A Balance of Power: Exploring the Opportunities and Challenges of AI for a Nation

Shasha Yu and Fiona Carroll

Abstract Artificial intelligence is having a profound impact on the development of human society. It is improving—in some case, re-inventing—our economic, political, cultural, educational and medical sectors, to name a few. For many it is a cost effective solution that makes processes more effective, more intelligent and often more independent. However, in doing this, it is also having a deterministic influence on the dynamics of our societies. From an economic perspective, AI technology could be a game-changer, giving emerging markets the opportunity to outpace more developed markets. In fact, it has the ability to change the balance of global power, so much so that many countries are now striving for a national strategy on AI. And this goes to the very heart of a nation's security where AI can also create significant implications for the protection and defence of it's citizens, and economy. This chapter presents how Artificial Intelligence technology is extremely important in how it can shape the strength and power of a nation. Moreover, it highlights how AI can both positively and negatively impact a nation's security. In summary, the chapter will provide a detailed overview of AI, it will analyse the direct and indirect effects of AI on national security and will present some potential solutions.

Keywords Artificial intelligence · National security · AI · Machine learning · Big data

S. Yu (✉)
School of Professional Studies, Clark University, Worcester, MA, USA
e-mail: ShaYu@clarku.edu

F. Carroll
Cardiff School of Technologies, Cardiff Met University, Cardiff, Wales
e-mail: fcarroll@cardiffmet.ac.uk

R. Montasari (ed.), *Applications for Artificial Intelligence and Digital Forensics in National Security*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-40118-3_2

1 Introduction

Research into artificial intelligence (AI) dates back to World War II. Alan Turing, a British mathematician, was most probably the first to decide that artificial intelligence was best studied through computer programming rather than by building machines [47]. In fact, Alan Turing's 1950 paper in *Computing Machinery and Intelligence* argued that if a machine can successfully pretend to be human in front of a knowledgeable observer, then it should be considered intelligence [69]. The term 'Artificial Intelligence' was first used in 1955 by John McCarthy et al. in the *Dartmouth Summer Research Project on Artificial Intelligence*, establishing Artificial Intelligence as a research discipline [48]. According to John McCarthy, AI includes, but is not limited to, the following branches: Logical AI, Search, Pattern recognition, Representation, Inference, Common sense knowledge and reasoning, Learning from experience, Planning, Epistemology, Ontology, Heuristics, and Genetic programming [47].

Today, artificial intelligence has been widely used in all walks of life and has had a profound impact on the development of human society. It has brought about fundamental changes in the development of countries in the economic, political, cultural, educational and medical spheres. According to PwC research, artificial intelligence could transform the productivity and GDP potential of the global economy [35]. By 2030, AI could contribute up to US$15.7 trillion to the global economy, more than the current output of China and India combined [35]. From a macroeconomic perspective, AI technology could be a game-changer, giving emerging markets the opportunity to outpace more developed markets.

The authors of this chapter highlight that Artificial Intelligence technology is extremely important in how it can shape the strength and power of a nation. In doing so, it can positively and negatively impact its national security. The following sections will give an overview on AI, they will analyse the direct and indirect effects of AI on national security whilst also, they will present some possible solutions.

2 Artificial Intelligence Overview

According to John McCarthy, artificial intelligence "is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable" [47, p. 2]. *UNESCO's World Commission on the Ethics of Scientific Knowledge and Technology (COMEST)* describes artificial intelligence as "involving machines capable of imitating certain functionalities of human intelligence, including such features as perception, learning, reasoning, problem solving, language interaction, and even producing creative work" [16, p. 6]. Furthermore, Stuart Russell and Peter Norvig

summarise previous definitions of AI and distil four possible goals to pursue in artificial intelligence: Acting humanly, Thinking humanly, Thinking rationally, and Acting rationally [62].

In 1997, IBM's supercomputer *Deep Blue* caused an uproar when it defeated one of the greatest chess masters of the time, Garry Kasparov. It became the first computer system to beat the world chess champion within the standard tournament time limit. Moreover, in 2015, a robot named *Eugene Goostman* won the Turing Challenge for the first time. In this challenge, human raters chatted with unknown entities using text input and then guessed whether they were talking to a human or a machine. *Eugene Goostman* tricked more than half of the human evaluators into thinking they had been talking to a human. Nowadays, the main application areas of AI include Natural Language Processing (NLP), Speech Recognition, Image Recognition and Processing, Autonomous Agents, Affect Detection, Data Mining for Prediction, and Artificial Creativity [70].

3 Artificial Intelligence in National Security

3.1 The Impact of Artificial Intelligence on Economy

Thanks to the Internet and computer technology, we are living in an era of rapid growth in the amount of data available. Analysis shows that Internet users have more than doubled in the last decade, climbing from 2.18 billion at the beginning of 2012 to 4.95 billion by early 2022 [42]. In addition, the 'typical' global Internet user now spends nearly seven hours a day using the Internet (consuming information and generating new information) on all devices [42]. IBM calculates that more than 2.5 quintillion bytes of data is generated every day [70]. The Internet has long surpassed radio, TV and newspapers as the largest source of information for people, and is also the main place for major companies to compete for potential users and customers.

Back in the 1970s, Nobel Prize winning economist Herbert Simon introduced the concept of the 'attention economy'. He said, "In an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention" [64, p. 37]. Goldhaber helped popularize the term 'attention economy', arguing that "the currency of the new economy is not money, but attention" [30, p. 1].

In today's era of big data, huge amounts of data is being produced every second and the rate of data production is still growing exponentially. Moreover, individuals have a limited attention span, which means that when they pay attention to something, they do not pay attention to other things. In contrast to the decreasing cost of information brought about by technological progress, attention is even more scarce under the impact of information overload. The scarcity of attention makes it highly valuable and

can lead to additional resources, such as money, fame, and power. Indeed, influencers can get a lot of money through live marketing, even the average everyday person can gain a large fan following by posting novel videos. Even politicians can gain public attention and support by going around giving speeches. And behind all of this, there is an increasing number of artificial intelligence algorithms.

In the fierce war for users' attention, major companies conduct *Psychographic analysis* of users. *Psychographic analysis* aims to analyse the subjective characteristics of users in order to understand or predict their behaviour. It analyses areas such as personality traits, activities, interests, opinions, needs, goals, values and attitudes [79]. It is usually information obtained by analysing a range of behavioural data. For example, researchers can uncover users' opinions, emotions, and attitudes based on the social relations between users on social networks and the interactions of user sentiment orientation [10]. AI-based *psychographic analysis* can accurately predict a user's preferences and likely future behavior based on previous behavior or the behavior of other users belonging to the same group. Furthermore it can apply targeted solicitations such as pushing ads, news, or even recommending people that they are likely to connect with.

