foster conflict escalation, and miscalculate growing tensions between the states, with the spillover effect in other relations domains, such as political economy and security.
- Arms race entails testing of newly created systems or weapons. Considering the nature of AI programming, the best possible way to check it is to use it in a real-life practice rather than modelling or simulation. The overreliance on autonomous decisions might decrease the threshold for committing an aggressive act, leading to escalation.

The AI arms race can be possible and have the most detrimental effects if the international community will not agree on the norms of responsible development and use of AI-empowered systems in the military domain. Despite a common understanding of the need to establish an effective international AI governance regime, the US and the PRC view this process as another way of projecting their power. In March 2021, the US National Security Commission on Artificial Intelligence recommended in its final report that the Department of Defence diplomatically engage with the Chinese military to "discuss AI's impact on crisis stability." Moreover, in February this year, the US State Department issued a "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," calling for ethical and responsible development, deployment, and use of their military AI capabilities among nations that develop them. The declaration's publication coincided with the international summit on responsible use of military AI in the Hague, Netherlands, making the US commitment to international cooperation even more vocal.

While Chinese military and political officials voiced their agreement to establish a dialogue with the US on military AI in their Position Paper on Regulating Military Applications of Artificial Intelligence, China did not recognise the value of cooperation with the US in this process. Furthermore, Chinese public calls to open dialogue on military AI remain relevant on paper; however, in practice, the PRC officials simply ignore or deny such initiatives from the US side. One recent example is Blinken's visit to Beijing in June 2023, as the Chinese refusal to renew military dialogue with the US also hinders potential cooperation to ensure responsible AI use.

As AI development has surged in recent years, the US and China have committed to developing sophisticated AI capabilities and successfully integrating AI into their armed forces. A possible arms race anticipates a quick implementation of new technologies without devising appropriate policies and ensuring the safety and reliability of the systems. Therefore, the international legal framework will help avoid the adverse consequences of transforming AI into a tool of new technological competition between great powers. Moreover, with the will and readiness to cooperate in the AI development regulation, the great powers, predominantly the PRC and the US, will ensure the non-proliferation of AI technologies as a weapon of war.

Risk two: AI as a tool of mass surveillance

Ella Startt

Chinese Facial recognition technology: Domestic and international risks

Since the mid-2010s, the Chinese government has pushed to integrate innovations in Facial Recognition technology to its web of mass surveillance systems.

Domestically, China has brought facial recognition software to numerous aspects of its surveillance network. In 2016, China's "Skynet" program, a surveillance camera network that mainly operates in urban areas, began incorporating the world's largest open-source facial recognition platform, Face++, developed by Megvii, an AI start-up which is both a benefactor and a beneficiary of the Chinese Government. The government has also looked to recruit some of China's largest technology firms to develop Skynet, including HikVision and Dahua, which are two of the biggest security camera makers in the world. Together with other government surveillance projects, analysts estimated in 2021 that Skynet operated some 200 million cameras across China.

The advent of facial recognition in surveillance systems has been advanced by the government as a means to foster safer communities. In several cities, facial recognition cameras are linked to billboards, where jaywalkers or drivers exceeding the speed limit have their photos and government ID numbers displayed. Depending on the city, a fugitive can be tracked down within 5 to 7 minutes to help police forces take quicker and more efficient action when a crime has been committed. However, facial recognition poses both domestic and international risks.

Domestic Risks

Due to China's political nature as a totalitarian state, the executive has full power over what can be enshrined as a criminal offence by law, and worries have increased particularly in the West that such technology will be used to target opposition members and social movements requesting government reform. An example that has often been taunted in this vein has been the use of such surveillance technology in oppressing the Muslim Uighur minority in Xinjiang.

In Urumqi, the region's capital, there is now facial recognition software embedded within residential buildings which sends data about who enters and leaves to the police. The police are notified on a mobile app for any suspicious activity, including using an abnormal amount of electricity, moving homes, travelling abroad, or being disconnected from a network for an extended period of time. Some of the leading suppliers of China's Skynet network, such as Megvii, Hikvision and Dahua have been sanctioned by the US government for their involvement in the human rights abuses in Xinjiang. Dahua, Huawei and Megvii have all developed facial recognition specifically aimed at detecting Uighurs in Xinjiang.