Most AI relies on learning knowledge from past data, and the larger the data sample, the better it performs, so data is considered the oil of the new age. Technology giants and business giants have the advantage of strong capital and technology to access more data resources and create more advanced AI products. This can significantly reduce costs and improve service quality, which in turn helps them to have greater access to more data resources. In contrast, the majority of small to medium-sized enterprises are at a disadvantage in terms of access to data resources. There are only an exceptional few small to medium-sized enterprises that are able to excel in their niche areas, resulting in a polarised situation. Indeed, it is only a few companies that dominate data resources thus become monopolies and undermine the healthy ecology of the national economy.

As the gatekeeper of the Internet monopoly, Google, for example, has billions of users and countless advertisers around the world. With its vast amount of data and powerful AI algorithms, it has become one of the world's richest companies with a market capitalization of $1 trillion [19]. Its influence even transcends national borders to become a global monopoly [19]. However, in 2017, Google was convicted and fined €2.42 billion by the EU for its monopolistic practices in advertising, the largest such antitrust fine issued by the European Commission [56]. Google accounts for almost 90% of all search queries in the U.S. and uses anti-competitive tactics to maintain and expand its monopoly on search and search advertising. In 2020, the U.S. Department of Justice sued monopolist Google for violating antitrust laws [32]. Indeed, Google has used its dominant position to engage in a series of anti-competitive practices that harm competition and consumers. It also has reduced the ability of innovative new companies to grow, compete, and discipline Google's behavior.

In fact, the impact of AI algorithms (driven by big companies) on the economy is much broader than that. When large companies gain a monopoly on access to user data, they can in fact control their users' lives in many ways. For example, short-form video platforms can decide what information to push to users; social media

platforms recommend from time to time what influencers they might be interested in promoting; and commercial websites push users merchandise, movies, and books that might appeal to them. This influence is so subtle that when a user who is influenced by it makes a decision, he/she may not even realize that he/she is influenced by it. For example, they may have chosen a product from brand A over brand B when shopping because they saw more push messages about brand A on the website, and that was the result of an AI algorithm. That is, when AI algorithms can influence a person's attention, they can influence how people spend their money. In this sense, business giants with AI algorithms at their disposal can more-or-less control the flow of money.

In the manufacturing industry, the adoption of AI can replace a portion of the work that would otherwise be performed by humans. It can limit the number of hours worked, significantly reduce the cost of products and make them more competitive in the marketplace. As a result, countries and companies that invest in AI earlier will benefit more from this, gaining accelerated economic growth. Less developed countries and regions, on the other hand, are likely to be left far behind. According to PwC research, the rate of adoption of AI technologies significantly impacts economic development potential, showing an imbalance across regions [57]. By 2030, the largest economic gains from AI are expected to occur in China (26% GDP growth) and North America (14.5% growth), totalling US$10.7 trillion and accounting for nearly 70% of the global economic impact [57]. They are followed by Southern Europe, developed Asia, Northern Europe and Latin America with 11.5%, 10.4%, 9.9% and 5.4% respectively, while for the rest of the world, the total impact is 5.6% [57].

3.2 The Impact of Artificial Intelligence on Employment

According to UN DESA, the global population is expected to reach 9.8 billion by 2050, of which more than 6 billion will be of working age [71]. At that time, people of working age may face significant employment pressures. At the same time, with the rapid development of artificial intelligence and automation, intelligent devices are replacing human work in various fields. The increased utilization of technology has reduced the number of jobs, and more and more jobs are being replaced by automated machines and software. A study by PwC shows that by the mid-2030s, 30% of jobs and 44% of workers with low levels of education will be at risk of automation as AI advances and becomes more autonomous [35]. In a similar research, the *World Economic Forum* estimates that, as a result of artificial intelligence and automation, 85 million jobs will be replaced by 2025, while 97 million new jobs will be created in 26 countries [78]. However, the report also sets out a list of jobs that are growing and decreasing in demand, with the growth being concentrated in highly skilled jobs such as artificial intelligence, data-related jobs, information security and the Internet of Things, while the decrease in demand is mainly for manual labour or simple skilled jobs [78].

By that time, more new jobs are being demanded by technology updates, placing higher skill requirements on the workforce. Workers who used to work in labor-intensive industries will have to face structural unemployment, and they will be forced to update their knowledge in order to adapt to the new demands. For those less developed countries and regions with low levels of education, they will be at an even greater disadvantage. The uneven economic development brought about by the development of AI technology will also trigger an uneven distribution of talent by association. Higher investments in AI in developed economies will yield higher returns, thus attracting more highly educated and skilled young people from less developed regions. Due to the siphon effect of talent aggregation [46], the talent resource gap between developed economies and less developed regions will be exacerbated. Especially, when more professionals flow to developed economies that are more suitable for their individual development.

In addition, with the rapid development of AI technology in recent years, computers have not only replaced human workers in many repetitive labor fields, but have even achieved good performance in creative fields. These include areas such as music, literature and painting, and in highly technically demanding fields such as medicine and architecture. For example, previous studies have shown that AI is more accurate than many doctors in diagnosing breast cancer from mammograms [75]. As a result, even the well-educated senior personnel are under pressure to update their knowledge and skills. According to the *World Economic Forum*, by 2025, half of all workers will need to upskill or reskill to prepare for job changes and new jobs [78].

3.3 The Impact of Artificial Intelligence on Education and Culture

In recent years, especially since COVID-19, artificial intelligence has been used in many applications in the education industry. On the one hand, it can provide personalized tutoring and 24/7 accessibility to students. This can help students from different backgrounds to get equal (and equitable) access to education. On the other hand, it helps educators automate tasks such as administration, assessment, grading, and repetitive question-answering, so they can focus on more innovative work. The rapid development of artificial intelligence technology also gives students more hands-on opportunities to implement their ideas. Some functions that previously required complex code can now be easily implemented with codeless AI [65]. For example, Microsoft's *lobe.ai* allows anyone to train computer image classification models to recognize objects and is developing a codeless object detection and data classification platform for the general public [51]. Another codeless training platform, *Teachable Machine*, can be used to recognize user-defined images, sounds, and poses [66].

As a result of natural language processing (NLP) technology, artificial intelligence is also increasingly being used in a variety of writing tasks to help students improve their writing. For example, students can use platforms such as *Grammarly* for grammar checking, *Wordtune* for sentence touch-ups, *Quillbot* for proofreading, plagiarism checking and citation, and even software such as *Rytr* to generate text on a variety of topics. This software learns from a large library of texts and can mimic the generation of texts that are almost indistinguishable from natural human language, even with the option of different languages and styles. Moreover, in the field of computer programming education, artificial intelligence is playing an amazing role. AI-powered code generators, such as *OpenAI Codex*, *DeepMind AlphaCode* and *Amzon CodeWisperer*, can convert natural language representations of tasks into computer-runnable code [5]. Most of them are trained on the GitHub codebase and can generate code based on various major computer programming languages and can convert them to each other. These code generators can help beginners understand various approaches to problem solving and develop their thinking.

In the field of art creation, artificial intelligence also has had an amazing performance. In September 2022, an artwork generated with the AI drawing tool *Midjourney* won the top prize in the digital category at the Colorado State Fair Art Competition in the United States. These AI-generated applications gain popularity at a far lower cost and quicker response than human artists [59]. OpenAI's image generator *DALL-E 2*, released in spring 2022, has more than 1.5 million users and creates more than two million images per day. *Midjourney*, another popular AI image generator released the same year, has more than three million users on its official *Discord* server [61]. Applications such as *DALL-E 2* and *Midjourney* are built by crawling millions of images from the open web, then teaching algorithms to recognize patterns and relationships in those images and generate new images in the same style. This means that artists who upload their work to the Internet may unwittingly help train their algorithmic competitors. *DALL-E 2*, *Midjourney*, and *Stable Diffusion* - enable amateurs to create complex, abstract, or realistic artwork [60]. These AI-created artworks are generated by *Adversarial Generative Network* (GAN). GAN can be seen as such a system. By adding a discriminatory model to the generative model, GAN mimics the mechanism by which humans judge pictures in the real world. Thus, transforms the hard-to-define sample differences into a game problem. Similar to this is *AlphaZero*, which accumulates a large amount of data in the form of self-play and then explores a more optimal strategy from it. In this new research paradigm, the model changes from a tool for analysis to a 'factory' of data.

From a higher perspective, the success of GAN essentially reflects the fact that AI research has entered deeper waters. The focus of research has shifted from perceptual problems such as vision and hearing to solving cognitive problems such as decision making and generation. Compared with machine perception problems, these new problems are often not well solved by humans either, and the solution to such problems must rely on new research methods. Generative AI not only analyzes existing data, but creates new text, images, videos, code snippets and more. On the one hand,

these AI tools help people learn to master various skills better and expand the range of their abilities. On the other hand, they bring new challenges and even potential risks to education, such as ethical issues, bias and bad habits, and over-reliance [5].

Firstly, these AI tools are based on learning from publicly available databases of data derived from the intellectual output of others. As a result, those who use the work generated by these AI tools inevitably face issues of academic integrity. Secondly, they have the potential to make students overly dependent on them [11], or to develop such overconfidence that they neglect their own individual learning and training. And as a result, struggle to obtain the expected performance once they leave these tools. Thirdly, even seemingly correct computer generated code can hide undetectable errors [45] that can be risky and even costly if adopted without full understanding by the user [55]. Fourthly, as AI algorithms learn from data, algorithmic bias can occur when data sampling bias is in the source data and this can result in the under representation of a portion of the population. These biased models may generate codes that impact gender, race, class, and other stereotypes [11].

3.4 The Impact of Artificial Intelligence on the Security of Our Society

In recent years, artificial intelligence and big data technologies have been increasingly used for public security and in police departments. For example, many countries have introduced AI-powered police assistance systems that work well in various areas such as crime prediction, police dispatch, scene investigation, and case solving [84]. Even some cases that have not been solved for years have now been solved with the help of AI technology to unearth and discover new clues. For example, in May 2022, Dutch police have received dozens of leads after using *Deepfake* technology to bring a teenager virtually back to life nearly 20 years after he was murdered [2].

Not only the police, but in fact ordinary people can benefit from AI technology in the judicial process. For example, facial recognition technology is often used by police to identify suspects and witnesses. It can also be used by public defenders to find witnesses to prove a defendant's innocence [37]. However, artificial intelligence technology can be like a double-edged sword, whilst protecting society's security, it's rapid development also continues to generate new challenges to public security. *DeepFake* is a good example here. There artificial intelligence-generated video clips can be used with a variety of techniques to create worlds in which the reality has never happened. In 2021, *DeepFake* creators uploaded a fake Tom Cruise deepfake video on *TikTok* that drew two and a half million views, and even the commercial tools used to identify deepfakes cleared the clips as "authentic" [36].

The artificial intelligence company *DeepTrace* discovered 15,000 deepfake videos online in September 2019, nearly doubling in nine months. A staggering 96% were pornographic content, 99% of which were mapped faces from female celebrities to porn stars [33]. Deep forgery can mimic biometric data and potentially spoof

systems that rely on facial, voice, vein, or gait recognition. The more insidious effect of deepfakes and other synthetic media and fake news is the creation of a zero-trust society where people can't or don't bother to distinguish between truth and falsehood. And when trust is eroded, it becomes easier to question particular events. Deepfake videos about business moguls or politicians can trigger stock price fluctuations and even political events.

Another area of concern is the privacy risk posed by the large datasets used to train AI, which crawl the internet for a variety of available data. Especially, as the data subjects may not even know their data has been proliferated across sites and used to train AI tools. The *LAION-5B* dataset, for example, has more than five billion images, which include artwork by living artists, photographs of photographers, medical images, and photos of people who may not believe that their images will suddenly become the basis for AI training. Worryingly, people cannot opt out of being included in these datasets. Even more, these datasets include photo-manipulated celebrity porn, hacked and stolen non-consensual porn, and graphic images of ISIS beheadings [83].

Artificial intelligence-enabled "nudity" technology makes it easy for people without any expertise to create images of people appearing to be naked. In fact, image-based abuse that creates or alters a person's image without their consent disproportionately affects women. The damaging experience for victims of these realistic images can be devastating, affecting their personal and professional lives, as well as their physical and mental health [15]. With the addition of facial recognition, biometrics, genomic data and artificial intelligence predictive analytics, the uncontrolled proliferation of data puts people's privacy at risk. For example, facial recognition company *Clearview AI* collected 20 billion faces from social media sites like *Facebook*, *LinkedIn* and *Instagram*, as well as other parts of the web, to build an application designed to mine every public photo of people online. These images, while publicly available on the Web, are collected without people's consent. The tool mines photos that people don't post of themselves and may not even realize are online. *Clearview AI* has been the target of multiple lawsuits, and its database has been declared illegal in Canada, Australia, the United Kingdom, France, Italy and Greece. It also faces millions of dollars in fines in Europe [37].

More and more research is now using artificial intelligence techniques to make analyses and predictions about data. However, this process can easily be exploited by the unsuspecting for their nefarious purposes. By injecting specially crafted adversarial data into a target training dataset, an attacker may achieve the goal of manipulating machine learning results [76]. For example, by adding perturbed data to the training dataset, researchers altered the results of selfdriving cars' recognition of traffic signs [20]. This is known as *data poisoning*, and this poisoned data is often difficult to detect, potentially leaving a back door for unscrupulous individuals to manipulate AI models if adopted [12]. Therefore, the results of AI predictions based on the use of poisoned data in research may be distorted, misleading, and even inaccurate.

3.5 *The Impact of Artificial Intelligence on Science and Technology*

With sophisticated sensing devices, vast amounts of data, powerful computing capabilities, and 24/7 working hours, AI has greatly expanded the limits of human capabilities. Indeed, it can perform specialized tasks better than many experienced human experts. Taking medicine as an example, studies have documented that AI systems can correctly classify suspicious skin lesions better than dermatologists [21]. Furthermore, the algorithms of AI can be continuously improved and applied to related fields on a large scale and over a short period of time. As a result, once the breakthrough is achieved, the results can often be seen as spectacular. We have seen similar examples many times in fields such as biology and medicine.