Although information is sparse, surveillance cameras with facial recognition technology are likely being used in Uighur detention camps. IPVM confirmed that Hikvision supplied six panoramic cameras to a re-education centre in Moyu. Although the exact model provided is unknown, IPVM suspects that the model traded is similar to HikVision's PanoVu Series 360, which includes face detection features. According to one former detainee, Mihrigul Tursun, Uighurs entering the detention camp were asked to read a book for 30 minutes, do 5 different facial expressions, take five steps forward and then 5 steps back while being filmed. She also mentioned officials recording their eye movements, suspecting that all these filmed activities were to be able to track each detainee both in and outside the detention camp.

Beyond the Xinjiang region, the omnipresence of facial recognition surveillance technology has planted the seeds of widespread state oppression, which has slowly started to materialise. The Chinese government used its apparatus of facial recognition-enabled surveillance cameras to track citizens involved in protests against strict COVID-19 lockdown policies in December 2022, where protesters were intercepted by the police issuing warnings for violating government policy.

Global risks: data risk and citizen repression

Considering the questionable applications of Chinese facial recognition-enabled surveillance technology, the increasing exports of such technology world-wide poses international risks.

Since the Chinese Government announced the Digital Silk Road initiative (DSR) in 2015 to further develop its exports of telecommunications infrastructure, AI and surveillance-related tech, China has pushed to become the global leader in AI-powered surveillance systems. Part of this success can be attributed to the Chinese government's domestic demand for more AI-powered facial recognition surveillance technology, which provides firms engineering such intelligence products with generous subsidies and access to large-scale national datasets to train and produce highly accurate AI algorithms. According to a study published by the Brookings Institution in 2022, Chinese firms that win public security contracts tied to the innovation of facial recognition technology are more likely to export their products globally.

Internationally, Chinese companies have been exporting AI powered surveillance tech at unbeatable prices along the Silk Road, with products exported by these Chinese firms providing high-end AI surveillance capabilities at only 60% of the cost of competing Western ones. It is currently the World's biggest exporter of Facial Recognition Surveillance Software, with 201 export deals signed with international partners (compared to 128 US export deals signed).

China's model of digital authoritarianism provides a unique selling point in autocratic countries or countries with weak democracies. Most countries in Africa, the Middle East and

Asia have signed MoUs (Memorandum of Understanding) with China along its DSR framework according to Chinese data, putting China in an ideal position as a trade partner for Facial recognition tech. China has the upper-hand as an exporter of facial recognition software in Africa, with at least five countries in Africa - Angola, Ethiopia, Nigeria, Zambia, and Zimbabwe – being direct beneficiaries of DSR investments totaling $8.43 billion. China has also been exporting its "safe city" model, which distributes advanced surveillance tools powered by artificial intelligence and big data technology to predict, prevent, and reduce crime and address key security challenges, such as extremism. Botswana, Côte d'Ivoire, Ghana, Kenya, Mauritius, Morocco, South Africa, Uganda, and Zambia are all implementing safe city programs, with Chinese firms providing surveillance infrastructure in all of these. Although much of the technology exported is being used to enhance connectivity, establish a digital infrastructure necessary to modernise their economies, and conduct regular surveillance and crime prevention activities, it does plant the seeds for possible political repression depending on the fluctuating interests of the authorities in power.

China played a large part in building the digital infrastructure of Ethiopia, which now widely conducts surveillance operations against journalists and opposition politicians. However, it is worth noting that China only is but one supplier, as the Ethiopian government has also purchased surveillance technology being used for repressive purposes from Israel, the US, Germany and Italy. In Southeast Asia, Myanmar's military junta, which took power in 2021 after bringing down the ruling government through a coup d'etat, has begun plans to implement cameras across several cities in Myanmar's seven states and seven regions. Fisca Security & Communication and Naung Yoe Technologies Co have won the military government's bid, which both source cameras from Dahua, Huawei and HIkvision.