Over the past few decades, research on antibiotics has been slow to develop, with few new antibiotics being developed and most newly approved antibiotics being slightly different variants of existing drugs [68]. In 2020, researchers at MIT used deep learning algorithms to analyze more than 100 million compounds in a few days. They discovered a new antibiotic capable of killing 35 potentially deadly bacteria [4]. In July 2022, AI lab DeepMind's *AlphaFold* announced that it had predicted the structures of nearly all of the more than 200 million proteins known to science and made them freely available [18]. This scientific leap, which covers almost all proteins of known organisms in the DNA database, is thought to have the potential to have a huge impact on global problems such as famine and disease [29]. Just a few months later, in November 2022, researchers at another tech giant, *Meta*, used AI to predict the structure of more than 617 million proteins from bacteria, viruses, and other as-yet-uncharacterized microbes in just two weeks [9]. This macrogenomic database reveals the structures of hundreds of millions of the planet's least-known proteins, promising to accelerate advances in medicine, renewable energy and green chemistry [49]. Moreover, many areas of cutting-edge scientific research have, traditionally, required large financial investments in laboratories, equipment and huge amounts of manpower and time to make some progress. However, now artificial intelligence technologies are changing the game. Elements of the scientific process will increasingly be driven by intelligent agents, especially for processes that do not rely on creativity and abstract thinking [6]. Therefore, countries that invest more in artificial intelligence will benefit more from it and will gain higher rates of scientific and technological development.

Although AI technology has all these advantages in scientific research, it still has some shortcomings. The difficulty in using AI technology for scientific research is how to interpret the data. While AI can often make very accurate predictions, it cannot itself explain why and how it makes such predictions. The AI's processing is unknown to humans, which is known as the algorithmic 'Black Box'. Despite the recent academic and industry efforts on 'Explainable AI' (XAI) [17], the results are hardly satisfactory [39]. This means that while advanced technologies can help

researchers to complete the process of data collection and analysis, more efforts are needed to interpret the data and translate the analysis results into knowledge. Some of the findings accomplished by AI are still to be verified and interpreted by human scientists.

In addition to technology, limiting the development of AI in science and technology is the availability of data. In the age of artificial intelligence and big data, more and more data is being collected by emerging digital methods, such as online communities, eye-tracking and wearable technology. On the one hand, this can be great for some developed countries. But on the other hand, some less developed countries and regions are not benefiting from the same technological development. In fact, collecting data in these places is more difficult than in other regions. And as a result, the availability of data is leading to the polarization of market research. That is, in developed countries and regions, the large amount of data allows AI to be better applied to various scientific studies, thus driving rapid growth in science and technology. In contrast, in less developed countries and regions, there is rarely enough data available for research [34]. Take COVID19 related services as an example. Developed countries and regions have near real-time access to a wide range of COVID-19-related data. This allowed for timely analysis and adjustments to vaccine supplies, financial assistance, travel policies, medical aid, and more. In contrast, in underdeveloped regions with more vulnerable populations, there is still not enough data available to study and provide targeted help to people [50].

One possible way to address the difficulties in obtaining data in underdeveloped areas, which affects the conduct of research, is to use artificial intelligence to infer data. *Facebook* has already done a good demonstration of this. Since 2017, *Facebook* has applied artificial intelligence to satellite data to map roads around the world that are unmapped and missing due to insufficient data. Facebook has named the project *Map With AI* [28], and these AI-mapped maps have helped during COVID-19 vaccine deliveries [50]. Similarly, more AI techniques can be used to infer data from underdeveloped regions for research.

4 Challenges of AI in National Security

As mentioned above, AI is bringing disruptive changes in the economy, employment, education and culture, public security, science and technology. As we have read, every country in the wave of this technological revolution is facing new challenges.

4.1 Disinformation Undermines National Security

In a healthy society, institutions, groups, and individuals make informed decisions based on reliable information received from a variety of sources on a daily basis. This is the foundation of a well-functioning society. However, when people are misled

by erroneous, false, or even maliciously falsified information, it may influence their rational judgment. They may even act contrary to their true intentions and interests, which can create many problems for our security on a local and national level. In truth, the ease of access to AI technology today has lowered the threshold for creating false information, posing risks and hazards to society and national security. Interpersonal interactions are often based on confirmation and trust in each other's identities. However, when identities can be falsified, this trust can be harmed, even with serious consequences, and AI-generated photos are one example of this.

Photos of faces generated with generative adversarial networks (GAN) are so realistic that it is difficult for the average person to tell if they are real photos or computer-generated. This is a technique that actually poses the risk of identity forgery. For example, many GAN-generated photos can be accessed from the *thispersondoesnotexist.com* website [40]. Unsuspecting people can use these photos and fictitious personal information to gain the trust of others and commit criminal acts. Officials in the UK, France and Germany have all issued warnings detailing how foreign spies have contacted thousands of people through *LinkedIn.* These spies target people through Deepfake-generated composite portraits and fake social media profiles. Once a target person accepts these spy invitations to connect, other users on the site can view the connection as an endorsement, thereby lowering their guard [63]. Even more alarming than false identities is manipulated information. This can be used to shape public opinion or undermine trust in the authenticity of information. As a result, it can disrupt and undermine social order, democratic institutions and national cohesion. The U.S. *Cybersecurity and Infrastructure Security Agency (CISA)* classifies information manipulation into three types, namely Misinformation, Disinformation, and Malinformation [14].

For example, Russian operatives used AI during the 2016 U.S. presidential election to create and disseminate fake news articles and social media posts in order to influence the outcome of the election [41]. These fake stories were designed to spread quickly and widely via the Internet, and many people believed them to be true. The use of artificial intelligence in this context enabled Russian agents to generate large amounts of false content in a short period of time, making it difficult for people to distinguish between truth and falsehood. This type of information manipulation can have serious consequences, as it can erode trust in the media and democracy.

4.2 Human Rights Issues in Artificial Intelligence

As AI technology rapidly evolves, they are also concerns about the ethics of AI. It seems that the generation of new laws is almost always a reactive response to address existing issues. Therefore, they usually lag behind the real-world needs, as do the industry norms and standards. It is important to note that just because an activity does not violate current laws, it does not mean that it is ethical.

The growth of the Internet and IoT has made vast amounts of data readily available; AI and big data technologies have in turn made it easy to infer new insights from a variety of seemingly unrelated data [73]. The aggregation of data often comes with the risk of privacy breaches. For example, the retailer giant *Target* could infer that a high school girl was pregnant based on her purchase history and hand out baby product ads to her, even while the girl's father was still in the dark [38]. As the cost of storing electronic data continues to decrease, more and more users data will be stored for long periods of time. In addition, some deidentified data may be re-identified, and non-sensitive data may become sensitive due to new information generated by data aggregation. This all can threaten the privacy of users. For example, many mobile applications collect users' locations to provide better services and then use this location data for marketing research. This location data, even de-identified, can be used to figure out the privacy of users, where they go, who they meet, and their daily activities, all of which can be easily tracked. Even the most privacy-conscious people, such as former USA President Trump, Secret Service agents or Supreme Court technicians, are not exceptions [67].