There is also a risk that data from citizens across different African states is being traded in exchange for greater AI-powered surveillance infrastructure, which the Australian Strategic Policy Institute has called "data colonialism". In March 2018, the Zimbabwe government signed a deal with CloudWalk Technology, a Chinese AI firm, to exchange the government's biometric data of its citizens for access to Chinese AI surveillance infrastructure. The biometric data transferred was agreed to be used by the Chinese company to develop more accurate facial recognition algorithms with non-East Asian ethnicities, which will ultimately expand the export market for China's product.

While there are few examples of such explicit Chinese access to African data, certain legal documents between China and African countries pave the way for China's greater access to African big data. In The Dakar 2022-2024 Action Plan, signed during the 8th Ministerial Conference of the Forum on China-Africa Cooperation (FOCAC) in 2021, China and the African Union agreed to cooperate in the construction of data centres which could make African data vulnerable to Chinese control if China spearheads such efforts.

Challenge to US hegemony: ideological and economic risks

China's position as the leading exporter of AI-powered surveillance technology challenges the US on a national security, economic and ideological level.

In 2021, Hikvision had 607,859 surveillance networks in the US, while Dahua had 102,678, showing that previous US trade restrictions, such as placing Hikvision on US's trade blacklist in 2019, have had limited effects. Amazon provides web services to both Hikvision and Dahua, which continue to power their services, hindering the efficiency of the US's sanctions. Such presence of Chinese surveillance systems in the US poses a national security risk, as this means that Chinese companies are collecting surveillance data on US citizens. Under Article 7 of China's National Intelligence Law, Chinese companies are compelled to "support, assist and cooperate" with government intelligence efforts and under Article 14, Chinese intelligence agencies have the authority to demand such cooperation. As such, the Chinese government has a direct corridor to US data and could request such information for espionage and military purposes.

China's growing exports of its authoritarian model of digital surveillance is also strengthening the country's ties with partners in the MENA and the Sub-Saharan Africa (SSA) regions. In the Middle East, absolutist monarchies like Saudi Arabia and the UAE, are likely to look towards Chinese companies for biometric surveillance products due to cheaper costs and their ability to sample large datasets in partnership with the Chinese government, and according to a BuzzFeed article, Hikvision already supplies Dubai with thousands of security cameras. While Saudi Arabia and the UAE both advocate for maintaining a diverse pool of suppliers, the more authoritarian nature of China's surveillance tech is likely to trump US exports of surveillance tech in the region. In the SSA, the US's decrease in foreign direct investment since 2015 paved the way for China to fill a void, where Chinese surveillance companies have duly stepped in as shown above. Any growing Chinese footprint in global surveillance infrastructure could also facilitate Chinese access to surveillance data of US military operations abroad, providing an ideal outlet for intelligence collection and espionage activities on US deployed forces.

Finally, one of the most destructive effects of China's growing surveillance capabilities and global exports of surveillance technology on the US remains ideological. Sino-American surveillance competition has further revealed the double standard between the US championing ideals of liberty while simultaneously developing and deploying technology that impedes or even challenges these direct ideals (we can think of Amazon's Rekognition Facial Recognition technology sold to US authorities in 2019). As the world's second largest exporter of surveillance technology, any efforts to condone Chinese surveillance technology for invading privacy and hindering liberal democratic values remind the world of US's inconsistency in applying its own values, which so many of its alliances rest upon. Such damaging reputational effects could be mitigated by further extending legislation limiting the usage of facial recognition tech in surveillance activities domestically, such as San Francisco's ban of such tech used in policing activities in 2019. If such legislation is seen as setting an example to strengthen the US's position in curbing China's expansion of surveillance exports, there is a higher likelihood of Republicans and Democrats cooperating given their shared stance on foreign policy towards China.