Furthermore, the development of Internet of Things (IoT) and wearable devices has resulted in users' physiological data (e.g. breathing, heartbeat, blood pressure, pulse), behavioral habits (e.g. sleep patterns, exercise habits, driving habits), and behavioral preferences (e.g. dietary preferences, shopping preferences, entertainment preferences) being captured precisely. Frighteningly, this data can even analyze information about their state-of-behavior more accurately than the users themselves can. By analyzing a person's posts, likes, ad clicks, and browsing history, it is possible to figure out their personality traits, attitudes, feelings, perceptions, beliefs, and product/service brand preferences. In addition, online users rarely need to disguise themselves to meet social expectations as they do offline, so they will show a more authentic side of themselves. Moreover, this user data collected on an ongoing basis can more accurately reflect the stable characteristics of the users in question. With the help of Content Mining and Natural Language Processing (NLP) techniques, researchers can analyze surveys, web text, online comments, tweets, etc. to generate useful insights, such as for opinion mining and sentiment analysis. This information extracted from text data can often be used for psychographic profiles to more accurately reflect the attitudes, interests, personalities, values, opinions and lifestyles of users, but often without the data subject's knowledge, exposing them to privacy violations [79].

Some data protection laws, such as the EU's *General Data Protection Regulation (GDPR)*, regulate the collection, processing and storage of data. However, there are still many operational gaps and a need for more practical and detailed industry standards to ensure that data is used ethically before, during, and after research. With the rapid development of AI, there is an increasingly urgent need to address the ethical issues associated with it. This requires careful consideration by policymakers, academia, industry, and other stakeholders. Especially, when they need to take effective measures to ensure that the benefits of AI are balanced with the need to protect the rights and the interests of individuals.

Another human rights hazard posed by AI is discrimination and bias. Datasets used to train AI models may have sample bias, or developers may inadvertently introduce bias into the system, which can produce biased results, and the use of these biased results in automated decision-making can result in discriminatory treatment. For example, a study on a health management algorithm that affects millions of people in the United States showed that because the algorithm predicts disease risk in terms of how much health care costs, but inequities in access to care mean that black patients have less health care costs, black patients are in fact much sicker than white patients for a given risk score predicted by the system [53]. As the use of AI becomes more prevalent, discrimination and bias in AI can have widespread negative effects, and without effective action, any individual or group may be treated unfairly because of race, color, gender, age, religion, sexual orientation, and a variety of other reasons.

4.3 Legislative Improvement of Artificial Intelligence

Although various countries have enacted various laws on data protection, the legal protection provided in practice is still inadequate and data privacy violations still occur. For example, in the 2010s, personal data belonging to millions of *Facebook* users was collected without consent by the British consulting firm *Cambridge Analytica* for political advertising. A New York Times report called 'Times Privacy Project Links to an external site' also revealed how cell phone location data can expose an individual's whereabouts. These invasions of privacy in fact put people in danger—even presidents and their security experts, What's more, with the rapid development of artificial intelligence, even some unrelated information may generate new sensitive information under the role of data aggregation. For example, merchants can generate psychographic profiles from users' purchase records to understand their interests, beliefs, values and other personal traits. Therefore, in fact, every piece of personal information we handle is more or less related to personal privacy.

As we discussed earlier, in the era of Big Data, data is the new oil, containing valuable information resources [7] that can bring power and wealth to its owners. The rapid concentration of citizen data to monopolies is a hidden danger to democracy, human rights and even national security. Once such a monopoly is established, it will be difficult to counterweight it. Therefore, the timely establishment of a sound legal system to regulate access to data and the use of artificial intelligence is necessary to ensure long-term healthy economic development and national security. Indeed, to prevent inappropriate uses of technology, data, and automated systems from threatening the rights of the American public, the White House *Office of Science and Technology Policy (OSTP)* has released the *Blueprint for an* AI *Bill of Rights* in October 2022. This bill identifies five principles to guide the design, use, and deployment

of automated systems. These principles include Safe and Effective Systems, Algorithmic Discrimination Protections, Data Privacy, Notice and Explanation, as well as Human Alternatives, Consideration, and Fallback. Of these five principles, data privacy is considered a fundamental though cross-cutting principles are required to achieve all the other goals in this framework [80].

The *Federal Trade Commission (FTC)* is increasingly using algorithmic vandalism as a tool to control technology companies. Algorithmic vandalism requires companies that illegally collect data to "delete the data they illegally obtained, destroy any resulting algorithms, and pay fines for their violations. Algorithmic vandalism may hold organizations accountable not only for the way they collect data, but also for the way they process it" [8, p. 1]. In fact, legislatures around the world are recognizing the need to hold companies that illegally collect data, to develop or train algorithms, accountable. As a result, additional regulations may be introduced to mitigate the problems associated with these practices.

5 Discussion

As we discussed earlier, AI is changing people's lives in every aspect. In doing so, it is also posing some challenges, and we should proactively take effective measures to reduce possible risks and make it better for human beings.

5.1 Reducing Regional Imbalances

Regional imbalances are a common problem between countries and between regions within countries. Various reasons such as historical development and resource distribution cause imbalances, along with differences in development between countries or regions in the fields of economy, culture, healthcare, education, etc. We have seen the impact of this imbalance from the gap between developed and underdeveloped countries, and even between regions in countries with large territories like China, India, and the United States. This imbalance has caused huge differences in people's income levels and even happiness indices. If the opportunity is grasped, the application of AI technology is expected to bring more development opportunities and faster development speed to relatively less developed regions and reduce regional disparities. Less developed regions can even benefit from the development of AI technology more than developed regions, so that people in these regions can enjoy improved medical conditions, equal educational opportunities, and more employment opportunities. For example, the *World Health Organization's World Cancer Report* shows that more than 60% of the global cancer burden occurs in Asia, Africa, and LMICs in Central and South America, and 70% of cancer deaths occur in these regions [82]. Therefore, the development of AI in cancer treatment will benefit people in these regions even more. Smaller regional development gaps will lead to a more

prosperous international market and improve the common welfare of all humanity. But on the other hand, we should also be aware that this gap is likely to continue to widen in the area of cutting-edge technology. A comparative study of eastern, central, and western China shows that industrial intelligence improves inequality in consumer welfare between regions, while having the potential to exacerbate regional inequality in innovation [44]. Less developed regions may face greater technological dependence if they fail to keep and catch up with the ever advancing technological wave.

5.2 Building Accountable AI Systems

To reduce the risks posed by AI, it should first be controlled at the source. By this we mean that it should be transparent, fair, and accountable from the time when it is first designed, developed, and then used. Firstly, accountability should be considered from the earliest stages of development, with a commitment to eliminate bias and/or unfairness. This means incorporating mechanisms to explain and justify decisions made by AI, and ensuring that AI acts in a responsible and ethical manner. Secondly, AI systems should be tested and evaluated to ensure that they operate as intended and do not make biased and/or unfair decisions. Thirdly, there should be a strong legal and regulatory framework to support responsible AI. This framework should define the rights and responsibilities of AI developers, users, and other stakeholders. In addition, it should provide clear guidance on how to ensure that AI systems act in a responsible manner.