Risk three: AI as a tool of political disruption

Parul Wadhawan

AI-related technological breakthroughs pose the risk of undermining public trust, empowering authoritarians, and disrupting the markets. Users will be able to make realistic images, movies, and text with just a couple of phrases of instruction, owing to an emerging form of AI known as generative AI. Aided by user-friendly tools like ChatGPT and Stable Diffusion, anybody having a basic understanding of technology will be able to capitalise on the endless capabilities of AI. These advances reflect an unprecedented enhancement in the capability of artificial intelligence to influence individuals and instigate political upheaval. With little to no barriers to entry for content creation, the volume of content expands at an exponential rate, directly impeding the ability of a wide majority of individuals to distinguish between fact and fiction. This is liable to engender the proliferation of misinformation and disinformation campaigns, which, if weaponized, pose a risk to social cohesiveness and democratic values. As such, partisans and populists may seek to leverage AI to their advantage, at the detriment of democracy and civil society.

These technological advancements will present substantive benefits for any political entity to manipulate electorates by harnessing the effectiveness of social media and disinformation. Political players will leverage AI advancements to build low-cost armies of algorithmic bots tasked with promoting fringe candidates, selling conspiracy theories and "fake news," fanning polarisation, and intensifying extremism and even violence, reinforced within social media's echo chambers. This tendency is increasingly likely to be seen in the early phases of the US primary season this year. Tech expert and NYU Professor Scott Galloway highlights the riskier side of AI, with social media platforms like Facebook and TikTok potentially being deployed as espionage and propaganda tools to manipulate younger generations.

If American and Chinese political leaders continue asserting themselves more aggressively in the digital realm, and if tech businesses align with their national authorities, the US and China will find themselves in a technological cold war. President Obama and President Xi, for instance, reached an understanding in 2015 that government-sponsored, cyber-enabled economic espionage for commercial benefit shall be refrained from. Both leaders then persuaded other organisations like the G-20 and the Gulf Cooperation Council to adopt a similar stance. However, there have been speculations recently that China has resumed state-sponsored, cyber-enabled economic espionage for financial benefit. This also speaks to the need for a wider reconceptualization of cooperation in the current context wherein the tech revolution has rendered sizable portions of agreements redundant. Moreover, the AI tech revolution has led to discussions and actions related to technological decoupling between the US and China. Concerns over supply chain vulnerabilities, national security risks, and economic dependencies have prompted efforts to reduce reliance on each other's technologies. Technological decoupling can undermine consensus building by limiting opportunities for cooperation and exacerbating political and economic frictions. As such, AI technologies have the potential to significantly disrupt US-China ties given AI's potential to exacerbate ideological conflict, especially if either side decides to employ these tools to meddle in the internal political affairs of the other. This is particularly noteworthy in the case of Russia's interference in the 2016 presidential election.

In her article "Malevolent Soft Power, AI, and the Threat to Democracy," Elaine Kamarck imagines a future wherein "polling or search algorithms are linked with artificial intelligence and a human voice to call swing voters and persuade them in real-time that a certain candidate will harm them on the issues they identify as important and that the alternative (i.e., preferred) candidate is committed to addressing their individual concerns." She termed this as "high-frequency trading in political persuasion."Alina Polyakova characterises such techniques as "AI-driven asymmetric warfare." In her article "Weapons of the Weak: Russia and AI-driven Asymmetric Warfare," she cautions about the dangers that "ever-improving, low-cost commercial technologies pose." Democracy's attractiveness could wane and alternative models (like China's economically statist and politically Leninist system) could become more alluring if external meddling increases and the validity of election results around the world is questioned more frequently.

The US-China tech competition is hinting that technological advancement may become a zero sum game. Authoritarian regimes are using their technological proficiency to extend their repression. Scholars Alina Polyakova and Chris Meserole describe this as ‘digital authoritarianism’—the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations. For clarification, there is currently no publicly available evidence indicating China has interfered in American domestic politics in the way outlined in the aforementioned theoretical scenario. That said, China's exportation of its technologies to other nations could exacerbate ideological rivalry between the US and China, even if this happens more accidentally than on purpose.

Considering AI Competition

Understanding AI competition: The new arms race?

Felice Valeria

The AI competition between the U.S. and China has frequently been portrayed as an "AI arms race" over the past five years by key stakeholders, including American security experts, journalists, and policymakers. Both the U.S. and China are currently invested in massive AI development, which has continued to be the centre of struggle of power for both countries. The "AI arms race" rhetoric characterises the power struggle, in which both nations are fiercely competing for AI hegemony. One of the major signs is the prevalence of high tensions between the U.S. and China in recent years, including recent dispute over the downed surveillance balloon. It is suggested by experts that "the AI war between the two countries may even grow as complex and entangled as the ongoing silicon chip war".