To better control the risks of AI systems, many countries and regions are committed to building responsible AI. The European Union proposed the *European Artificial Intelligence (AI) Act* in April 2021, a law that classifies applications of AI into three risk categories [26]. Under this category, applications and systems that pose unacceptable risks would be banned, high-risk applications would need to comply with specific legal requirements, and applications not explicitly banned or classified as high-risk would be largely unregulated [3]. However, some scholars have questioned this conflation of 'trustworthiness' with 'acceptability of risk' and have pointed out that there is still a threat of misalignment between the actual level of trust and the trustworthiness of the applied AI [43].

5.3 Strengthen AI Education and Skills Training

In contrast to the rapid development of AI technology, education is a long, slow process. There is a need to take a forward-looking view to provide the younger generation and those educating them with the knowledge and skills to exist safely in this AI era. For young people, it is important to enhance their AI literacy. This includes giving them a basic understanding of what AI is and how it works. It gives

them access to AI tools and systems, and enables them to learn how to use AI to solve real-world problems. For educators, it should focus on helping students develop the critical thinking and problem-solving skills that are useful in an AI-driven world. This could include teaching them on how to assess and understand the reliability and validity of information, how to solve complex problems, and how to think creatively and innovate. It is also important to educate young people about the ethical and social implications of AI, such as the potential biases and limitations regarding AI algorithms, and how to use AI responsibly and ethically.

For those who may be affected by AI technologies and need to upgrade their skills, they should be provided with vocational skills training tailored to their needs. For example, this can be an AI-driven, personalized system of skills enhancement that helps them learn faster and more effectively to adapt to new job demands. The state should also make more AI research resources available to the public to enrich the AI research ecosystem. More educational resources for AI professionals should be made available to a broader population so that AI professional education is equitably accessible to all, especially those from underrepresented groups, as one measure to avoid or reduce bias. According to an analysis on LinkedIn, only 22% of AI professionals worldwide are women, a huge contrast to the 78% of male professionals [77]. And the AI industry, dominated by men, tends to produce systems and products with gender biases and stereotypes [81]. For example, AI virtual personal assistants are often set up with feminine images and voices that are in fact an extension of the stereotype of the female secretary and reinforce the discrimination of women being in a submissive position [1, 13]. To bridge the resource divide in AI research, the U.S. established the *National AI Research Resources (NAIRR) Task Force* in June 2021 to establish a *National AI Research Resource* that democratizes access to AI R&D for U.S. researchers and students by making computational infrastructure, public- and private- sector data, and testbeds easily accessible [54].

5.4 Improve the Legal and Regulatory System

The data used for AI learning is closely related to people's privacy, and strengthening the protection of data is an important prerequisite for protecting people's privacy. At present, more than 130 countries have enacted laws and regulations related to privacy protection [31], but people's privacy is still not fully protected, and with the development of AI technology, more risks of privacy infringement may emerge. This means that our legal system still needs to be further refined in detail to make it more workable. Traditional privacy protection laws or data protection laws focus on the protection of existing data processing processes such as data collection, storage, and transmission, and fail to provide protection for new information generated in the process of data aggregation, analysis, and inference [74]. In today's increasingly intelligent AI algorithms, the law should provide more detailed and clear regulation of data aggregation and inference, and how to apply the results. Moreover, while many laws provide for data desensitization, there is no clear definition of what standards should

be met [58], which makes it de facto difficult for the laws to be effectively enforced. The authors of this paper argue that when data controllers provide desensitized data to external parties, they should have a reasonable expectation of the possibility of data re-identification and take proactive measures to prevent re-identification.

In response to the increasingly pressing legal issues regarding the use of AI, countries are stepping up their efforts to improve legislation related to AI. In the United States, at least 17 states have introduced general AI bills or resolutions as of August 2022 and enacted them in Colorado, Illinois, Vermont, and Washington [52]. In October 2020, the European Parliament adopted several resolutions related to AI, including on ethics, liability and copyright [22–24], and in 2021, resolutions were adopted on AI in criminal matters and in the fields of education, culture and audio-visual [25, 72]. The European Commission has put forward a proposed regulatory framework on AI that proposes a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum requirements necessary to address the risks and issues associated with AI without unduly restricting or impeding technological development or otherwise disproportionately increasing the cost of placing AI solutions [27].

6 Conclusion

In the era of Industry 4. 0, artificial intelligence has been involved in all aspects of social development. As we have discussed, this is closely related to the strength of a nation's power. But there needs to be a balance. Indeed, the rapid development of artificial intelligence technology is forcing every country to take on the opportunities it affords but also to face the challenges it creates.

On the one hand, the discipline of artificial intelligence has only been in existence for a few decades, and it has already experienced a stagnation (e.g,. lack of growth). It has really only been developing rapidly in the last two decades. AI's development can be described as being at the starting phase of a race in which every runner has the opportunity to win. Indeed, every country can benefit from this disruptive technology to promote economic development, improve the labor environment, enhance the quality of education, enrich cultural life, and accelerate technological development for the benefit of its people. As we have read, the development of artificial intelligence today cannot be achieved without the contributions of scientists from all disciplines around the world. The prosperity of artificial intelligence depends on having a unified vision of benefiting all of humanity. Artificial intelligence has given people a fairer choice, reduced the gap between the rich and the poor, freed workers from monotonous and heavy manual labor. It has also given people the opportunities to choose job positions that better realize their values. It has made it possible for children in remote areas to enjoy personalized educational experiences. Moreover, it has allowed people suffering from illness to benefit from medical breakthroughs discovered through the technological development.

On the other hand, we should also be soberly aware that the rapid development of AI technology is creating challenges and putting every country under immense pressure. Artificial intelligence is still developing faster than people can think. This challenges and even counters the existing ethical and legal systems which are still dangerously lagging far behind AI. Just as nuclear energy can either generate electricity for the benefit of humanity or be used as a weapon to destroy it, AI is similar. Therefore, we need to push to ensure that the tremendous energy released by AI is used for good purposes, rather than being exploited for the interests of criminal groups. History has shown countless times that when a force is extremely powerful, it often lacks a counterweight. This usually has disastrous consequences, and in many ways, the same can be said for the field of AI. Therefore, the time has come to demand strict governance and control of AI. A nation needs to ensure that their citizens are protected and that their rights are not violated. Especially, when people's data can be in the hands of a few large corporations. There needs to be standards, an approved way of designing, developing and working with AI. We need to make sure that there are checks in place and that these new technologies are not being misused. Finally, we need a society in which everyone benefits from AI, rather than being constrained, manipulated and/or endangered by it. This is our only hope when striving for a responsible national security.

References

1. Adams R (2022) Artificial intelligence has a gender bias problem—just ask siri. The Conversation, Sep. https://theconversation.com/artificial-intelligence-has-agender-bias-problem-just-ask-siri-123937
2. AFP (2022) Dutch police create deepfake video of murdered boy, 13, in hope of new leads. https://www.theguardian.com/world/2022/may/23/dutchpolice-create-deepfake-video-of-murdered-boy-13-in-hope-of-new-leads
3. Artificial Intelligence Act (2022) What is the EU AI act? the artificial intelligence act, Nov. https://artificialintelligenceact.eu/
4. BBC (2020) Scientists discover powerful antibiotic using AI. BBC News, Feb. https://www.bbc.com/news/health-51586010
5. Becker BA, Denny P, Finnie-Ansley J, Luxton-Reilly A, Prather J, Santos EA (2023) Programming is hard–or at least it used to be: educational opportunities and challenges of AI code generation
6. Briscoe E, Fairbanks J (2020) Artificial scientific intelligence and its impact on national security and foreign policy. Orbis 64(4):544–554
7. Buhl HU, Röglinger M, Moser F, Heidemann J (2013) Big data. Bus Inf Syst Eng 5(2):65–69
8. Caballar RD (2022) "Algorithmic destruction" policy defangs dodgy AI new regulatory tactic of deleting ill-gotten algorithms could have bite. https://spectrum.ieee.org/ai-concerns-algorithmic-destruction
9. Callaway E (2022) Alphafold's new rival? meta AI predicts shape of 600 million proteins. Nature News, Nov. https://www.nature.com/articles/d41586-022-03539-1
10. Chen J, Song N, Su Y, Zhao S, Zhang Y (2022) Learning user sentiment orientation in social networks for sentiment analysis. Information Sciences
11. Chen M, Tworek J, Jun H, Yuan Q, Pinto HPdO, Kaplan J, Edwards H, Burda Y, Joseph N, Brockman G et al (2021) Evaluating large language models trained on code. arXiv preprint arXiv:2107.03374

12. Chen X, Liu C, Li B, Lu K, Song D (2017) Targeted backdoor attacks on deeplearning systems using data poisoning. arXiv preprint arXiv:1712.05526
13. Chin C, Robison M (2022) How AI bots and voice assistants reinforce gender bias. Brookings, Mar. https://www.brookings.edu/research/how-ai-botsand-voice-assistants-reinforce-gender-bias/
14. CISA: Homepage: Cisa. Cybersecurity and infrastructure security agency (CISA). https://www.cisa.gov/
15. Cole S (2019) Deepnude: the horrifying app undressing women, Jun. https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudesof-any-woman
16. COMEST: Preliminary study on the ethics of artificial intelligence. Unesdoc.unesco.org. https://unesdoc.unesco.org/ark:/48223/pf0000367823
17. Das D, Nishimura Y, Vivek RP, Takeda N, Fish ST, Ploetz T, Chernova S (2021) Explainable activity recognition for smart home systems. arXiv preprint arXiv:2105.09787
18. Deepmind: alphafold reveals the structure of the protein universe. https://www.deepmind.com/blog/alphafold-reveals-the-structure-of-the-proteinuniverse
19. Department of Justice (2020) Justice department sues monopolist google for violating antitrust laws. The United States Department of Justice, Oct. https://www.justice.gov/opa/pr/justice-department-sues-monopolist-googleviolating-antitrust-laws
20. Ding S, Tian Y, Xu F, Li Q, Zhong S (2019) Trojan attack on deep generative models in autonomous driving. In: International conference on security and privacy in communication systems, pp 299–318, Springer
21. Esteva A, Kuprel B, Novoa RA, Ko J, Swetter SM, Blau HM, Thrun S (2017) Dermatologist-level classification of skin cancer with deep neural networks. Nature 542(7639):115–118
22. EU: European parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(ini)). EUR, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020IP0277amp;from=EN
23. EU: European parliament resolution of 20 October 2020 with recommendations to the commission on a civil liability regime for artificial intelligence (2020/2014(inl)). EUR, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020IP0276amp;from=EN
24. EU: European parliament resolution of 20 October 2020 with recommendations to the commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(inl)). EUR, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020IP0275amp;from=EN
25. EU: European parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2021). https://www.europarl.europa.eu/doceo/document/TA-9-20210405_EN.html
26. EU: Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (Sep 2021). https://artificialintelligenceact.eu/the-act/
27. EU: Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. EUR (2021), https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52021PC0206amp;from=EN
28. Gao X (2020) AI is supercharging the creation of maps around the world. Tech at Meta, Jul. https://tech.fb.com/artificial-intelligence/2019/07/ai-is-superchargingthe-creation-of-maps-around-the-world/
29. Geddes L (2022) Deepmind uncovers structure of 200m proteins in scientific leap forward. The Guardian, Jul. https://www.theguardian.com/technology/2022/jul/28/deepmind-uncoversstructure-of-200m-proteins-in-scientific-leap-forward
30. Goldhaber MH (1997) The attention economy and the net. First Monday 2(4). https://doi.org/10.5210/fm.v2i4.519. https://journals.uic.edu/ojs/index.php/fm/article/view/519
31. Greenleaf G (2019) Global data privacy laws 2019: 132 national laws & many bills
32. Guardian (2020) US justice department sues Google over accusation of illegal monopoly. The Guardian, Oct. https://www.theguardian.com/technology/2020/oct/20/us-justice-departmentantitrust-lawsuit-against-google