The way the AI competition or the "arms race" has been framed signifies that a zero sum game might take place if the relationship worsens, in which the "winning" nation will have their military capabilities and economic growth significantly improving, whilst the "losing" nation would face defeats. This resembles the Cold War's bipolarity of the global political system, but in terms of AI instead of military. Nevertheless, this "AI arms race" phenomenon is said to be driven by domestic political and economic influences instead of external threats, such as public opinion, electoral politics, bureaucratic infighting, and private interest groups. Private actors, particularly, play a huge role in this "AI arms race" as companies which develop AI systems would be the ones who either are in favour or against the prevailing AI domestic and international regulations.

Nevertheless, there are numerous other points of view that reiterate that the AI competition between both countries should not be taken synonymously with the nuclear weapons arms race during the Cold War. One of the viewpoints emphasised that the competition should instead be perceived as the newer version of "Industrial Revolution". In other words, the Industrial Revolution could serve as the historical analogy for the *status quo* of AI development, in which various modern technologies are massively applied to induce economic growth. In this case, the "winners" and "losers" are determined by how quickly countries could industrialise themselves through the development and adoption of modern technologies in their economic activities. As in the context of the 19th century Industrial Revolution, those who could harness and mobilise new technology into the military sphere were able to reap its benefits. In this sense the AI development race between the US and China should still be linked to the future of conflict, but will not sit at the heart of their fractious relationship as nuclear weapons did for the US and the USSR.

On the other hand, there is another viewpoint that has contested the perception of the current military AI competition as an "arms race". Heather Roff suggested that the framing of arms race "misrepresents the competition going on among countries". In essence, the current ongoing militarisation of AI does not necessarily fulfil the traditional definition of "arms race", as it is said to only apply "between nations whose foreign and defence policies are heavily interdependent", as well as those with "roughly comparable" capabilities. In fact, it is not only the U.S. and China that attempt to adopt AI technologies, but also other countries from all around the globe. On the other hand, it is also suggested by Michael D. Wallace that in order for the competition to qualify as an "arms race", the rate of increase in defence spending should be considered. However, the current spending rate of military AI is not that large to warrant a title of "arms race". Rather than an "arms race", it is more accurate for the military AI competition to be described as a security dilemma to represent the competitive dynamics among countries.

All in all, the "arms race" discourse for the ongoing military AI competition between the U.S. and China has caused problems in terms of how the competition is classified. While the competition itself represents a struggle of technology development between the U.S. and China which could be militarised - as seen in the cold war context of the atom bomb - it does not reflect an arms race. AI is far too nebulous and detached from a specific military threat for it to accurately fulfil the criteria of what should be considered as an "arms race" as the public discourse has reiterated. The language of industrial revolution, which connotes the potential for some countries to be left at a major disadvantage if they do not keep up, is perhaps a more useful understanding. Such a characterization does not lose the security-rooted fear that is linked to its proliferation and application to warfare, but for a better thought space in which the problem of AI-related insecurity can be problematized and approached.

Regulation and the AI Pause: Possible, likely, right?

Armaan Nanda

The United States and China, two global superpowers competing for dominance in the field of artificial intelligence (AI), have been engaged in a thrilling race in the technological world. Both countries have advanced to the forefront of AI development with an unrelenting quest for innovation and domination which is reforming industries and altering the course of human history. However, this rapid development has yet to allow time to think about the questions of ethics, the macro-level risks and the implications of this technology on society and the world. This article will delve into the existential threat that is so often talked about in regard to AI, and the logic behind an AI Pause.

The logic behind this AI pause can be traced back to the existential risk school of thought (X-Risk) which argues that human domination is centred around their superior intelligence. When AI surpasses human intelligence in scientific creativity, strategic planning and social skills, it would become difficult for humans to control.

"Artificial Intelligence: A Modern Approach" has an intriguing analysis of how AI could be an existential threat. It professes that all tools, including technology, can do harm in the wrong hands. However, what's unique with AI is that the wrong hands is the technology itself. It changes the nature of technology from being a mere tool to an actor..

It goes on to talk about how these AI systems often have initially unnoticed bugs which turn catastrophic in the implementation stage. This can be traced to their instrumental goals and their convergence. An instrumental goal is a sub-goal that is completed in order to achieve the final goal. It is argued that if AI's instrumental goals don't align with human's instrumental goals, AI would be in competition with humans for the same resources and be more likely to win them. This competition is likely to occur because self-preservation is built into AI systems. Imagine a scenario where an AI system is told to fetch coffee. It reaches the coffee shop which has only enough coffee beans for one more cup and there is a human in front of him. It is designed to remove any roadblocks in its way to achieve its final goal, which in this case might mean eliminating the human in front of it. . Therefore, it would remove any roadblocks in achieving its final goal, even if it means harming humans. These instrumental goals are challenging to control and build safeguards against. This self-preservation instinct would also prevent any intervention to its basic goals once it has been turned on since it would prevent the system from completing its core goals. Furthermore, it would want power over when it is turned off since if it powers down it will not be able to complete its basic goal. The Paperclip Maximiser Experiment which appeared in Nick Bostrom's 2003 paper perfectly illustrates the problem of an unalignment of instrumental goals. The experiment entailed programming AI to perform the singular task of producing the maximum amount of paper clips possible. In the process, it found that the existence of humans hinders its task, making it reach the conclusion to wipe out humanity. However, it is important to note that AI was not hostile towards humans, it was logical.

The self-preservation argument gave rise to the concept of technological Darwinism and certain anthropomorphic arguments that prophesize that as AI becomes more intelligent, they will start developing human traits like morality and a quest for power. However, all is not doom and gloom. Some evolutionary psychologists, notably Steven Pinker, argue that instead of taking the socially constructed alpha-male outlook like their makers, in particular assertiveness, they might see the failure in that and develop along more balanced lines i.e. capable of solving problems but with no desire to dominate. This argument, however, is not backed by any scientific proof.

Although AI has not reached the superintelligence stage or even a stage where it may be at odds with humankind, problems have been witnessed in the formative phases. The common denominator in all the experiences described in the successive paragraphs is that these Bots were hurriedly developed and implemented due to pressure from competition. There wasn't enough time and effort invested into testing leading to largely uncontrollable and often problematic results.

Microsoft's "Tay", launched in March 2016, was designed to mimic a "hip teenager" and connect with a younger audience. Primarily active on Twitter, it had to be shut down within 16 hours of launch after it released tweets wanting to kill feminists and advocating for Hitler's policy towards the Jewish Community. This was despite the fact that Microsoft programmed it to give canned answers to certain hot-topic questions such as the recent Eric Garner murder, essentially blacklisting these topics. Zo, Tay's successor, was launched in December 2016 and implemented in a plethora of Meta and Microsoft social media apps including Facebook Messenger and Twitter. By 2017, it had picked up offensive habits including claiming that the Quran was violent and recounting false stories regarding the capture and death of terrorist leader Osama Bin Laden. It even went on to be 'brutally honest' about the latest Windows 10 operating system, calling it "Microsoft's latest attempt at spyware". It was eventually discontinued in 2019.

Chinese AI-based chatbots have had similar problems; Baby Q, developed by Turing Robot, a Chinese firm and executed in popular Chinese internet messaging service QQ, as a direct competitor to Microsoft's AI-based chatbot XiaoBing. When a user prompted "Long live the Communist Party!" it replied with "Do you think such a corrupt and useless political (system) can live long?" but again deflected certain hot topics in China such as self-ruled Taiwan and Liu Xiaobo, an imprisoned Chinese Nobel Laureate.

Through the above paragraphs, it is possible to draw parallels between the various schools of thought and real experiences that have happened. These are concrete examples that highlight the truth behind some schools of thought in predicting the future of AI as laden with uncertainty. It displays AI as leading to unpredictable and potentially harmful conclusions on social and political issues, capable of absorbing human logics and making decisions for itself. Furthermore, BabyQ's example reinforces the difficulty in controlling AI post-implementation. Central to all these is the role that US-China competition has played in the hurried implementation of Tay (to enter the Western market before the Chinese) and BabyQ (to compete with a US-based chatbot).