33. Guardian (2020) What are deepfakes—and how can you spot them? https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakesand-how-can-you-spot-them
34. Hair JF, Ortinau DJ, Harrison DE (2010) Essentials of marketing research, vol 2. McGraw-Hill/Irwin, New York, NY
35. Hawksworth J, Berriman R, Goel S (2018) Will robots really steal our jobs? an international analysis of the potential long term impact of automation
36. Hern A (2021) 'I don't want to upset people': Tom Cruise deepfake creator speaksout. https://www.theguardian.com/technology/2021/mar/05/how-startedtom-cruise-deepfake-tiktok-videos
37. Hill K (2022) Clearview AI, used by police to find criminals, is now in public defenders' hands. https://www.nytimes.com/2022/09/18/technology/facialrecognition-clearview-ai.html
38. Hill K (2022) How target figured out a teen girl was pregnant before her father did. Forbes, Oct. https://www.forbes.com/sites/kashmirhill/2012/02/16/howtarget-figured-out-a-teen-girl-was-pregnant-before-her-fatherdid/?sh=7d59935a6668
39. Innerarity D (2021) Making the black box society transparent. AI Soc 36(3):975–981
40. Karras T (2022) This person does not exist. https://thispersondoesnotexist.com/
41. Kelly M, Samuels E (2019) Analysis|how Russia weaponized social media, got caught and escaped consequences, Nov. https://www.washingtonpost.com/politics/2019/11/18/how-russia-weaponizedsocial-media-got-caught-escaped-consequences/
42. Kemp S (2022) Digital 2022: global overview report—datareportal—global digital insights. Data Reportal, May. https://datareportal.com/reports/digital-2022global-overview-report
43. Laux J, Wachter S, Mittelstadt B (2022) Trustworthy artificial intelligence and the European union AI act: on the conflation of trustworthiness and the acceptability of risk. Available at SSRN 4230294
44. Li S, Hao M (2021) Can artificial intelligence reduce regional inequality? evidence from China
45. Li Y, Choi D, Chung J, Kushman N, Schrittwieser J, Leblond R, Eccles T, Keeling J, Gimeno F, Lago AD et al (2022) Competition-level code generation with alphacode. arXiv preprint arXiv:2203.07814
46. Liu M, Yu J, He H, Wang R, Zhan H (2018) Research on industrial cluster and the siphon effect of talent accumulation. In: 2018 14th international conference on natural computation, fuzzy systems and knowledge discovery (ICNC-FSKD), pp 815–818, IEEE
47. McCarthy J (2007) What is artificial intelligence?
48. McCarthy J, Minsky ML, Rochester N, Shannon CE (2006) A proposal for the dart mouth summer research project on artificial intelligence, August 31, 1955. AI Mag 27(4):12–12
49. Meta (2022) New AI research could drive progress in medicine and clean energy, Nov. https://about.fb.com/news/2022/11/ai-protein-research-could-driveprogress-in-medicine-clean-energy/
50. Meta AI (2022) How maps built with Facebook AI can help with covid-19 vaccine delivery. https://ai.facebook.com/blog/how-maps-built-with-facebook-aican-help-with-covid-19-vaccine-delivery/
51. Microsoft: Machine learning made easy, Lobe. https://www.lobe.ai/
52. NCSL (2022) Legislation related to artificial intelligence, Aug. https://www.ncsl.org/research/telecommunications-and-informationtechnology/2020-legislation-related-to-artificial-intelligence.aspx
53. Obermeyer Z, Powers B, Vogeli C, Mullainathan S (2019) Dissecting racial bias in an algorithm used to manage the health of populations. Science 366(6464):447–453
54. Parker L (2022) Bridging the resource divide for artificial intelligence research, May. https://www.whitehouse.gov/ostp/news-updates/2022/05/25/bridgingthe-resource-divide-for-artificial-intelligence-research/
55. Pearce H, Ahmad B, Tan B, Dolan-Gavitt B, Karri R (2022) Asleep at the keyboard? assessing the security of GitHub Copilot's code contributions. In: 2022 IEEE symposium on security and privacy (SP), pp 754–768, IEEE
56. Person, Francois Aulner, F.Y.C. (2021) Google loses challenge against EU antitrust ruling, fine. Reuters, Nov. https://www.reuters.com/technology/eu-court-upholdseu-antitrust-ruling-against-google-2021-11-10/

57. PwC: Pwc's global artificial intelligence study: sizing the prize. https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificialintelligence-study.html
58. Quinn P (2021) The difficulty of defining sensitive data—the concept of sensitive data in the EU data protection framework. German Law J 22(8):1583–1612
59. Roose K (2022) A.I.-generated art is already transforming creative work. https://www.nytimes.com/2022/10/21/technology/ai-generated-art-jobs-dall-e2.html
60. Roose K (2022) An A.I.-generated picture won an art prize. Artists aren't happy. https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligenceartists.html
61. Roose K (2022) A coming-out party for generative A.I., Silicon Valley's new craze. https://www.nytimes.com/2022/10/21/technology/generative-ai.html
62. Russell SJ (2010) Artificial intelligence a modern approach. Pearson Education Inc.
63. Satter R (2019) Experts: spy used AI-generated face to connect with targets. https://apnews.com/article/ap-top-news-artificial-intelligence-socialplatforms-think-tanks-politics-bc2f19097a4c4fffaa00de6770b8a60d
64. Simon HA et al (1971) Designing organizations for an information-rich world. Comput Commun Public Interes 72:37
65. Smith CS (2022) 'No-code' brings the power of A.I. to the masses. The New York Times, Mar. https://www.nytimes.com/2022/03/15/technology/ai-nocode.html?action=clickamp;module=RelatedLinksamp;pgtype=Article
66. Teachable Machine (2022). https://teachablemachine.withgoogle.com/
67. Thompson SA, Warzel C (2019) How to track president trump. The New York Times, Dec. https://www.nytimes.com/interactive/2019/12/20/opinion/locationdata-national-security.html
68. Trafton A (2020) Artificial intelligence yields new antibiotic. MIT News, Massachusetts Institute of Technology. https://news.mit.edu/2020/artificialintelligence-identifies-new-antibiotic-0220
69. Turing AM (2012) Computing machinery and intelligence (1950). In: The essential turning: the ideas that gave birth to the computer age, pp 433–464
70. UNESCO (2021) AI and education: guidance for policy-makers. Unesdoc.unesco.org. https://unesdoc.unesco.org/ark:/48223/pf0000376709
71. United Nations (2022) Will robots and AI cause mass unemployment? not necessarily, but they do bring other threats. https://www.un.org/en/desa/will-robots-and-ai-cause-mass-unemploymentnot-necessarily-they-do-bring-other
72. Verheyen S (2021) Report on artificial intelligence in education, culture and the audiovisual sector: A9-0127/2021: European parliament. REPORT on artificial intelligence in education, culture and the audiovisual sector | A9-0127/2021 | European Parliament. https://www.europarl.europa.eu/doceo/document/A-9-20210127_EN.html
73. Wachter S (2020) Affinity profiling and discrimination by association in online behavioral advertising. Berkeley Tech LJ 35:367
74. Wachter S, Mittelstadt B (2019) A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Colum Bus L Rev, p 494
75. Walsh F (2020) AI 'outperforms' doctors diagnosing breast cancer. BBC News, Jan. https://www.bbc.com/news/health-50857759
76. Wang Y, Chaudhuri K (2018) Data poisoning attacks against online learning. arXivpreprint arXiv:1808.08994
77. Weforum (2018) Global gender gap report 2018. World Economic Forum. https://www.weforum.org/reports/the-global-gender-gap-report-2018
78. Weforum (2020) The future of jobs report 2020. World Economic Forum. https://www.weforum.org/reports/the-future-of-jobs-report-2020
79. Wells WD (1975) Psychographics: a critical review. J Mark Res 12(2):196–213
80. Whitehouse: Blueprint for an AI bill of rights. https://www.whitehouse.gov/wpcontent/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf
81. Whittaker M, Crawford K, Dobbe R, Fried G, Kaziunas E, Mathur V, West SM, Richardson R, Schultz J, Schwartz O et al (2018) AI now report 2018. https://ainowinstitute.org/AI_Now_2018_Report.pdf

82. Wild C, Weiderpass E, Stewart BW (2020) World cancer report: cancer research for cancer prevention. IARC Press
83. Xiang C (2022) AI is probably using your images and it's not easy to optout. https://www.vice.com/en/article/3ad58k/ai-is-probably-using-yourimages-and-its-not-easy-to-opt-out
84. Yu S, Carroll F (2022) Insights into the next generation of policing: understanding the impact of technology on the police force in the digital age, pp 169–191