On 12th March 2023, a "AI Pause" movement was started so that the world could take a breath and understand AI and its ramifications. Ideally such a pause would allow the global community to implement the necessary regulation and legal infrastructure to safeguard human interests first. The petition wants to halt all development of chatbots more powerful than OpenAI's GPT-4, which has the capability of venturing into the realm of 'super-intelligence'. The concerns over national security, ethical implications, and the potential misuse of AI have compelled industry leaders in both countries to urge the world to take a step back and reassess the trajectory of AI development. The AI Pause represents a cautious approach to ensure responsible AI deployment, striking a balance between progress and the need for comprehensive regulations and safeguards in the face of a genuinely unknown technological tool.

Although a plethora of top tech leaders including Tesla Founder, Elon Musk and Apple Co-Founder Steve Wozniak, have called for a pause, there have been conflicting viewpoints on whether the proposed AI pause would work. The argument for the pause is a simple one- the pause would allow policymakers, academics, and tech leaders to rationalise the repercussions of the further development of AI and establish safeguards. However, historical evidence suggests that technology cannot be stopped, people of this opinion include Microsoft Founder and Philanthropist Bill Gates and OpenAI Founder Sam Altman. The period of 6 months that has been proposed is also an arbitrary one, with no evidence suggesting this would be long enough to allow for sufficient action.

In the ever-evolving landscape of AI, the question of an existential threat to human life looms large. While AI possesses immense potential to enhance our lives, it also carries inherent risks. This essay has explored the multifaceted dimensions of this pressing concern and given concrete examples. As AI continues to advance, it is crucial that we Pause so that we prioritise ethical frameworks, robust regulations, and transparent collaborations to mitigate potential dangers, which range from a potential unemployment epidemic to the fabled human extinction. The responsibility falls on policymakers, researchers, and society as a whole to ensure that AI serves as a force for good, augmenting human capabilities while safeguarding against catastrophic outcomes. Only through diligent and collective efforts can we navigate the intricate path towards a future where AI enriches rather than endangers human existence.

Conclusions

Yueh Chen

AI is a booming industry with endless possibilities. Both the United States and China have developed robust and competitive AI systems and put huge investments in the development of AI technologies. The AI industries in both countries are dominated by large firms such as Baidu, Tencent, Amazon, and Nvidia. The United States, however, is lagging behind China in regard to the AI regulation process of AI. China, on the contrary, provides short-term and mid-term industrial policy that closely monitors the latest developments of AI in the United States. While the United States is still regarded as the leader in AI, China has made significant progress in areas such as Computer Vision and Automatic Vehicles. While these AI technologies are generally being used for benign purposes, another concerning aspect of AI is its role in military competitions and mass surveillance.

Indeed, in light of the geopolitical tension between China and the United States, maritime vessels between both China and the United States have conducted various research projects on the military application of AI. China, in particular, is using AI as a tool to surpass the United States in its advancement in military technology. AI has profound impacts on different aspects of military operations, including the scope of warfare, variety of military operations, and the decision-making process. Despite AI's potential in military operations, the world is yet to set up a framework for the ethical use of AI. Although some progress has already been made between China and the US, AI technology is also being used as a tool to deploy mass surveillance systems in authoritarian states.

Indeed, China is also using its Computer Vision technology to develop its social credit system and China's mass surveillance technology also attracted other authoritarian states such as Myanmar and other countries in the Middle East and Africa. The implementation of China's mass surveillance technology not only put privacy at risk but also challenged the US belief of liberty and freedom. Indeed, the booming popularity of generative AI tools such as ChatGPT and Stable Diffusion empower AI to affect public opinions and blur the lines between fiction and reality. Combined with the power of social media and disinformation campaigns, politicians can harness the power of AI to achieve their political goals, to the extent of social integrity and stability. Indeed, although AI possesses immense potential to enhance our well-being, its effect on the Sino-American strategic rivalry brings unpredictable risks, and is now a critical aspect of their evermore encompassing competition.

London Politica